Foresight of Evolving Security Threats Posed by Emerging Technologies

Project acronym: FESTOS
Project no: 217993

WP2: Horizon scanning
Deliverable D2.3:
Final report on potentially threatening technologies

Formal Deliverable
Distribution: Public
Version 2.0

Start date of project: 1.03.09
Duration: 30 months

Authors: Aharon Hauptman, Yoel Raban, Ori Katz, Yair Sharan – ICTAF
# Change Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>25.10.2010</td>
<td>Aharon Hauptman</td>
<td>ICTAF</td>
</tr>
<tr>
<td>0.2</td>
<td>09.11.2010</td>
<td>Aharon Hauptman</td>
<td>ICTAF</td>
</tr>
<tr>
<td>0.3</td>
<td>05.12.2010</td>
<td>Aharon Hauptman</td>
<td>ICTAF</td>
</tr>
<tr>
<td>1.0</td>
<td>15.12.2010</td>
<td>Aharon Hauptman</td>
<td>ICTAF</td>
</tr>
<tr>
<td>2.0</td>
<td>29.5.2011</td>
<td>Aharon Hauptman</td>
<td>ICTAF</td>
</tr>
</tbody>
</table>

# Release Approval

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aharon Hauptman</td>
<td>Leader WP2</td>
<td>29.5.2011</td>
</tr>
<tr>
<td>Yair Sharan</td>
<td>Project Manager</td>
<td>29.5.2011</td>
</tr>
</tbody>
</table>
Table of Contents

Chapter 1: Introduction .................................................................................................................. 6

Chapter 2. Overview of the FESTOS expert survey ................................................................. 8

2.1 The survey structure ............................................................................................................. 8

2.2 Respondents profile ............................................................................................................. 8

2.3 General Attitudes towards Future Technology Threats ..................................................... 10

Chapter 3. Main Field: Information and Communication Technologies (ICT) ... 13

3.1 ICT – introductory overview ............................................................................................. 13

3.2 Selected ICTs and evaluation of associated potential threats ........................................... 16

1. Internet of Things (IoT), Ambient Intelligence (AmI), Ubiquitous Computing .. 16

2. Smart Mobile telephone technologies mash-ups ................................................................. 19

3. Radio-frequency identification (RFID) and “RFID-dust” .................................................. 21

4. Ultra-dense Data Storage ...................................................................................................... 24

5. Artificial Intelligence (AI) ................................................................................................... 26

6. Cloud Computing .................................................................................................................. 29

Chapter 4. Main Field: Nanotechnologies ................................................................................. 31

4.1 Nanotechnologies: Introductory Overview ...................................................................... 31

4.2 Selected Nanotechnologies and evaluation of associated potential threats ................. 34

1. Self-replicating Nanoassemblers ......................................................................................... 34

2. Energetic nanomaterials ....................................................................................................... 36

3. Tailored Nanoparticles ......................................................................................................... 38

4. Medical Nanorobots ............................................................................................................. 40

5. Molecular manufacturing ...................................................................................................... 42

6. Molecular nanosensors ......................................................................................................... 43

Chapter 5. Main Field: Biotechnology ....................................................................................... 45
5.1 Biotechnology: Introductory Overview .......................................................... 45

5.2 Selected biotechnologies and evaluation of associated potential threats ....... 48
1. Synthetic Biology (Synbio) .............................................................................. 48
2. DNA-protein interaction .................................................................................. 51
3. Induced Pluripotent Stem Cells (iPS cells) ...................................................... 53
4. Bio-mimicking for fluids mixing at extremely small scales .......................... 55
5. Gene transfer .................................................................................................... 57

Chapter 6. Main Field: Robotics ........................................................................ 59

6.1 Robotics: Introductory Overview .................................................................. 59

6.2 Selected Robotics technologies and evaluation of associated potential threats ........................................................................................................ 62
1. AI-based Robot-Human Interaction and Co-existence ................................. 62
2. Autonomous & Semi-Autonomous Mini Robots: Toys and Amateur Objects . 65
3. Robots as artificial limbs .................................................................................. 67
4. Ethical Control of Robots ................................................................................ 69
5. Swarm Robotics ............................................................................................... 71

Chapter 7. Main Field: New Materials ............................................................... 74

7.1 New Materials: Introductory Overview ....................................................... 74

7.2 Selected New Materials technologies and evaluation of associated potential threats ........................................................................................................ 78
1. Metamaterials and Optical Cloaking ............................................................... 78
2. Future fuels and structural materials for nuclear technologies. ..................... 81
3. Crystalline polymers, polymer blends, multilayer assemblies. .................... 83
4. Water catalyzing explosive reactions ............................................................ 85
5. Personal rapid prototyping and 3-D printing machines .................................. 87
6. Programmable Matter .................................................................................... 90

Chapter 8. Converging Technologies .............................................................. 93

8.1 Converging Technologies: Introductory Overview ................................... 93
8.2 Selected Converging Technologies and associated potential threats..............96

1. Nanotechnology-enabled brain implants..........................................................96

2. Brain-to-brain communication ("Radiotelepathy") ........................................99

3. Brain-Computer Interface – "Mind Reading" commercial gadgets.............101

4. Cyborg Insects ...................................................................................................104

5. Human enhancement .........................................................................................106

Chapter 9. Technologies and potential threats – integrative assessment ...... 108

9.1 Maturity timeframes ......................................................................................108

9.2 Severity of Threat and Easiness of Use for Malicious Purposes ...............111

9.3 Likelihood to actually pose a security threat in the future .........................118

9.4 The impact on society: different societal spheres that might be affected......130

9.5 Some observations and insights from respondents’ comments..................132

10. Conclusions......................................................................................................134

Appendix A – Full text of selected respondents’ comments.............................136
"Unless we invent new threats, we won't be able to prevent them."
Karlheinz Steinmüller

Chapter 1: Introduction

FESTOS deals with future security threats posed by emerging technologies and emerging areas of applied research. The main goal of the project is to identify and assess these potentially evolving threats and to propose policy guidelines aimed at minimizing the likelihood of their realisation. This report is the final deliverable in Workpackage 2: "The Technology Landscape and Horizon". It integrates the results (and respected deliverables) of the following tasks of WP2.

Task 1: Horizon scanning of emerging technologies and scientific developments, which may pose security threats in the future. Summarised in D2.1 – Preliminary mapping of potentially threatening technologies.


In accordance with the project’s workplan, the scanning effort focused on selected technologies in five main fields: ICTs, Nanotechnologies, Biotechnology, Robotics, New Materials, and Converging Technologies (i.e. Nano-Bio-Info-Cogno convergence). Naturally, many technologies are associated with more than one of the five main fields, as the boundaries between them are blurred, and technologies very often do not clearly fall into a single distinct category.

In order to define a reasonable and manageable scope for the study, the following principles were agreed upon by the FESTOS consortium:

1. The security threats under consideration are potential threats of intentional malicious use of new technologies by terrorism and/or organized crime. Hence, safety hazards caused by unintentional inadequate use or natural disasters are out of scope.

2. The scanning for relevant technologies shall focus on emerging technologies that are being developed (or could be developed) for civilian (non-military) use, and may pose potential security threats if abused. Hence, military technologies (developed specifically for the military market and for military purposes) are out of scope.

Despite the decision to limit the scope to civilian technologies, we have to be cautious and remember that the boundaries between the military and civilian domains are sometimes vague. Numerous non-military spin-offs and start-ups stem from military applications and from defence industries. On the other hand, new technologies are often being developed in defence laboratories for dual use or even for “pure” civilian applications. Therefore the defence arena is not ignored altogether, but rather explored selectively.

The results of the horizon scanning (D2.1) were based on a broad literature survey, interviews with relevant experts, and internal discussions within the project team. For each technology, "potential threat indications" were pointed out as preliminary "weak signals" to be further analysed in the next stages of the project.
The main objective of the worldwide online expert survey that followed the initial scanning was to elicit experts' knowledge and opinions about the threat potential of selected emerging technologies. The survey results provided additional dimension to the preliminary mapping, and additional insights were provided by the subsequent analysis and categorisation of threats performed in WP3, deliverable D3.2 ("Categorised security threats in foresight perspective"). The expert survey also covered issues important for analysing "security climates" (general attitudes to technology-related threats), as an input to the subsequent WP4 dealing with this topic.

The particular technologies in the survey were selected by the project consortium based on the 80 technologies previously described in D2.1 as a result of the preliminary mapping. As in every expert survey, an inevitable compromise had to be made between the desire to cover as many technologies as possible, and the necessity to refrain from a too long time-consuming questionnaire. On the other hand, several technologies (e.g. cloud computing) were added to the survey due to their importance, although not previously covered in D2.1.

The process of the preliminary scanning and then the selection of technologies for further evaluation in the expert survey are two steps of the so-called "surveillance filtering" process as described in FESTOS deliverable D3.2. In order to accomplish the filtering we convened internal expert discussion groups to sort out the technologies to be addressed in the survey, taking into account the six S&T fields to be covered. Discussion groups included in addition to consortium members also experts from the technology fields to verify with them the relevance of the detailed technologies for the survey. The involvement of the project's Advisory Security Board (ASB) members was very valuable at this stage. Hence, the final list of technologies selected for assessment in the expert survey and presented in this report represents a good balance between technologies from the different fields, minimises the overlap between technologies and excludes some of those for which sufficient available information was available.

In the present report the description of each technology is followed by the expert survey results regarding this technology. Integrative results are also presented, as well as additional observations and insights.

For completeness, in the introductory overviews of each technology field we briefly mention also the technologies mapped in D2.1 but not analysed in the expert survey.
Chapter 2. Overview of the FESTOS expert survey

2.1 The survey structure

The survey consisted of three parts:

Part A: General attitudes towards future technology threats

Part B: Specific emerging technologies and their potential threats (33 technologies in 6 fields, as detailed in the following chapters)

For each technology the experts were asked about their level of knowledge in this particular technology and to assess:

- When will this technology be sufficiently mature to be used in practice?
- How easy will it be to use it for malicious purposes? (scale 1 to 5: 1=not easy at all, 5=very easy).
- How severe is the potential security threat posed by this technology? (scale 1 to 5: 1=very low severity, 5=very high severity).
- The likelihood that it will actually come to pose a security threat, in different time frames (scale of 1 to 5: 1= very unlikely, 5=very likely).
- To which societal spheres it will pose a security threat.

Part C: Personal comments

2.2 Respondents profile

FESTOS survey invitations were sent to several hundred experts from several target groups: academia and research institutes, industry and policy makers. About 280 experts responded to the survey (namely, answered at least part of the questions)*.

*In the first stage of the survey (as reported in the internal deliverable D2.2) the amount of respondents to several technologies in the fields of Biotechnology and Materials was rather low (less than 9 responses per specific technology). Therefore, in order to strengthen the validity of the survey results an additional round was carried out, focusing on those technologies. As a result the number of responses in these fields was significantly increased, in most cases reaching more than 20 responses per each technology.
Effort was made to include experts in the five technology fields (ICTs, Robotics, Nanotechnology, Biotechnology, Converging Technologies, and New Materials), as well as security experts. Most respondents are from Europe, but their countries are diverse (27% are from countries with less than 4% of respondents each). Relatively larger percentages of responses came from the countries of the FESTOS consortium (Poland, Germany, Israel and the UK).

Most respondents come from the academia or research institutes and are experts in specific technology fields. Many respondents have some experience in security (50% have high or medium experience). This is an important factor because security experience may grant a respondent the appropriate view of the potential "dark side" of the technologies.

![Figure 2.2 – Respondents Affiliation](image1.png)

![Figure 2.3 – Respondents' security experience](image2.png)
Figure 2.4 – Respondents’ areas of interest

The respondents were asked to choose their areas of interests in a multiple choice question, therefore the numbers above the bars in Fig.2.4 do not sum up to the total number of respondents. As can be seen the main area of interest is ICT, followed by Nanotechnology and New Materials. The “other” category includes respondents who added areas of interest that were not specifically listed in the questionnaire. (e.g. chemistry, psychology). These respondents, however, were able to answer part of the questions in bordering areas.

2.3 General attitudes towards future technology threats

Figure 2.5 – Awareness of the public

69% (155 out of 226) of the experts think that the public is rather badly informed about the potential dangers of new technologies. Only 9% think that the public is rather well informed. This may imply that the information about the potential dangers is currently neglected, and therefore such a badly informed society would be surprised by attacks using new technologies and would not react adequately.
The research and security experts assess the current regulations mainly as appropriate (54%). The general tendency shows that experts regard the regulations rather as too loose than too strict. This means that the government might underestimate the potential threats of new technologies.

**Figure 2.6 – Regulation assessment**

Are the potential dangers that might be posed by new technologies overestimated or underestimated?

Public: The experts assess the degree of awareness very differently. Only 19% of the experts think that the dangers are assessed adequately by the public, but also 19% believe that the public highly underestimate them. At the same time they think that in public the dangers are overestimated (21%) or very overestimated (9%).

**Figure 2.7 – Overestimation or underestimation of potential dangers**
Interestingly this does not correlate with the answers regarding the adequate information the public have about dangers which stem from new technologies. Experts seem not to believe in an adequate assessment by the public. This scepticism is the most noticeable finding of the five questions.

**Government:** Most of the experts assume that the government assesses the technical inherent threats adequately (40%) but 34% think that governments rather underestimate the danger and further 10% that governments very underestimate the danger.

**Colleagues:** The majority of respondents think that their colleagues assess the threats of new technologies in an adequate way (61%). Nobody thinks their colleagues overestimate the dangers seriously and only 2% believe that they very underestimate the dangers. It seems that more experts would rather underestimate the dangers than overestimate them. Hence, awareness of the dangers exists, but is not sufficient.
Chapter 3. Main Field: Information and Communication Technologies (ICT)

3.1 ICT – introductory overview

The field of information and communications technologies (ICT) is an extremely broad one, as it incorporates all technologies for the production, processing and communication of information. Therefore, developments in areas such as computing, telecommunications, information storage and retrieval, and others, are all pertinent here. The digital universe (information created, captured or replicated in digital form) is growing at a very fast pace. In 2007 it amounted to 281 exabytes (billion gigabytes), and it is expected to reach 1,800 exabytes in 2011\(^1\).

\*\*\*\*\*\*\*\*\*\*\*

A relatively large part of this universe, including personal digital information (or “digital shadow”) that is created by people or organizations (in their everyday activities, and in many cases unintentionally), may be used (or abused) for different purposes without the specific authorization of the individual. The digital trails (shadow) that each of us leaves is getting richer as ICT-related technologies make inroads into our life.

\*\*\*\*\*\*\*\*\*\*\*

In the future, new Internet uses, such as massive multi-party applications, will bring new threats. By the year 2020, the Internet will probably connect 500 million machines, 3 billion people, and 1 trillion objects. There will be huge flows of multimedia content and virtual distribution services, which will make traceability difficult. Through multitudes of sensors and actuators, the virtual and the physical worlds will become connected, as the visions of "Ambient Intelligence" (AmI) and the "Internet of Things" (IoT) become reality. The question will be how to defend critical infrastructures in this case. Another critical issue is security for mobile devices of persons, groups and swarms of things. Major threats could emanate from illicit computer programs when computers offer massive power for everyone and the possibility to disturb the distributed physical worlds.

Technologies in general, and in particular ICTs, increasingly dominate both the economy and society. This involves also new risks and threats. Some foresight experts foresee that “ultimately, speculation may prove correct that we are approaching the ‘Singularity’s event horizon’. At that time, our artifacts will be so intelligent that they can design themselves, and we will not understand how they work [...] The Internet, private networks, and a host of other technologies are quickly weaving the planet into a single, massively complex ‘infosphere’. These nearly infinite connections cannot be severed without overwhelming damage to companies and even to national economies. Yet, they represent unprecedented vulnerabilities to espionage and covert attack.”

It may sound fantastic, but a recent study commissioned by the International Commission on Nuclear Non-proliferation and Disarmament (ICNND) suggests that under the right circumstances, terrorists could break into computer systems and launch an attack on a nuclear state – triggering a catastrophic chain of events that would have a global impact. According to this study, in the current inadequate level of protection, a well-coordinated cyberwar could quickly elevate to nuclear levels. In fact, says the study, "this may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb themselves".

A number of different kinds of threats are suggested by the items that are described in this chapter. One kind of threat involves exposing information that people deposit in online places such as Facebook and Twitter (or their future generations), or the aggregation of location-based information collected anonymously by cellular providers. At the simplest level, information of a sensitive nature may be posted and then discovered or revealed and put to maleficent use, or a terrorist might be able to see where crowds are gathering in real time. More complex variations of threats in this regard refer to the possibilities of de-anonymising social network data and thus inferring information about people. This information may be of strategic value to someone wishing to cause harm (it could be used in an attempt at blackmail, or it could provide operationally useful information). There is concern that as the internet grows to incorporate objects that the information thereby created may also be

---


misused, that identity theft may become more prevalent, and that new ways of invading privacy may emerge.

Another kind of threat involves the use of ICTs to make people or machines do things (or, in the case of humans, also think things) from afar. Various kinds of brain-machine interfaces might be abused to direct the actions of objects through the power of thought, and brain-to-brain interfaces might offer the possibility of controlling the actions of another human being, using him/her as a kind of remotely controlled robot.

The convergence of a number of technologies within a single platform – such as the (next generation) smartphone – may also be considered a kind of threat. The integration of GPS, a compass, a camera, possibly additional sensors, and a broadband Internet connection in a single, small device is enabling the emergence of Augmented Reality, whereby information is superimposed on the image captured by the device’s camera. While not necessarily giving rise to an entirely new kind of threat (at the moment), it is suggested that this may improve the planning and operational capabilities of those wishing to cause harm.

A further type of quite general threat relates to society’s increasing dependence on technology for everyday tasks. The more dependent on technologies we become, the more disruption that tampering with those technologies can cause. For instance, developers are working on traffic management systems, which are aimed at preventing accidents by having cars “talk” with one another and a central control system. Such a system could be tampered with in a way that might cause city-wide disruption in the best case, or fatal traffic accidents in the worst case.

In the following pages we describe several selected ICTs with the assessment of their potential threats based on the FESTOS expert survey.

For completeness, we mention here ICTs that were described in D2.1 but were not included in the expert survey:

- SIGINT with COTS hardware;
- Intelligent Transport Systems and Crash Avoiders;
- Location-based systems: Locating the crowds;
- Emergency Personnel Tracking System;
- De-anonymising social networks;
- Capturing of secret information from computers through "side channels";
- Galvanic Vestibular Stimulation (GVS);
- Augmented Reality;
- Holographic 3DTV;
- Controlling the Weather;
- Sense-through-the-wall technology;
- Universal Translation;
- Virtual Reality;
- Computer Hacking and Cyberwarfare;
- Non Nuclear EMP Technologies;
- Artificial Neural Networks (ANN);
- Optical Computers/Optical Super Computing;
- Reflective/Affective Computing;
- Tracking users behavior by cellphone monitoring of sounds;
- Terahertz Detection;
- Quantum computing;
- Networked gaming;
3.2 Selected ICTs and evaluation of associated potential threats

1. Internet of Things (IoT), Ambient Intelligence (AmI), Ubiquitous Computing

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**

Internet of Things (IoT) refers to the “idea of things, especially to everyday objects, that are readable, recognizable, locatable, addressable, and/or controllable via the Internet—whether via RFID, wireless LAN, wide-area network, or other means”. Everyday objects may include food items, home appliances, clothing, components, commodities, and many others. Through communications systems, humans and objects may be connected, but also objects may connect to other objects, forming sensor networks or networks of machines (machine-to-machine). IoT involves the use of tags, devices or sensors that will need to be uniquely identified by a single numbering system, such as IPv6, so that every object is addressable.

IoT is related to the (broader) concept or vision of Ambient Intelligence (AmI) where people are surrounded by various interconnected devices, unobtrusively embedded in their surroundings and easily accessed via intelligent intuitive interfaces. This intelligent environment is expected to be capable of recognising and responding to the presence of different individuals in a seamless and often even invisible way. AmI is a vision of total integration of ICTs to the environment, where the ubiquitous computers “disappear”, so that from the point of view of the user it is absolutely unimportant what are the technologies or applications he/she is interacting with. Another closely related concept is Ubiquitous Computing (Ubicomp), which is considered the emerging “third wave” in computing. The first were mainframes, each shared by lots of people. Now we are in the personal computing era, person and machine staring uneasily at each other across the desktop. Next comes ubiquitous computing, when technology recedes into the background of our lives. Ubicomp is a post-desktop model of human-computer interaction in which information processing is thoroughly integrated into everyday objects and activities, as intelligent objects are replacing traditional PCs and are communicating by means of mobile ad-hoc networks.

Several technology enablers can be mentioned with regards to the future of IoT:

- **Energy:** Low-power devices, energy harvesters, new technologies for energy storage, generation, and transition.
- **Intelligence:** Context awareness, inter-machine communication, integration of memory and processing power, affordable security, optimal power consumption management.
- **Communication:** Multi frequency band antennas, on-chip antennas, modulation schemes.
- **Integration:** Packaging into products (textiles), System-in-Package (SIP).
- **Interoperability:** Tags must integrate different communication standards and protocols, different frequencies.
- **Standards:** Unique addressing has 2 standards – Ubiquitous ID and EPC Electronic Product Code) Global. Global, energy efficient communication standards that are security and privacy centered and are using compatible or identical protocols at different frequencies.

**Potential threat indications:**

The vision of massively interconnected systems of computers and sensors embedded everywhere, combined with intelligent collection and processing of private information, should naturally raise concerns.
A recent book summarized the EC FP6 project SWAMI (Safeguards in a World of Ambient Intelligence), and described in detail several "dark scenarios" related to AmI. These scenarios deal with several critical issues that need to be addressed for successful deployment of AmI. These vulnerabilities and risks include issues of privacy, security, trust, identity (and identity theft), loss of control, dependency, exclusion and digital divide, victimization, surveillance, spamming and malicious attacks.

For example, with regard to RFID tags used in products, one of the dark scenarios describes how criminals (burglars) might use RFID readers to select potential victims by obtaining information about purchased expensive items.

According to the report TAUCIS, written of behalf of the Federal Ministry of Education and Research (Germany), the security risks of Ubiquitous Computing are first of all related to information privacy/data privacy. This means the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. Identifiable information may be easily collected and stored. This technology in relation to wireless communication (blue-tooth, Wlan, infra-red etc.; possibly also related to RFIDs) means that privacy vs. control of the individual becomes a general issue of the open, democratic society. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources. Possible examples are related to healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, residence and geographic record etc.

Sources for technology description:
ITU INTERNET REPORTS 2005: THE INTERNET OF THINGS
Ambient Intelligence Forum 2009:
www.confabb.com/conferences/82321-ambient-intelligence-forum-2009

Sources for threat indication:
SWAMI Project: http://swami.jrc.es

Sources for relevant Foresight:
Science and Technology Foresight Survey: Delphi Analysis. Science and Technology Foresight Center, National Institute of Science and Technology Policy (NISTEP), Japan, May 2005 (NISTEP report No. 97)
www.dni.gov/nic/confreports_disruptive_tech.html
Description of this technology in the FESTOS expert survey:
The Internet of Things (IoT) means a network of many everyday objects (food items, home appliances, clothing, etc), as well as various sensors, that will be addressable and controllable via the Internet. IoT is related to the vision of Ambient Intelligence (AmI) where people are surrounded by various interconnected devices, unobtrusively embedded in their surroundings and easily accessed via intuitive interfaces. Such intelligent environment is expected to seamlessly respond to the presence and needs of individuals. Closely related concept is Ubiquitous Computing (Ubicomp), the emerging “third wave” in computing when computers are everywhere but they recede into the background and become "invisible".

(Potential threat: Will these technologies offer new opportunities for hacking, identity theft, disruption, and other malicious activities? Experts have warned that the security risks of Ubiquitous Computing are first of all related to information privacy)

FESTOS experts survey results:

When will this technology be sufficiently mature to be used in practice? 2018
How easy will it be to use this technology for malicious purposes that might pose security threats? easy (3.61)
How severe is the potential security threat posed by this technology? medium severity (3.49)

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>29%</td>
<td>24%</td>
<td>93%</td>
<td>80%</td>
<td>22%</td>
<td>66%</td>
</tr>
</tbody>
</table>

Interpretation:
The experts' opinion is that the likelihood of the threat will increase with time with slight decrease in the long range. The most threatened societal spheres are people and infrastructures, followed by economy. Other spheres are expected to be much less threatened. However, it should be noted that the threat to the values sphere is not negligible and should be considered.
2. Smart Mobile telephone technologies mash-ups

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
Mobile telephones have long ceased to be mere telephones. Today they come equipped with (stills and video) cameras, GPS, Internet connectivity, and more. As these capabilities are “mashed up” (i.e., brought together in new combinations, and in tandem with new Internet-based services, such as Twitter), they turn the cell phone into an extremely versatile communications device. Other Internet-based services such as Google maps can be combined. Google’s “Street View” is already easily downloadable to iPhone. Its future version may be especially adapted to mobile phones, including “Augmented Reality” (AR) features. For example, novel AR capabilities are demonstrated in a video: [www.physorg.com/news166186470.html](http://www.physorg.com/news166186470.html)

**Potential threat indications:**
A report published by the 304th Military Intelligence Battalion of the US Army mentions three possible maleficent uses of Twitter (accessed through a mobile phone):

1) for communication between terrorists
2) Terrorist B using Terrorist A’s tweets to determine the optimal time and place to remotely detonate A’s explosive vest
3) A spy joining a US soldier’s group of Twitter followers, then using the information gathered to somehow target the soldier

It might be suggested that it is unclear why text messaging (SMS) would not be preferable to Twitter, which is an open and public service. However, there is no doubt that Twitter can be an extremely powerful tool for organising crowds of people, as shown by the demonstrations in Iran of June 2009.

Mobile telephones also enable Open Source Intelligence (OSINT) to be carried out discretely and without any special equipment. A mobile phone with a video camera and a GPS device would enable a terrorist to collect location-based video imagery of a possible target area. Combination with Google maps, Street View, and their future enhanced versions such as advanced Augmented Reality features may obviously be very useful for planning and executing terrorist actions.

**Sources for technology description and for threat indications:**
Document by the 304th Military Intelligence Battalion of the US Army: “Sample Overview: al Qaida-Like Mobile Discussions & Potential Creative Uses”:
[www.fas.org/irp/eprint/mobile.pdf](http://www.fas.org/irp/eprint/mobile.pdf)

NOKIA’s research on Augmented Reality:
[http://research.nokia.com/research/labs/teams/visual_computing_and_user_interfaces](http://research.nokia.com/research/labs/teams/visual_computing_and_user_interfaces)


**Description of this technology in the FESTOS expert survey:**
New cellphones are equipped with video cameras, GPS, Internet connectivity, and more. As these capabilities are “mashed up” (i.e., brought together in new combinations, and in tandem with new Internet-based services), including emerging “Augmented Reality” (AR) features, they turn the cellphone into an extremely versatile communications and surveillance device.

(Potential threats: Mobile phones could enable Open Source Intelligence (OSINT) to be carried out discretely and without any special equipment. A mobile phone with a video camera and a GPS device would enable a terrorist to collect location-based video imagery of a possible target area.)
area. Could combinations with advanced Augmented Reality features be even more useful for planning and executing terrorist actions?)

**FESTOS experts survey results:**

<table>
<thead>
<tr>
<th>Question</th>
<th>2012</th>
<th>easy (3.69)</th>
<th>medium severity (3.49)</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td></td>
<td>easy (3.69)</td>
<td></td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td></td>
<td>medium severity (3.49)</td>
<td></td>
</tr>
</tbody>
</table>

The likelihood to pose a security threat (from 1 - very unlikely, to 5 - very likely)

<table>
<thead>
<tr>
<th>Societal spheres potentially threatened:</th>
<th>Economy</th>
<th>Environment</th>
<th>Infrastructures</th>
<th>People</th>
<th>Political systems</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>41%</td>
<td>13%</td>
<td>56%</td>
<td>94%</td>
<td>34%</td>
<td>31%</td>
</tr>
</tbody>
</table>

**Interpretation:**
The most threatened societal spheres are people and infrastructures, followed by the economy. However, it should be noted that the threats to political and value systems are also considerable.
### 3. Radio-frequency identification (RFID) and "RFID-dust"

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

**Description:**
Radio-frequency identification (RFID) “tags”, or microchips with antennas, allow the automatic identification and localisation of objects and persons using radio waves. Data collection and their registration become possible. RFID are active (with batteries) or passive (needing an outside signal/impulse). They are used in pricing, cashing and inventory of products (increasingly instead of barcodes), in biometric passports and credit cards, tickets to concerts and football games, marathon (to register start times of participants), transportation payments, libraries, schools and universities to register attendance, marking animals in agriculture... Widely spread RFID tags reaching the size of a few mm – the size of rice. Miniaturization of the RFID tags: Prototypes in the size of 0.05 mm × 0.05 mm × 5 µm (by Hitachi in February 2007) (90-Nanometer production process). This size implies the possibility for such chips to be embedded for example in ordinary sheets of paper, and heralds an era in which almost anything can be discreetly tagged and read by a scanner that it need not touch. In 2009 it was demonstrated that RFIDs can be glued to living ants.

Thus, RFIDs could soon be embedded in virtually everything bought, worn, driven, or read, enabling for example law enforcement and retailers to track consumer items, and consequently consumers, wherever they go. As such, RFIDs are considered as an important component of the future “Internet of Things” (see 1.). A seamless, global network of electronic scanners will be able to scan radio tags in a variety of public settings, identifying people and their tastes and instantly sending them customized ads or “live spam.” Smart homes could be built with sensors in the walls, floors, and appliances that will inventory possessions, record eating habits, monitor medicine cabinets, and report data to marketers. Much of the technology that would be used to monitor and track people already exists, and new, potentially intrusive uses are being patented and deployed.

The U.S. Justice Department says that with so many tags in objects, relaying information to databases could be linked to credit and bank cards, and almost no aspect of life would be safe from government and industry monitoring. By placing scanners in strategic areas, companies could search people's pockets, purses, luggage, and possibly their kitchens or bedrooms, at anytime, without being detected. "Once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile," the U.S. Government Accountability Office concluded in a 2005 report. As RFID goes mainstream and the range of readers increases, it will be "difficult to know who is gathering what data, who has access to it, what is being done with it, and who should be held responsible for it," Maxwell wrote in RFID Journal.

“…computer scientists in Massachusetts are working on software, aptly named Mementos, that could allow an RFID to perform computations that span many power losses and reboots. The software may enable the chip to compute cryptographic protocols, leading to more secure signals. And it might allow RFID chips to be more than just data collectors. They could analyze and possibly take action based on changes to the stress on a “smart” bridge or to trends in a person’s vital signs, for instance. Such computational RFIDs could play a role in the transformation of the Internet from a network of computers to a network of things--appliances, cars, smart clothes, and so on.”
Potential threat indications:
There will come a time when anyone from police to identity thieves to stalkers might scan locked car trunks, garages or home offices from a distance. RFIDs can be used to collect information to identify categories of people in order to target them. Potential threats are in the abuse of human microchip implants for medical use or mass surveillance. The control mechanisms offered by this technology are reaching from control of (all) citizens to the control of moves of potential terrorists. They offer friend-enemy identification for those able to control the receiver of the signal. They can identify those with (and consequently also those without) a RFID. This makes a security application of this technology interesting for all sides in conflicts, meaning both the authorities of a state, as also opponents (terrorists, criminals). Furthermore it can be a perfect tool to reduce privacy and democracy by (remote-) controlling the citizens. Miniaturization and/or rising efficiency, development of highly effective batteries and dropping of the price will make this technology increasingly attractive. They may be implanted into human beings in the name of “safe identification” at border controls etc.
Another related threat is the use of RFID readers by terrorists and criminals in order to steal identity or personal details of people, and even to physically harm people by interfering with implantable medical devices. In a research related to RFID security, K. Fu and his colleagues at the University of Massachusetts found that they could lift account numbers and expiration dates from smart cards - even cards inside a wallet - just by walking past them with a homemade scanner. In another research they built a radio transmitter that can stop the latest generations of ICD's that are connected to the internet, and can be programmed by doctors using radio communication. ICD is an implantable cardioverter defibrillator – a device implanted in some half-million people around the world every year. Stopping them will cause a heart-attack to the patient and possibly kill him (Source: Technology Review, Sept 2009)

Sources for technology description:
www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9054958
www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=privacy&articleId=9132581&taxonomyId=84&intsrc=kc_top
www.spectrum.ieee.org/computing/it/RFID-chips-gain-computing-skills
www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9054958

Sources for threat indication:
RFID Security & Privacy Lounge: www.avoine.net/rfid/
http://www.technologyreview.com/TR35/Profile.aspx?TRID=760&Cand=&pg=1

Sources for relevant Foresight:

Description of this technology in the FESTOS expert survey:
RFID tags allow the automatic identification and localisation of objects or persons using radio waves. They are used for pricing and inventory of products (replacing barcodes), in biometric documents, marking animals in agriculture, etc. Their miniaturization (to 0.05 mm or less) will enable embedding "RFID dust" in everything, including sheets of paper; hence almost anything can be discreetly tagged and read by a nearby scanner. RFIDs could be a component in the future "Internet of Things".
(Potential threat: Could criminals with RFID readers scan cars, houses or people in order to locate valuable goods and select potential victims? Or to collect useful information to identify categories of people in order to target them for malicious purposes? Could RFID readers be used by perpetrators in order to steal identity or smart card details, or even to physically harm people by interfering with implantable medical devices?)

FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2012</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (3.14)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (3.03)</td>
</tr>
</tbody>
</table>

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Societal sphere</th>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>31%</td>
<td>23%</td>
<td>91%</td>
<td>63%</td>
<td>9%</td>
<td>54%</td>
</tr>
</tbody>
</table>

**Interpretation:**
The overall likelihood of the threat doesn't change over time. The most threatened societal sphere is people. Infrastructure and the economy are likely to be threatened too. It should be noted that the threats to values and to political systems are also considerable.
## 4. Ultra-dense Data Storage

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
Computer data storage is advancing with rapid speed - as random access memory (RAM) and secondary storage in mass storage device (hard disks) and removable media (CDs, ZIP drives, DVDs, flash memory/USB sticks). Capacity, accessibility speed are growing, their size is smaller and smaller. In connection with nanotechnology data storage of 100,000 terabit per cm³ seem to be possible in future. (With such storage capacity an iPod could store MP3 music for 300,000 years without repeating a single song)

**Potential threat indications:**
Miniaturization, rising accessibility & mutability changes in future the quality of any data storage. Together with increasing mobility and internet anybody can have access to any data – opening up finally unlimited possibilities for the misuse of information. This is a chance for open societies, but includes possible risks concerning the wrong use of the information by the citizens.

**Sources for technology description:**
The International CIIP Handbook 2008/2009, full text at:
- [www.crn.ethz.ch/publications/crn_team/detail.cfm?id=92838](http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=92838)
- [www.heise.de/newsticker/Mini-Speicher-funktioniert-mit-Wasser--/meldung/72561](http://www.heise.de/newsticker/Mini-Speicher-funktioniert-mit-Wasser--/meldung/72561)

**Description of this technology in the FESTOS expert survey:**
Nanotechnology-enabled data storage of 100,000 terabit per cm³ is foreseen in the not-so-far future. With such capacity a device like iPod could store music for 300,000 years without repeating a single song. Together with mobile Internet connectivity, anybody will be able to have access to any information.

(Potential threat: As data storage is getting increasingly miniaturized and dense, huge amounts of information can be easily transported, stolen and transferred. Could this offer new opportunities for misuse, including large computer programmes to schedule attacks, etc.?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2018</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (3.05)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.72)</td>
</tr>
</tbody>
</table>

![Graph showing likelihood to pose a security threat](image)

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>6%</td>
<td>39%</td>
<td>78%</td>
<td>33%</td>
<td>17%</td>
<td>89%</td>
</tr>
</tbody>
</table>

**Interpretation:**

Threat likelihood is increasing with time. The most threatened societal spheres are economy and people. The potential threat to political systems is also significant.
### 5. Artificial Intelligence (AI)

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**

Thinking is nothing but the processing of information and data, it doesn’t need a human brain.‖

Intelligence is mind implemented by any patternable kind of matter." At least the purely cognitive part may be reproduced by computers, speed an amount of data is increasing, size decreasing. In 1996 for the first time a chess computer beat a world champion, Garry Kasparov. Such cognitive capacities, knowledge-based systems, and logic deduction are not the main challenge for AI research anymore. Relevant is the emotional part of intelligence: once the machine is able to read (or to understand) our feelings and facial expression – and can additionally convince us in the communication that we are dealing with a human being – we have to speak about a system/computer acting on the level of human intelligence. Practical relevance for this is found in robotics: in industrial production, in services, and households; fulfilling difficult or dangerous duties in repairing and e.g. in space.

**Some applications of AI:** (based on http://www-formal.stanford.edu/jmc/whatisai/node3.html):

- **Game playing** You can buy machines that can play master level chess for a few hundred dollars. There is some AI in them, but they play well against people mainly through brute force computation--looking at hundreds of thousands of positions. To beat a world champion by brute force and known reliable heuristics requires being able to look at 200 million positions per second.

- **Speech recognition** In the 1990s, computer speech recognition reached a practical level for limited purposes. Thus United Airlines has replaced its keyboard tree for flight information by a system using speech recognition of flight numbers and city names. It is quite convenient. On the other hand, while it is possible to instruct some computers using speech, most users have gone back to the keyboard and the mouse as still more convenient.

- **Understanding natural language** Just getting a sequence of words into a computer is not enough. Parsing sentences is not enough either. The computer has to be provided with an understanding of the domain the text is about, and this is presently possible only for very limited domains.

- **Computer vision** The world is composed of three-dimensional objects, but the inputs to the human eye and computers' TV cameras are two dimensional. Some useful programs can work solely in two dimensions, but full computer vision requires partial three-dimensional information that is not just a set of two-dimensional views. At present there are only limited ways of representing three-dimensional information directly, and they are not as good as what humans evidently use.

- **Expert systems** A "knowledge engineer" interviews experts in a certain domain and tries to embody their knowledge in a computer program for carrying out some task. How well this works depends on whether the intellectual mechanisms required for the task are within the present state of AI. When this turned out not to be so, there were many disappointing results. One of the first expert systems was MYCIN in 1974, which diagnosed bacterial infections of the blood and suggested treatments. It did better than medical students or practicing doctors, provided its limitations were observed. Namely, its ontology included bacteria, symptoms, and treatments and did not include patients, doctors, hospitals, death, recovery, and events occurring in time. Its interactions depended on a single patient being considered. Since the experts consulted by the knowledge engineers knew about patients, doctors, death, recovery, etc., it is clear that the knowledge engineers forced what the experts told them into a predetermined framework. In the present state of AI, this has to be true. The usefulness of current expert systems depends on their users having common sense.

- **Heuristic classification** One of the most feasible kinds of expert system given the present
knowledge of AI is to put some information in one of a fixed set of categories using several sources of information. An example is advising whether to accept a proposed credit card purchase. Information is available about the owner of the credit card, his record of payment and also about the item he is buying and about the establishment from which he is buying it (e.g., about whether there have been previous credit card frauds at this establishment).

**Potential threat indications:**
Important applications of AI are in the field of robotics (see threats in the Robotics chapter).

AI technology could also be used to conduct a sophisticated cyberwarfare,

Leading computer scientists, AI researchers and roboticists, who recently met in a conference organized by the Association for the Advancement of Artificial Intelligence at the Asilomar Conference Grounds on Monterey Bay in California, generally discounted the possibility of highly centralized super intelligences and the idea that intelligence might spring spontaneously from the Internet. But they agreed that robots that can kill autonomously are either already here or will be soon. They have been debating whether there should be limits on research that might lead to loss of human control over computer-based systems that carry a growing share of society’s workload. Their concern is that further advances could create profound social disruptions and even have dangerous consequences. As examples, they pointed to a number of technologies as diverse as experimental medical systems that interact with patients to simulate empathy, and computer worms and viruses that defy extermination (and could thus be said to have reached a “cockroach” stage of machine intelligence).

They focused particular attention on the specter that criminals could exploit artificial intelligence systems as soon as they were developed. What could a criminal do with a speech synthesis system that could masquerade as a human being? What happens if AI technology is used to mine personal information from smartphones?

**Sources for technology description:**
www.scinexx.de/dossier-42-1.html
www-formal.stanford.edu/jmc/whatisai

**Sources for threat indication:**

Scientists Worry About AI Threats: www.futurepundit.com/archives/006396.html

**Sources for relevant Foresight:**
Fraunhofer Institute research assumes that robotics to be used in households and services will be in mass production around 2015/2020. (see Steinmüller 2006, pp. 134ff.)

**Description of this technology in the FESTOS expert survey:**
“Intelligence is mind implemented by any patternable kind of matter.” Once the computer is able to "understand" human feelings and facial expression, we will refer to it as acting on the level of human intelligence. Artificial General Intelligence (AGI) is an emerging field aiming at the building of "thinking machines" – general-purpose systems with intelligence comparable to the human mind. Related term is "Strong AI".

While this was the original goal of AI, the mainstream AI research has turned into domain-dependent and problem-specific solutions. According to some extrapolations, desktop computers may have the processing power of human brains by the year 2029, and by 2045 AI could be able to "improve itself" at a rate that far exceeds anything conceivable in the past. Experts speculate a so-called Heterogeneous Self-Configurable Systems that will reach a level where they can "protect
themselves” from their human creators and can change their capabilities depending on new tasks. Related technologies are Intelligent Agents and Artificial Neural Networks (ANN). ANN are inspired by biological nervous systems, including the brain, with the ability to learn by examples. They involve a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems, in a different way from conventional computers.

(Potential threats: Could high level of machine intelligence open new opportunities for malicious use by criminals or terrorists e.g by interpreting facial expressions and human intentions? Or the design of "smart" malware for cyber-attacks? Or enabling malicious use of autonomous robots? Or, more speculatively, could it lead to machines that have intentions themselves?)

**FESTOS experts survey results:**

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (3.21)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (3.43)</td>
</tr>
</tbody>
</table>

![Likelihood to pose a security threat](chart.png)

**Societal spheres potentially threatened:**

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>31%</td>
<td>51%</td>
<td>82%</td>
<td>76%</td>
<td>38%</td>
<td>67%</td>
</tr>
</tbody>
</table>

**Interpretation:**
The threat likelihood is gradually increasing with time. All societal spheres are potentially threatened by the abuse of AI to a certain degree, with emphasis on people and infrastructures. The potential threat to political systems is significant.
6. Cloud Computing\textsuperscript{5,6}

**S&T Field:**

<table>
<thead>
<tr>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description (as presented in the expert survey):**

Cloud computing typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet. Providers deliver business applications online which are accessed from a web browser, while the software and data are stored on servers. Customers consume resources as a service and pay only for resources that they use. In January 2010 HP and Microsoft announced an agreement to invest $250 million over 3 years to significantly simplify technology environments via cloud computing.

**Potential threat indications (as presented in the expert survey):**

As businesses and individuals are handing storage and other tasks to outside providers, new opportunities arise for hacking and cyber-attacks.

**Sources for technology description:**

M. Armbrust et al, "A View of Cloud Computing: Clearing the clouds away from the true potential and obstacles posed by this computing capability" Communications of the ACM, April 2010, vol. 53, no. 4

**Sources for threat indication:**


**FESTOS experts survey results:**

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (3.29)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>high severity (3.53)</td>
</tr>
</tbody>
</table>

![Graph showing the likelihood to pose a security threat](image)

**Societal spheres potentially threatened:**

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>19%</td>
<td>32%</td>
<td>81%</td>
<td>65%</td>
<td>10%</td>
<td>90%</td>
</tr>
</tbody>
</table>

\textsuperscript{5} Cloud computing was not included in the preliminary scanning report D2.1

\textsuperscript{6} Cloud computing was defined by Gartner as one of the “top 10 strategic technologies” for 2011: [www.gartner.com/it/page.jsp?id=1454221](http://www.gartner.com/it/page.jsp?id=1454221)
**Interpretation:**
The threat likelihood is slightly decreasing in the long rang. The most threatened societal spheres are clearly the economy and people, followed by infrastructures. Political systems and values could be threatened to a lesser degree.

**ICT – overall assessment:**

The expert survey indicates that new developments in ICT may give rise to potential security threats in the near future, some of them with medium to high severity. The likelihood to actually pose a threat by the abuse of some technologies decreases with time, but remains effective also in the long range. All spheres of society are at risk, though people are usually mostly affected. The results also indicate that we should pay attention to the sensitivity of value systems to some of these threats.
Chapter 4. Main Field: Nanotechnologies

4.1 Nanotechnologies: Introductory Overview

Nanotechnologies deal with studying of phenomena at the nanoscale and the ability to manipulate matter at this scale, namely, at atomic, molecular and macromolecular levels (1 nanometer = $10^{-9}$ meter). At the nanoscale the borders between classical disciplines (e.g. physics, chemistry, biology) blur, and materials' properties (e.g. optical, magnetic, electronic, chemical, mechanical) are strongly influenced by any change in size of the material elements under consideration.

Advances in nanotechnology (or NT) have led, and are likely to continue to lead, to many beneficial applications in diverse areas. These include, for example, super-strong lightweight materials, highly efficient photovoltaic and fuel cells, the further miniaturization of electronic components, ultra-dense magnetic discs, targeted drug delivery systems, direct connection between electronics and biology (e.g. electronic devices connected to nerve cells), biocompatible implants, nano-electromechanical systems (NEMS), and many more. More futuristic NT visions include molecular assemblers and self-replicating nanobots. First generations of nanotech-based products are already in use and their markets are expected to grow very significantly in the coming decade. The EC expects that they will contribute to the European Union’s growth, competitiveness and sustainable development objectives and many of its policies, including public health, employment and occupational safety and health, information society, industry, innovation, environment, energy, transport, security and space.

The late Nobel Laureate Richard Smalley, testifying before the US Congress in a hearing on nanotechnology on June 22,1999, declared that "The impact of nanotechnology on health, wealth, and lives of people will be at least the equivalent of the combined influences of microelectronics, medical imaging, computer-aided engineering, and man-made polymers developed in this (the 20th) century."

In assessing the future of nanotechnology some experts have tried to categorize the types of research being conducted and/or the types of possible applications. For example, a straightforward categorization has been employed by James Tour based on work in his Rice University laboratory. He categorizes nanotechnologies as passive, active or hybrid (i.e. intermediate between active and passive). Tour estimates the time it will take to commercialize each of these types as 0–5 years for passive nanotechnologies, 15–50 years or more for active nanotechnologies and 7–12 years for hybrids. According to Tour, almost all the current applications of nano are passive, and most involve adding a nanomaterial to an ordinary material as a way of improving performance. For example, adding carbon nanotubes to rubber can greatly increase its toughness without reducing flexibility. Passive nanotechnology

---

7 Nanotechnology research portal of the European Commission: [http://ec.europa.eu/nanotechnology/index_en.html](http://ec.europa.eu/nanotechnology/index_en.html)

8 J. C. Davies, "Oversight of Next Generation Nanotechnology", Project on Emerging Nanotechnologies, PEN 18, Woodrow Wilson International Center for Scholars, April 2009
applications use nanomaterials to add functionality to products by nature of their physical and chemical form, rather than by how they respond to their environment.

James Tour defines an active nanotechnology as one where “the nano entity does something elaborate.” One example is a “nanocar,” a unique nano-engineered molecule that can be used to physically move atoms from one place to another, and has a potential to be used in future “nano robots” and other “nano machines”. Mimicking biological processes by using artificial molecules like the “nanocars” may enable the construction of sophisticated new materials and products as diverse as medicines (including advanced drug-delivery devices), new electronic devices and building materials. It is highly likely that the next-generation of nanotechnologies will strive to imitate nature by designing systems and devices that construct things “bottom up”, (i.e. atom by atom and molecule by molecule), rather than “top down” as in current manufacturing and miniaturization processes. This could be done by self-assembly, molecular construction or a combination of the two. Novel nanodevices such as the “nanocar” could be used as a basis for molecular construction. Practical applications of bottom-up construction are endless and open to imagination.

![Molecular “nanocar”](https://www.jmtour.com/?page_id=33)

Fig. 4.1 Molecular “nanocar” (Source: J. Tour lab, Rice University)

M. C. Roco, a key individual behind the US national nanotechnology initiative (NNI), elaborated a more detailed typology of nanotechnologies consisting of four generations: passive nanostructures, active nanostructures, “systems of nanosystems” and molecular nanosystems. Roco’s fourth generation nanotechnology, the most visionary one, “will bring heterogeneous molecular nanosystems where each molecule in the nanosystem has a specific structure and plays a different role”. It will include nanoscale machines and an interface between humans and machines at the tissue and nervous system levels.

---

9 Ibid.
10 [www.jmtour.com/?page_id=33](https://www.jmtour.com/?page_id=33)
As such, it is rather similar to the ideas of Eric Drexler, the famous “nano visionary” whose speculative future visions from the mid 80’s were dismissed by some people as unrealistic “science fiction”.

It is now widely accepted by experts that an important trend of future nanotechnology will be its merging with other technologies and the subsequent emergence of complex and innovative hybrid or converging technologies. In this scenario, the convergence of nanotechnology, biotechnology and information and cognitive sciences (NBIC) will become the defining technological characteristic of the 21st century (this trend is described in Chapter 6: Converging Technologies).

The huge beneficial potential of NT is accompanied by a large potential for various safety risks and hazards and also of intentional abuse. Numerous studies have identified NT related risks, many of them associated with current industrial research and in particular with defence R&D. Naturally, if these technologies become more easily accessible and affordable, the risk potential may grow.

Examples of existing and potential threats include health and environmental risks of various nanoparticles, dangerous result of nano-enabled genetic manipulations, explosives and propellants enhanced by nanoscale additives, NT-enabled active camouflage, networks of ultra-miniature tracking sensors (“smart dust”), and even nanotechnology-based “doomsday weapons” based on futuristic nano-assemblers or self-replicating nano-robots.

In the following pages we describe several selected nanotechnologies, along with the assessment of their potential threats based on the FESTOS expert survey.

For completeness, we mention here nanotechnology topics that were described in D2.1 but not included in the expert survey: "Nanotechnologies – general" (this was split into several technologies in the survey, such as molecular manufacturing and molecular nanosensors), "self erasing colour images", and "swarms of nano-machines controlled by 'chemical brain'".
4.2 Selected Nanotechnologies and evaluation of associated potential threats

1. Self-replicating Nanoassemblers

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
Nanoassemblers, and in particular "universal nanoassemblers" are an important potential outcome of the vision of molecular nanotechnology, leading to an industrial revolution (molecular manufacturing). According to this vision, with the appropriate program, the assemblers could self-replicate exponentially, and they would autonomously assemble and manufacture almost any desired product "bottom up", molecule by molecule.

Self-replicating nano-assemblers or nano-robots as an outcome of advanced molecular nanotechnology, and related "dark side" scenarios, have been described in the Science Fiction literature and in several speculative articles, and have been often dismissed by scientists as unrealistic. The idea was introduced for the first time in the influential book "Engines of Creation" (1986) by the nanotech visionary Eric Drexler (sometimes called "the father of nanotechnology"). He also speculated about the so-called "Grey Goo Scenario": uncontrolled "runaway self-assembling nanoreplicators" that cause damage, kill and destroy the world.

The "Grey Goo Scenario" was used by Michael Crichton in his popular Science Fiction book "Prey", where it was suggested that a simple experiment could quickly evolve into a terrifying swarm of nano-robots capable of destroying everything. In the book (described by the author as a serious warning based on actual developments in nanotechnology, robotics and AI), the fictional scientists were reckless and didn't follow proper guidelines.

In 2004, Eric Drexler wrote in the Institute of Physics journal Nanotechnology that self-replicating machines are not vital for large-scale molecular manufacture, and that nanotechnology-based fabrication can be non-biological and inherently safe. He admitted that talk of "grey goo" (which he first cautioned against in his book Engines of Creation in 1986) “cannot happen by accident”, and that it has spurred fears that have long hampered rational public debate about nanotechnology: "Runaway replicators, while theoretically possible according to the laws of physics, cannot be built with today’s nanotechnology toolset,” they "aren't necessary for molecular nanotechnology, and aren't part of current development plans." However, one may envision that major advances in molecular nanotechnology may lead to future toolsets and future development plans that in turn will enable such devices.

**Potential threat indications:**
Even if uncontrolled "runaway replication" is highly unlikely, or can be prevented by appropriate safeguards, one cannot preclude intentional malicious design of such devices, for evil purposes. According to J. Altman, "Molecular Nanotechnology could develop into very scary scenarios, not only if used for weapons. Despite its potential importance, molecular NT and related ideas have been practically ignored by the mainstream-science community.... Sidestepping universal molecular assemblers and self-replicating nano-robots, many of the other molecular-NT-related ideas were presented as realistic possibilities at the US converging-technologies workshop of 2001."

Eric Klein, the founder of "Lifeboat Foundation", warns: "Our biggest concern is that a lone individual will unleash a nanotechnology-based doomsday weapon with the same ease as those who send anthrax through the mail. All this individual would have to do is modify technologies that will be easily available to thousands if not millions of individuals by 2020".
Sources for technology description:
E. Drexler, "Engines of Creation", 1986
J. Altmann, "Nanotechnology: The Next Industrial Revolution", in "Nanotechnology and Preventive Arms Control"
www.bundesstiftung-friedensforschung.de/pdf-docs/berichtaltmann.pdf

Sources for threat indication:
Interview with Eric Klein:
www.themichiganjournal.com/home/index.cfm?event=displayArticlePrinterFriendly&uStory_id=62032a4d-1c02-4dfc-a121-1b921e862038
J. Altmann, "Nanotechnology and Preventive Arms Control"
www.bundesstiftung-friedensforschung.de/pdf-docs/berichtaltmann.pdf

Description of this technology in the FESTOS expert survey:
Nanoassemblers, envisioned as a future tool for molecular manufacturing, could self-replicate exponentially. Uncontrolled "runaway replication" has been described in fictional/speculative scenarios of futuristic nanotechnology.

(Potential threats: Even if uncontrolled "runaway replication" is highly unlikely, or can be prevented by appropriate safeguards, could this technology enable intentional design of such devices for malicious purposes?)

FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2030</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (2.75)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.92)</td>
</tr>
</tbody>
</table>

likelihood to pose a security threat
(from 1 - very unlikely, to 5 - very likely)

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>18%</td>
<td>73%</td>
<td>55%</td>
<td>82%</td>
<td>55%</td>
</tr>
</tbody>
</table>

Interpretation:
The likelihood of the threat is increasing with time. The most threatened societal spheres are people and the environment, followed by infrastructures and the economy.
### 2. Energetic nanomaterials

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**

Various nanoparticles can improve the reactivity and other properties of energetic materials. For example, they enable better mixing of fuels and oxidizers, resulting in much faster reaction than conventional materials. By varying the composition of composite explosives that contain nanoparticles it is possible to control the energy density. Various nano-sized metal particles have higher heats of combustion and faster energy release rates than the same metals in usual form. For example, an aluminum can is perfectly safe, but nano-sized aluminum can be highly explosive. Because of their capability to enhance performance, various metals have been introduced in solid propellant formulations, gel propellants, and solid fuels. Numerous techniques have been developed for synthesizing nano-particles of different sizes and shapes. In general, using energetic nano-sized particles as a new design parameter, propulsion performance of future propellants and fuels can be greatly enhanced.

According to a publication of the US DOE, a new trend in high explosives (HE) formulations is to add metal nanoparticles to the mix. Metals make a HE reaction hotter but reduce its pressure. Nanoparticles react much more easily than large metal particles, thanks to their much larger surface-to-volume ratio. In the right proportion, metals can almost double the energy content of an explosive. Heavy metals such as tungsten, titanium, and zirconium can also be used to alter the energy delivery rate of a reaction.

Moreover, it has been suggested that entirely new molecules with high energy density, that are not easily accessible by traditional chemistry, will be created by using molecular nanotechnology methods. In their futuristic form, these methods could include molecular manufacturing means such as molecular assemblers.

**Potential threat indications:**

As mentioned above, making nanoparticles of usually safe and not harmful metals can result in dangerous substances. For example, nano-sized aluminium is highly explosive and can be used to make bombs. If such technologies become more accessible and affordable in the future, the potential threats are obvious: more lethal explosives, more efficient propellants (e.g. for home-made large-range rockets), etc. Another issue to consider is the possibility to construct explosives which could be carried by traditional post systems.

**Sources for technology description:**


**Sources for threat indication:**


J.F. Davies, "Oversight of the Next Generation Nanotechnology", Project on Emerging Nanotechnologies, Woodrow Wilson International Center, PEN 18, April 2009
Description of this technology in the FESTOS expert survey:
Various nanoscale additives can improve the chemical reactivity and other properties of materials. For example, nano-sized aluminium can be highly explosive. Entirely new molecules with high energy density could be created by molecular nanotechnology methods.
(Potential threat: Could this enable new powerful propellants and explosives?)

FESTOS experts survey results:

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (3)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (3.33)</td>
</tr>
</tbody>
</table>

![Graph showing the likelihood to pose a security threat](image)

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>25%</td>
<td>92%</td>
<td>83%</td>
<td>58%</td>
<td>25%</td>
</tr>
</tbody>
</table>

Interpretation:
The likelihood that this technology will actually pose a threat is increasing with time. The most threatened societal spheres are people and infrastructure, followed by the environment. Other spheres are much less affected.
3. Tailored Nanoparticles

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**

"Scientists at the University of California at San Diego and the nearby Veterans Affairs Medical Healthcare System in La Jolla recently concluded that magnetic nanoparticles may be hazardous to your health. Experiments revealed that iron oxide particles less than 10 nanometers in diameter stunt the growth of nerve cells. Separate in vitro experiments at the National Institute of Standards and Technology (NIST) have also concluded that nanotubes shorter than 200 nanometers interfere with human lung cells. Both groups called for animal testing that would not only quantify the toxic effects of nanomaterials on living organisms but also characterize the most toxic types of nanomaterials. Currently the National Science Foundation (NSF) spends almost 10 times more on developing nanomaterials than on engineering to prevent their toxic effects. One group has found that iron oxide nanoparticles smaller than 10 nanometers in diameter can stunt the growth of nerve cells. Instead of responding to the natural chemical signals from nerves by extending neuritis that facilitate communications, nerve cells tend to go dormant in the presence of iron oxide nanoparticles, they found."

**Potential threat indications:**

According to an EC Workshop report (2004) nanoparticles can enter the body via the digestive tract by ingestion, via the respiratory tract by inhalation, and possibly via the skin through direct exposure. Once in the body, nanoparticles can translocate to organs or tissues of the body distant from the portal of entry. Such translocation is facilitated by their propensity to enter cells, to cross cell membranes, and to move along the axons and dendrites that connect neurons. Notably, under certain conditions, some particles can cross the blood/brain barrier, which opens therapeutic possibilities as well as radically novel health concerns.

Knowledge of the properties of nanoparticles and the technological capability to control these properties can be used to develop harmful and destructive nanoparticles. Nanoparticles can act as chemical agents (inducing biochemical reactions), and can also act mechanically in living organisms. Both aspects could pose a real threat.

**Sources for technology description:**

www.eetimes.com/showArticle.jhtml;jsessionid=5EOUEV31UKFRAQSNDLPSKHSCJUNN2JVN?articleID=199000914

**Sources for threat indication:**


**Description of this technology in the FESTOS expert survey:**

Various nanoparticles designed for use in commercial products can enter the body (by ingestion, inhalation or via the skin) and could be hazardous to health. For example, iron oxide particles less than 10 nanometers in diameter stunt the growth of nerve cells. Some particles can cross the blood/brain barrier.

(Potential threat: Could the capability of tailoring their properties be used to develop harmful nanoparticles?)
**FESTOS experts survey results:**

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2012</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (2.53)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.89)</td>
</tr>
</tbody>
</table>

![Graph showing likelihood to pose a security threat](image)

**Societal spheres potentially threatened:**

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>11%</td>
<td>0%</td>
<td>100%</td>
<td>21%</td>
<td>84%</td>
<td>16%</td>
</tr>
</tbody>
</table>

**Interpretation:**
The threat likelihood is relatively constant with time. The most threatened societal sphere is people, with the environment lagging a little behind.
### 4. Medical Nanorobots

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

**Description:**
According to imaginative nanotechnology visions, special nanorobots inserted in the human body will be one of the next steps in medical diagnostics and treatment. Nanomedicine can address many important medical problems by using nanoscale-structured materials and simple nanodevices, including nanorobots or engineered organisms. Some experts foresee that in the longer term (10–20 years from today), the earliest nanorobots may join the medical routines, giving physicians the most potent tools imaginable to conquer disease, ill-health, and aging.

A possible "shortcut" to bio-nanorobotics is to engineer natural nanosystems—biological viruses and bacteria—to create new, artificial biological devices.

"Imagine going to the doctor to get treatment for a persistent fever. Instead of giving you a pill or a shot, the doctor refers you to a special medical team which implants a tiny robot into your bloodstream. The robot detects the cause of your fever, travels to the appropriate system and provides a dose of medication directly to the infected area. Surprisingly, we're not that far off from seeing devices like this actually used in medical procedures. They're called nanorobots and engineering teams around the world are working to design robots that will eventually be used to treat everything from haemophilia to cancer."

As an example of practical experimental achievements that could be one of many avenues towards medical nanorobots it is worthwhile to mention the work of Montemagno and Bachand who modified a natural biomotor to incorporate nonbiological parts, creating the first artificial hybrid nanomotor. Using the tools of genetic engineering, they added metal-binding amino acid residues to ATPase, a ubiquitous enzyme whose moving part is a central protein shaft (or rotor, in electric-motor terms) that rotates in response to electrochemical reactions.

**Potential threat indications:**
The possibility that medical nanorobots could be hacked and instructed to harm should be considered, as well as the threat that future nanorobots could be built for destructive purposes as well as medicinal purposes.

Recent research shows that micro/nano robots could be inserted into the body by their incorporation in food or drinks. One may envision using such remotely controlled devices to control humans.

**Sources for technology description:**
http://electronics.howstuffworks.com/nanorobot.htm

**Description of this technology in the FESTOS expert survey:**
Nanorobots inserted in the human body could be one of the next steps in medical diagnostics and treatment, to conquer disease, ill-health, and aging. A possible "shortcut" to bio-nanorobotics is to engineer natural nanosystems (e.g. viruses and bacteria) to create new, artificial bio-devices. Future advances could include controlled swarms of molecular nanorobots, reacting faster than neurons.

(Potential threats: Could harmful nanorobots be inserted into the body by food or drinks? Could they be instructed to harm humans and/or to remotely control human actions?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2030</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>difficult (2.27)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.73)</td>
</tr>
</tbody>
</table>

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Societal spheres</th>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>18%</td>
<td>9%</td>
<td>100%</td>
<td>9%</td>
<td>46%</td>
<td>18%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood is clearly increasing with time. The most threatened societal sphere is people. Environment might be affected to lesser degree. There is some impact on values as well.
5. Molecular manufacturing

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

**Description (as presented in the expert survey):**
Assembling various desired products "bottom up", molecule by molecule, possibly in small "nanofactories".

**Potential threat indications (as presented in the expert survey):**
Could it be used to create new hazardous materials, or new types of weapons? According to the expert J. Altman, "Molecular Nanotechnology could develop into very scary scenarios, not only if used for weapons. Despite its potential importance, molecular NT and related ideas have been practically ignored by the mainstream-science community…"

**Sources for technology description:**

Advances in Atomic & Molecular Nanotechnology, in "Nanotechnology: The emerging cutting-edge technology", UN-APCTT Tech Monitor, pp.53-59, Sep-Oct 2002 Special Issue

**FESTOS experts survey results:**

<table>
<thead>
<tr>
<th></th>
<th>2023</th>
<th>somewhat difficult (2.5)</th>
<th>medium severity (2.5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Societal spheres potentially threatened:**

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>13%</td>
<td>25%</td>
<td>75%</td>
<td>38%</td>
<td>88%</td>
<td>50%</td>
</tr>
</tbody>
</table>

---

11 Molecular manufacturing was not included in the preliminary scanning report D2.1
Interpretation:
The threat likelihood is increasing with time. The most threatened societal spheres are the environment and then people. Impact is envisioned on the economy and infrastructure as well.

6. Molecular nanosensors

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Description (as presented in the expert survey):
These include physical, chemical and biological sensors, with molecular precision. Such sensors will be able to detect where a person have been by sampling environmental clues on clothes. Moreover, they could enable advanced nano-diagnostics, and could make people "molecularly naked".

Potential threat indications (as presented in the expert survey):
Could such personal information be abused by criminals? Or, looking from another angle, could this technology enable "molecular camouflage"?

Sources for technology description:
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1703495

Sources for threat indication:
www.nature.com/nnano/journal/v2/n4/full/nnano.2007.93.html

FESTOS experts survey results:
<table>
<thead>
<tr>
<th></th>
<th>2016 - 2020</th>
<th>2021 - 2025</th>
<th>2026 - 2035</th>
<th>After 2035</th>
</tr>
</thead>
<tbody>
<tr>
<td>likelihood to pose a security threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(from 1 - very unlikely, to 5 - very likely)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

When will this technology be sufficiently mature to be used in practice? 2018
How easy will it be to use this technology for malicious purposes that might pose security threats? difficult (2.08)
How severe is the potential security threat posed by this technology? low severity (1.85)

---

12 This technology was not included in the preliminary scanning report D2.1
Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>40%</td>
<td>100%</td>
<td>20%</td>
<td>30%</td>
<td>20%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood is increasing with time. The most threatened societal sphere is people. The threat to political systems is also considerable.

Nanotechnology: overall assessment

Potential new security threats are posed by various nanotechnologies both in the short and long range. While several nanotechnologies are maturing, using them for malicious purposes won't be easy, and most potential threats considered in the survey are expected to be of medium severity. All societal spheres are potentially threatened to a certain degree. People are usually most threatened, but also the environment and infrastructures might be very much affected by some technologies. The political systems and values also exhibit sensitivity in some cases. The likelihood that the technologies will actually pose security threats vary. While in some technologies the likelihood increases with time, in others it decreases in the long range – probably because the experts envision growing counter-measures availability.
Chapter 5. Main Field: Biotechnology

5.1 Biotechnology: Introductory Overview

Biological research includes a very broad spectrum of activities, including classical biotechnology, healthcare (genetics, clinical research and drug development), physiology, synthetic biology, and more. Modern genetic engineering is instrumental for the fast development rate of biological scientific research at the end of the 20th century, and is expected to remain so throughout the 21st century.

The current dominant application areas of biotechnological research include: medicine (health care), food production (agriculture, and food industry), and materials (e.g. biodegradable materials, biofuels, etc).

In healthcare research several areas have particular application opportunities:

- Pharmacogenomics/Pharmacogenetics – the study of relationships between human genetics and drugs action which will make possible developments of new drugs (personalized drugs), based on individual differences between people and their responses to drugs (ability to metabolize drug products).
- Gene therapy – a general approach of treating genetic disorders by delivering a 'working gene' for the missing protein at the appropriate expression locus in the body.
- Genetic diagnosis – a number of diagnostic technologies related to the detection and prediction of congenital and hereditary diseases, and possible remedies.
- Stem cells – "primordial cells" with the specific ability to differentiate into all other types of cells. The huge potential application areas are replacement of non functional (regenerative medicine), cancerous tissues and organs, with self, new tissues grown from personal stem cells.
- Telemedicine and ‘e-health’ - a set of enabling technologies, largely based on ICT, that help distance health care workers be more effective in their service.

Additionally, an increasing convergence between biotechnology, nano-technology, and cognition science is expected, with large application opportunities in the health sector (neuroscience, cardiovascular and metabolism illnesses treatments). In agriculture, modern biotechnological methods have been instrumental in the development of new genetically modified crop varieties with improved yields, reduced vulnerability to environmental stresses, and resistance to pesticides and herbicides. Biotechnology has also been applied in the production of novel non-food substances such as detergents, fatty agents from oilseed, biofuels, and in research programs carried on by the pharmaceutics industry\(^\text{13}\), in the field of drugs and vaccines production by genetically modified plants.

New advanced materials based on biological subparts such as self-assembling proteins and various biological nano-materials might be available. These new materials could be potentially very strong, light, long lasting or self disintegrate in the environment, and even display disruptive physical properties such as stealth (optical or other).

Artificial biological creatures and Synthetic Biology: Artificial biological self replicating agents such as artificial viruses with sensing properties (like DNA and proteins chips)

\(^\text{13}\) [www.pnas.org/cgi/content/full/104/26/10757]
could be used for remote sensing in medical and environmental applications. An exciting and promising development in this direction is the advent of Synthetic Biology. Synthetic Biology makes use of genetic (and other) materials from biological life forms to design and construct novel organisms. The main vision is to develop a dynamically expanding inventory of standard genomic parts and procedures that engineers can draw from to construct life forms with the desired functionalities, e.g. “manufacturing” vaccines, chemicals and energy (e.g. hydrogen, biofuels), coding information, or supplementing our immune systems. Potential applications of all the above technologies are foreseen in many areas of human activity such as medicine, environment, and also in military activities, and as such they have serious potential for abuse and threat. The creation or modification of biological organisms pose inherent risks of bio-error and hence threats of bio-terror. In particular, Synthetic Biology poses an obvious threat of “bio-hacking”. It could lead to cheaper and widely accessible tools to build bioweapons that would be available to terrorist organizations.

An illustrative example for the evolving bioterrorism threats posed by proliferation of commercial gene synthesis was an investigation of the newspaper “New Scientist” in 2005. The investigation showed that it was rather easy to order synthesised genes from biotech firms and get them by post. The firms didn’t check at all the identity and purposes of the orderer. Such genes could be used, with appropriate knowledge, to construct deadly pathogens. To cope with the potential threat of gene synthesis, in 2008 a European consortium of companies called the International Association of Synthetic Biology (IASB) initiated a formulation of a code of conduct that includes special gene-screening standards. At a recent meeting in San Francisco in August 2009, two of the leading companies — DNA2.0 of Menlo Park, California, and Geneart of Regensburg, Germany — announced that they had formulated a code of conduct that differs from the IASB recommendations. However, experts still worry that these activities are insufficient.

There is an increasing threat of wide proliferation of new genetic engineering technologies and equipment in many (non-military) biological laboratories, which could be used for malicious and illegal activities. Reproductive cloning raises well known ethical concerns – and also concerns about illegal activity. Even novel techniques developed for disease immunisation might be abused and applied for precisely the reverse effect.

---


15 P. Aldhous, “The Bioweapon is in the Post”, New Scientist news service, 9.10.2005

In the following pages we describe several selected biotechnologies, along with the assessment of their potential threats based on the FESTOS expert survey.

For completeness, we mention here biotechnology topics that were described in D2.1 but not included in the expert survey:

- Genetically Engineered biological warfare agents;
- Walking DNA motor;
- Chemical and biosensor systems for safeguards and environmental control;
- Bio-Hacking;
- Seeing a virus in three dimensions;
- Bio-attacks by using social network analysis;
- "Evolution Machine";
5.2 Selected biotechnologies and evaluation of associated potential threats

1. Synthetic Biology

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Description:

Unlike conventional biotechnology, in which modest genetic changes are induced in cells to serve certain industrial purposes, synthetic biology involves large-scale rewriting of genetic codes to create metabolic machines with singular purposes. "I see a cell as a chassis and power supply for the artificial systems we are putting together," says Prof. T. Knight of MIT, who likes to compare the state of cell biology today to that of mechanical engineering in 1864, when the US began to standardize thread sizes for nuts and bolts, an advance that allowed the construction of complex devices from simple, interchangeable parts. The vision of scientists like Knight is to make turn synthetic biology into a kind of engineering discipline, with similarly standardized parts – a collection of interchangeable genetic components that the MIT researchers call BioBricks.

Hence, synthetic biology means in vitro building of natural biological agents and new artificial agents combinations, from basic building blocks of life/ "biobricks" (nucleic acids, peptides, proteins, and intracellular organelles), that will be available in the future in biological equivalents of hardware stores (as the MIT's registry used in the "International Genetically Engineered Machine" competition at the Massachusetts Institute of Technology). According to the BioBricks Foundation (BBF), a not-for-profit organization founded by engineers and scientists from MIT, Harvard, and UCSF, by using such standard biological parts a biological engineer can already, to some extent, "program living organisms in the same way a computer scientist can program a computer" (see references below).

As a step toward programming cells as precisely as computers, by linking a series of protein switches, synbio researchers at MIT constructed "cell-level counters" that could eventually be used to coordinate complex sets of genetic instructions running on biomolecular machines, from disease-hunting cells to intracellular computing networks. Using computer models to explore molecular manufacturing possibilities and enzyme tweezers to assemble their designs, synthetic biologists seek not merely to tweak a gene or two, but to "hack and remix" cells, even build them from scratch. (Scientists have already succeeded to built certain viruses “from scratch”).

The company Synthetic Genomics in Rockville, founded and headed by Dr. Craig Venter, plans to design and built special purpose microbes to produce fuels. Venter's company already built the first fully artificial chromosomes, and one of its visions is to develop "an operating system for biologically-based software." In 2007, Venter researchers published a paper describing a genome transplant, in which a genome from one type of bacteria was transferred to a closely related one, giving the host the characteristics of its donor. Then, in 2009, the researchers created a synthetic genome by stitching together pieces of synthesized DNA.

Recently (July 2009) researchers at the J. Craig Venter Institute transplanted a bacterial genome into yeast, altered it, and then transplanted it back into a hollowed bacterial shell, producing a viable new microbe. The researchers expect that this technique will provide a way to more easily genetically engineer organisms not commonly studied in the lab and could aid in
the expanding effort to create microbes that can produce fuels or clean up toxic chemicals. The new technology emerged from the Venter Institute's quest to create life from scratch--generating a synthetic genome and then using it to control, or reboot, a recipient cell.

**Potential threat indications:**

Such technologies in wrong hands could facilitate production of classic and new biological warfare agents, without special need of LARGE biotech production facilities. Basic feasibility already shown in scientific circles debates, as those brought up by the "International Genetically Engineered Machine" competition at MIT. The conjunction between genetic engineering and synthetic biology may pose a real threat in the future because of the possibility of new gene constitutions.

It is imaginable that the above-mentioned "Cell level Counters" could produce cell-destroying proteins. Perhaps these could be used as built-in "kill switches" for engineered organisms released into the environment or human bodies.

"Ultimately synthetic biology means cheaper and widely accessible tools to build bioweapons, virulent pathogens and artificial organisms that could pose grave threats to people and the planet," concluded a recent report by the Ottawa-based ETC Group, one of the advocacy groups that want a ban on releasing synthetic organisms pending wider societal debate and regulation. "The danger is not just bio-terror but bio-error," the report says.

To cope with the potential threat of gene synthesis, since 2008 a European consortium of companies called the International Association of Synthetic Biology (IASB) has been drawing up a code of conduct that includes gene-screening standards. At a recent meeting in San Francisco in August 2009, two of the leading companies — DNA2.0 of Menlo Park, California, and Geneart of Regensburg, Germany — announced that they had formulated a code of conduct that differs from the IASB recommendations. However, experts still worry that these activities are insufficient. The two firms are now merging their databases of genes of concern. This raises concerns, because it is difficult to translate the list of select-agent organisms into lists of dangerous genes and no one believes that such lists will catch every dangerous gene. For instance, they might not identify genes from harmless organisms that had been modified in some new and deadly way.

**Sources for technology description:**

- www.guardian.co.uk/science/2009/apr/14/genetically-engineered-machine-competition
- The Biobricks Foundation: http://openwetware.org/wiki/The_BioBricks_Foundation
- www.wired.com/wiredscience/2009/05/cellcounters/

**Sources for threat indication:**


**Description of this technology in the FESTOS expert survey:**

In vitro building of natural biological agents and new artificial agents combinations, from basic building blocks (interchangeable biological components called "biobricks"). Using such standard parts will enable bio-engineers "program living organisms in the same way a computer scientist can program a computer". The vision includes generating a synthetic genome and then using it to control, or reboot, a recipient cell. Synthetic biology goes beyond
classic genetic engineering as it attempts to engineer living systems to perform new functions not found in nature. There are even ideas to create forms of life with an altered biochemical basis, e. g. with PNA (Peptide Nucleic Acid).

(Potential threat: Could this lead to cheaper and widely accessible tools to build bioweapons, virulent pathogens, dangerous organisms, etc., especially as “recipes” may one day be readily downloadable from the Internet?)

FESTOS experts survey results:

| When will this technology be sufficiently mature to be used in practice? | 2018 |
| How easy will it be to use this technology for malicious purposes that might pose security threats? | somewhat difficult (3.16) |
| How severe is the potential security threat posed by this technology? | medium severity (3.4) |

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>31%</td>
<td>23%</td>
<td>100%</td>
<td>15%</td>
<td>69%</td>
<td>23%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases with time. The most threatened societal spheres are people and the environment. Attention to the impact on values should be paid.
### 2. DNA-protein interaction

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
DNA may contain the blueprint for life but it takes proteins to read the plan and build an organism. The mechanism of this vital biological process has remained a mystery but now researchers are proposing a physical model wherein individual proteins can "slide" freely along DNA strands in search of target sequences.

The team envisions the process involving ‘DNA-binding proteins’ swarming around the iconic double helix on account of electric attraction — proteins have a net positive charge and DNA has a net negative charge. These proteins can then bind to exactly the right section of the long, coiling DNA so they can carry out vital functions such as copying genetic information and translating genes into templates for protein production. This complex biological set-up was reduced into more general physical shapes.

Using Monte Carlo computer simulations, DNA was modelled as a long cylinder, and the protein as one of four solids: a sphere; a cylinder; or a cube or cylinder with a groove carved in one side.

**Potential threat indications:**
The technology can pose threats because of ability to construct new harmful organisms. Specific threat is sophisticated simulation or modelling techniques allowing the design of new organisms that would be available for terrorist or crime groups.

**Sources for technology description:**

**Description of this technology in the FESTOS expert survey:**
Using computer simulations, researchers envision a process involving ‘DNA-binding proteins’ that bind to exactly the right section of the DNA so they can carry out vital functions such as copying genetic information and translating genes into templates for protein production. This in one of possible ways to control DNA expression.

(Potential threat: Could such knowledge could enable the construction of harmful biological materials/organisms?)
FESTOS experts survey results:

| When will this technology be sufficiently mature to be used in practice? | 2023 |
| How easy will it be to use this technology for malicious purposes that might pose security threats? | somewhat difficult (2.58) |
| How severe is the potential security threat posed by this technology? | medium severity (2.58) |

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>25%</td>
<td>8%</td>
<td>100%</td>
<td>8%</td>
<td>75%</td>
<td>17%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases slightly in the long range. People are clearly the most threatened sphere. Impact on the environment could be considerable.
**3. Induced Pluripotent Stem Cells (iPS cells)**

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
In recent studies, published in July 2009 in the journals "Nature" and "Cell Stem Cell", Chinese scientists (from two independent groups) used viruses to flip genetic switches in the DNA of skin cells from adult mice to turn them into iPS cells (induced pluripotent stem cells) in the laboratory. The researchers then injected some of the iPS cells into very early embryos that are capable of forming a placenta but not of fully developing on their own. The resulting embryos were then transferred into the wombs of surrogate mice. This achievement is considered as a proof that iPS cells are functionally equivalent to embryonic stem cells. According to the researchers, "This gives us hope for future therapeutic interventions using patients' own reprogrammed cells (without using embryonic stem cells)." Opponents of human embryonic stem cell research said the findings provide the latest in a growing body of evidence for why such research is no longer necessary.

**Potential threat indications:**
According to the Washington Post article, "the cells' ability to produce almost genetically identical offspring raised the fear that rogue scientists might misuse the technique to attempt to clone humans." Dr. Robert Lanza, a stem cell researcher at Advanced Cell Technology in Worcester, Mass. Said that this research revives concerns raised by reproductive cloning. "With just a little piece of your skin, or some blood from the hospital, anyone could have your child -- even an ex-girlfriend or neighbor…. This isn't rocket science -- with a little practice, any IVF clinic in the world could probably figure out how to get it to work." Perhaps one can even imagine criminal organizations using this as an opportunity to fabricate fictitious fraternity suits from billionaires… According to the recent publications, researchers could also genetically engineer traits into the cells before using them to create embryos for "designer babies". Such activity, if forbidden by law, could be an opportunity for crime organizations. In the words of Dr. Lanza: "For instance, the technology already exists to genetically increase the muscle mass in animals by knocking out a gene known as mystatin, and could be used by a couple who wants a great child athlete."

**Sources for technology description:**
Researchers May Have Found Equivalent of Embryonic Stem Cells, Washington Post, July 24, 2009

"Meet 'tiny,' a mouse grown from induced stem cells", Scientific American, July 24, 2009


**Sources for threat indication:**
Researchers May Have Found Equivalent of Embryonic Stem Cells, Washington Post, July 24, 2009
Description of this technology in the FESTOS expert survey:
Scientists used viruses to flip genetic switches in the DNA of skin cells from adult mice to turn them into iPS cells that are functionally equivalent to embryonic stem cells. A recent research showed that mice skin cells can be transformed into neurons quickly and efficiently. According to some opinions, this may enable genetically engineer traits into the cells before using them to create "designer embryos". It also revives concerns regarding reproductive cloning.

(Potential threat: Could such techniques be used by criminals or "rogue organisations" for malicious purposes? Perhaps one could speculate about camouflage at the cell level?)

FESTOS experts survey results:

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>very difficult (1.44)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>low severity (1.87)</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases with time. As expected, the most threatened societal sphere is people. The impact on values is also likely to be considerable.
4. Bio-mimicking for fluids mixing at extremely small scales

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description:
The problem of mixing at very small scales has confronted biomedical researchers for many years. Scientists now hope to speed up biomedical reactions by filling reservoirs with tiny beating rods that mimic cilia, the hair-like appendages that line organs such as the human windpipe, where they sweep out dirt and mucus from the lungs. The researchers created a prototype that mixes tiny volumes of fluid or creates a current to move a particle. They used a novel underwater manufacturing technique to overcome obstacles faced by other teams that have attempted to build a similar device. The resulting prototype is a flexible rubber structure with fingers 400 micrometers long that can move liquids or biological components such as cells at the microscopic scale. The team varied the length and spacing of the fingers to get different vibration frequencies. When they now apply a small vibration to the surrounding water, the fingers move back and forth at 10 to 100 beats per second, roughly the vibration frequency of biological cilia.

Potential threat indications:
Some extremely toxic substances to be produced need very small scale mixing. New mixing technologies like the one described above, if abused, might pose a threat by enabling preparation of toxins harmful for humans in micro quantities.

Sources for technology description:
Bio-mimetic silicone cilia for microfluidic manipulation, Lab Chip, 2009,9, 1561 - 1566, DOI: 10.1039/b817409a

Sources for threat indication:
Description of this technology in the FESTOS expert survey:
Scientists plan to speed up biomedical reactions by filling reservoirs with tiny beating rods that mimic cilia. They created a prototype that mixes tiny volumes of fluid or creates a current to move a particle: a flexible structure with fingers 400 micrometers long that can move liquids or biological components such as cells at the microscopic scale. (Potential threat: Perhaps such technologies will enable the preparation of toxic substances that need very small scale mixing and are harmful in micro quantities?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2030</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (1.92)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.07)</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood is increasing with time. People and the environment are clearly the most threatened societal spheres.

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>0%</td>
<td>100%</td>
<td>13%</td>
<td>50%</td>
<td>13%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood is increasing with time. People and the environment are clearly the most threatened societal spheres.
5. Gene transfer

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description (as presented in the expert survey):**
New devices and methods are being developed for transferring genes from one living organism to another. Such devices could be increasingly available (and affordable) in the future.

**Potential threat indications (as presented in the expert survey):**
Could future tinkering with biological organisms resemble the "culture" of computer hackers? Could this trend evolve into "bio-hacking" culture?

**FESTOS experts survey results:**

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (3.52)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (3.22)</td>
</tr>
</tbody>
</table>

**Societal spheres potentially threatened:**

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>27%</td>
<td>9%</td>
<td>90%</td>
<td>9%</td>
<td>82%</td>
<td>25%</td>
</tr>
</tbody>
</table>

**Interpretation:**
The most threatened societal spheres are first of all people, followed by the environment. Nevertheless, the results indicate that potential threats to values and to the economy should not be ignored.

----

17 Gene transfer was not included in the preliminary scanning report D2.1
Biotechnology: overall assessment

It seems that most of the potential bio-threats will mature only in the next decade (after 2020) and will have an impact relatively late. The likelihood of the threats increases with time, hinting at the difficulties to actually use the technologies for malicious purposes. If perpetrators overcome the difficulties and realize the threats, people will be the most affected sphere in society (100% in most cases) and other spheres might be affected to a lesser degree. It is important to stress that values are also significantly threatened in several areas – implying that value systems could undergo significant changes due to advances in biotechnology and the associated potential threats.
Chapter 6. Main Field: Robotics

6.1 Robotics: Introductory Overview

Robotics was born in the Science Fiction literature, and Science Fiction visions have inspired the field for many years. The term “robot” was coined by Czech author Karl Capek in 1924. The Science Fiction writer Isaac Asimov, introduced the term “robotics” in 1941 as a discipline of study, and wrote many stories about humanoid robots, where the main basis for the plot was his famous (fictional) “three laws of robotics”. These laws were invented to assure that robots perform their missions without harming humans. According to some experts, and in particular robotics scientists in Japan and Korea, the 21st century will witness humanoid robots leaving the pages of fiction and stepping into the real world and everyday life.

The field of robotics encompasses a broad spectrum of technologies in which computational intelligence is embedded in machines, creating systems with capabilities far exceeding the core components alone. Such robotic systems are then able to carry out tasks that are unachievable by conventional machines, or even by humans working with conventional tools. In particular, the ability of a machine to move and act “autonomously” opens up an enormous range of applications that are uniquely suited to robotic systems.

According to a panel report of the World Technology Evaluation Center (WTEC), robotics is a very active research and development field worldwide\(^\text{18}\). The WTEC report includes a comprehensive evaluation of the state of robotics worldwide, based on an extensive survey and visits in key laboratories in many countries.

The WTEC panel found that, as of 2006, Japan, Korea, and the European Community have invested significantly larger funds in robotics R&D for the private sector than the U.S. The U.S. leads in such areas as robot navigation in outdoor environments, robot architectures (the integration of control, structure and computation), and in applications to space, defense, underwater systems and some aspects of service and personal robots. Japan and Korea lead in technology for robot mobility, humanoid robots, and some aspects of service and personal robots (including entertainment). Europe leads in mobility for structured environments, including urban transportation. Europe also has significant programs in eldercare and home service robotics. Australia leads in commercial applications of field robotics, particularly in such areas as cargo handling and mining, as well as in the theory and application of localization and navigation. In contrast with the U.S., Korea and Japan have national strategic initiatives in robotics\(^\text{19}\).

Robotic vehicles (mostly developed in the defense and space fields) are machines that move “autonomously” on the ground, in the air, undersea, or in space. In general, such vehicles move under their own power, with sensors and computational


\(^{19}\) ibid
resources onboard to guide their motion. Usually such “unmanned” robotic vehicles involve some form of human oversight or “supervisory control” or even more direct remote control. A higher level of autonomy is an important trend of emerging technologies, and in certain future systems there will probably be zero (or almost zero) human intervention. The autonomy of robotic vehicles is heavily dependant on available power and energy efficiency. Important developments directions in this aspect are various “energy harvesting” means (e.g. solar cells, temperature gradients, currents, wind, vibrations, and biological batteries), and energy management techniques.

In the evolution of robotics, there is a long tradition of utilizing biological systems as inspiration and models for new technological solutions. Several labs carry out Biomimetics research for robotic applications.

NextGen Research forecasts that the worldwide demand for all-purpose service robots will reach $15 billion by 2015, or roughly 5 million robots per year\(^{20}\). Japan Robot Association estimates that the robotics sector should exceed $66 billion by 2025. Most of the growth will be in non-industrial applications, especially, in areas such as toys, transportation, and health and elderly care\(^{21}\).

According to a recent forecast by Techcast\(^{22}\), it is likely that by the year 2023 “intelligent robots that sense their environment, make decisions, and learn are used in 30% of households and organizations”.

The last (2005) large-scale Delphi survey conducted in Japan by NISTEP evaluated, among other areas, the aspects of human and robot participation in manufacturing. According to the survey report: “This area can be roughly divided into topics likely to be achieved in the medium term (around 2020), and those likely to require longer times for realization (2020–2030). The former include robots for work in hazardous environments, the impact of robot use on employment opportunities in manufacturing, and avoidance of human error. In the long term, the path towards integration of humans, machines, and data can be seen, and beyond that lies biological integration including biotechnology and robot control utilizing advanced detection of human brain waves”.

A particularly interesting emerging trend in robotics is cooperative robotic teams and “robotic swarms”. Swarm robotics is a novel approach to the coordination of large numbers of robots, inspired by the behaviour of swarms in nature, e.g. social insects that show how a large number of simple individuals can interact to create collectively intelligent systems. Recent EU projects like SYMBRION have developed novel principles of adaptation and evolution for symbiotic multi-robot systems, which will be able to self-configure and self-evolve, based on bio-inspired approaches and advanced computing paradigms.

In a keynote address to the UK Royal United Services Institute (RUSI) in March 2008, Professor Noel Sharkey, a robotics and AI expert at the University of Sheffield, expressed his concerns that we are witnessing the first steps towards a robot arms race and that it may not be long before robots become a standard terrorist weapon to

\(^{20}\) CNET News 5/27/09
\(^{22}\) www.techcast.org
replace the suicide bomber. According to Sharkey, “With the current prices of robot construction falling dramatically and the availability of ready-made components for the amateur market, it wouldn't require a lot of skill to make autonomous robot weapons.” He pointed out that a small GPS guided drone with autopilot could be made for around £250.²³

In the following pages we describe several selected robotics technologies, along with the assessment of their potential threats based on the FESTOS expert survey.

For completeness, we mention here robotics topics that were described in D2.1 but not included in the expert survey:

- Artificial Exoskeletons;
- Autonomous Underwater Vehicles / Robots;
- Biped Gait;
- Cellphone-guided robots;
- Hexapod locomotion;
- LIDAR based navigation of robots;
- Simultaneous Localization and Mapping (SLAM);
- Robots that can map out underground tunnels;
- Micro Air Vehicles (MAV);

6.2 Selected Robotics technologies and evaluation of associated potential threats

<table>
<thead>
<tr>
<th>1. AI-based Robot-Human Interaction and Co-existence</th>
</tr>
</thead>
<tbody>
<tr>
<td>S&amp;T Field:</td>
</tr>
<tr>
<td>Nanotech</td>
</tr>
<tr>
<td>X</td>
</tr>
</tbody>
</table>

Description:
Japan and S. Korea are preparing for the “human-robot coexistence society,” which is predicted to emerge before 2030; S. Korea predicts that every home in its country will include a robot by 2020. These “Next Generation Robots” will have relative autonomy, working in ambiguous human-cantered environments, such as nursing homes and offices. Regulators are trying to figure out how to address the safety and legal issues that are expected to occur when an entity that is definitely not human but more than machine begins to infiltrate our everyday lives. Taiwanese researchers have recently proposed a framework for a legal system focused on Next Generation Robot safety issues. Their goal is to help ensure safer robot design through “safety intelligence” and provide a method for dealing with accidents when they do inevitably occur. They propose categorizing future robots as “third existence” entities: neither living/biological (first existence) or non-living/non-biological (second existence). A third existence entity will resemble living things in appearance and behaviour, but will not be self-aware. They believe that a third existence classification would simplify dealing with accidents in terms of responsibility distribution. Integrating robots into human society poses “open texture risk” - risk occurring from unpredictable interactions in unstructured environments. An example is getting robots to understand the nuances of natural (human) language. The authors have proposed a “legal machine language,” in which ethics are embedded into robots through code, which is designed to resolve issues associated with open texture risk. Most robotics researchers predict that human-based intelligence will inevitably become a reality following breakthroughs in computational AI (in which robots learn and adapt to their environments in the absence of explicitly programmed rules). Notably, in "ROBOT: Mere Machine to Transcendent Mind" Carnegie Mellon Robotics institute professor Hans Moravec (well-known robotics expert) predicts that robot intelligence will "evolve" from lizard-level in 2010 to mouse-level in 2020, to non-key level in 2030, and finally to human level in 2040 - in other words, some robots will strongly resemble “first-existence entities by mid-century. However, a growing number of researchers - as well as the authors of the current study - are leaning toward prohibiting human-based intelligence due to the potential problems and lack of need; after all, the original goal of robotics was to invent useful tools for human use, not to design "pseudo-humans".

Research by Spain's National Distance Learning University (UNED) and the Institute for Prospective Technological Studies on the potential impact of robots in society has concluded that the enormous automation capacity of robots, and their ability to interact with humans, will create a technological imbalance over the next 12 years between the “haves” and the “have nots.” During the next 15 years, the hybridisation of humans and robots will become just as prevalent as mobile phones and cars are today, says UNED professor Antonio Lopez Pelaez, a co-author of the study.

International experts working on inventing and adapting cutting edge robots for practical use were interviewed during the study, in order to find out by when we will be regularly using the models they are currently designing. All agreed on 2020 as a technological inflection point,
because by then robots “will be able to see, act, speak, manage natural language and have intelligence, and our relationship with them will have become more constant and commonplace”, said López Peláez. This will follow a revolution in robotics after which they will no longer be sophisticated machines, but tools to be used on a daily basis, helping us with a large number of work and social activities.

Another important role will be the replacement of people working in the areas of security, surveillance or defence. According to Professor López Peláez, it is predicted that 40% of armies will be automated with robot soldiers by 2020 “just as a car factory is today, which will result in less human deaths during violent conflicts”.

The most striking feature of this technological revolution are social robots, machines with artificial intelligence, and with which we will have emotional and even intimate interactions. “A robot might be a more effective partner and a better person than the humans we actually have in our immediate lives: just as you can see dog owners talking to their pets today, soon we will be talking to robots,” says López Peláez – to such an extent that sexual robots are currently being designed to carry out pleasurable personal interactions. These will be equipped with the required sensorial abilities, such as touch.

Potential threat indications:
Since these expected advances in AI and robotics are perceived as having serious potential safety threats, it not difficult to imagine what could result from an abuse by terrorists or criminals. What if “human-based intelligence” is not prohibited as proposed by the Taiwanese researchers, and it is used for sinister purposes? “Robot terrorists” may be envisioned. The threat is strongly dependent on the level of artificial intelligence embedded.

Sources for technology description:
http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=weng_yueh_hsuan

www.sciencedaily.com/releases/2008/12/081205100137.htm

Sources for threat indication:
Same as above

Description of this technology in the FESTOS expert survey:
Japan and S. Korea are preparing for the “human-robot coexistence society,” which is predicted to emerge before 2030. Some researchers propose categorizing future robots as “third existence” entities: neither living / biological (first existence), or non-living / non-biological (second existence). A striking feature of this development are "social robots" with artificial intelligence (Al), with which people will have emotional and even intimate interactions.

(Potential threat: What if an entity that is definitely not human but more than machine begins to infiltrate our everyday lives? Regulators are trying to figure out how to address the emerging safety and legal issues that are expected to emerge. Will these developments lead to new opportunities for malicious use of robots that have close intimate interactions with people that trust them?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2023</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (3)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.94)</td>
</tr>
</tbody>
</table>

![Graph showing the likelihood to pose a security threat over time.]

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Societal Spheres</th>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>41%</td>
<td>35%</td>
<td>88%</td>
<td>59%</td>
<td>41%</td>
<td>41%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases with time. The most threatened societal spheres are people and infrastructures. Note the relatively high score of values, environment and the economy.
# 2. Autonomous & Semi-Autonomous Mini Robots: Toys and Amateur Objects

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Description:

The progress in robotics, combined with micro/nano technologies, and in particular small robots with relatively high level of autonomy, reflects potential dangers. Experts such as J. Altmann foresee that future mobile mini/micro-robots have a high potential for intrusion into privacy and eavesdropping: "If small enough, they could covertly enter offices or houses – even through the crack under the door, or through an open window. Small robots could also act – e.g. steal, disrupt or destroy something. Injuring or killing people could be done while they sleep or, similar to an insect – and maybe even using an insect-like body, at any time and any place, in public or private. Tracing back the originator could be very difficult."

In this context, it is interesting to consider the project “Probo” as an example to the directions of study in human-robot relation, in particularly focused on children and with possible important implications on future toys for education and entertainment. Probo is “an intelligent huggable robotic friend” developed as research platform to study cognitive human-robot interaction (CHRI) with a special focus on children. The robot Probo is designed to act as a social interface, providing a natural interaction while employing human-like social cues and communication modalities. The robot will be used as a research platform to gradually incorporate more autonomy and intelligence. Probo is made accessible to the scientific community so that it can play a supportive research role in technical areas (such as vision, speech, AI and cognition), medical areas (exploration of Robotic Assisted Therapy (RAT)) and social/psychological areas (focus on HRI and emotional communication).

## Potential threat indications:

According to experts such as J. Altmann, fully capable small robots used as toys, or robots built by amateurs, pose a **great potential for accidents and abuse**. Thus, he suggests that toy and amateur robots should be limited in mobility and sensing/actuating capability: “To hamper certain covert uses, they should not be produced below about 20 cm size”, and amateurs “should not be allowed to use robots capable of moving outside of their homes or laboratories that are smaller than 0.2 or 0.5 m size”.

Thinking about “robotic friends” like Probo, it should be taken into account that children may be sometimes used as a tool in organised crime and terrorism as they are less easily detected and more easily expendable. Such technology could perhaps be used as an aid to “Brainwashing” children in different ideologies or to encourage them to commit crimes e.g. placing devices in strategic locations.

## Sources for technology description:


www.physorg.com/news148727070.html
Sources for threat indication:
Same as above

Description of this technology in the FESTOS expert survey:
There is a fast progress in robotics, combined with micro/nano technologies. Small robots with relatively high level of autonomy are being developed for non-military applications, e.g for medical applications as well as for the toys industry.

(Potential threats: Experts foresee that future mobile mini/micro-robots have a high potential for intrusion into privacy and eavesdropping: they could covertly enter offices or houses – even through the crack under the door. Could small robots also disrupt or destroy, or injure people in a similar way to an insect – maybe even using an insect-like body?)

FESTOS experts survey results:

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (3.36)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.83)</td>
</tr>
</tbody>
</table>

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>29%</td>
<td>14%</td>
<td>93%</td>
<td>71%</td>
<td>36%</td>
<td>43%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases with time. The most threatened societal spheres are people and infrastructures. Effects on economy and environment as well as values are not negligible.
### 3. Robots as artificial limbs

<table>
<thead>
<tr>
<th>S&amp;T Field</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cognition</td>
</tr>
</tbody>
</table>

#### Description:

The popular TV series "The Six Million Dollar Man" described a man with some artificial limbs implanted after a hard crash. By the use of this dexterous and very innovative new body parts he had extraordinary skills. Today there are different applications of robots which are/will be implemented in human bodies. For example, a research at the Technical University of Berlin deals with powered leg orthoses using electromyographic signals for control and on prosthetic hands.

In fact, these technical features are for recovery of physical functions after accidents or diseases, but in theory this technique could be used to enhance skills of a person by implementing robot arms or legs or something else. At the same time the development of interfaces between human bodies and brains become more and more successful. Precondition for this development is an improvement of microelectromechanical systems (MEMS).

#### Potential threat indications:

A person with extraordinary skills could become a very new kind of threat.

#### Sources for technology description:

- [http://www.wtec.org/robotics/](http://www.wtec.org/robotics/)

#### Sources for threat indication:

#### Description of this technology in the FESTOS expert survey:

Various applications of robots could be implemented in human bodies. For example, a research is carried out on powered leg orthoses using electromyographic signals for control, and on prosthetic hands. These technical features are being developed for recovery of physical functions after accidents or diseases.

(Potential threat: Could such features be employed to enhance skills of a person by implementing robot arms or legs, and be used for malicious purposes by perpetrators or terrorists?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2018</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (2.63)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>low severity (1.78)</td>
</tr>
</tbody>
</table>

Likelihood to pose a security threat (from 1 - very unlikely, to 5 - very likely)

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>33%</td>
<td>11%</td>
<td>89%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases with time. The most threatened societal sphere is people. The impact on values in significant.
4. Ethical Control of Robots

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
<th>Cognition</th>
</tr>
</thead>
</table>

**Description:**
The adoption of autonomous robots (drones) in military environments leads to new problems of control. The deployment of drones behind enemy lines and over long distances makes direct human control not feasible. Therefore, technologies have to be developed, which enables the robots to make autonomous decisions. These decisions have to be based on ethical considerations. Especially the questions, which rules of engagement this kind of vehicles should follow, when no human control is present demands an ethical control. To tackle these issues, recently, the development of ethical controls became a new field in computer science and philosophy.

The foreseeable use of autonomous systems in civilian (e.g. domestic) environments will lead to the use of such ethical control systems in new areas. An especially problematic field is the security area (policing) and domestic use (home care).

**Potential threat indications:**
1. Malfunctioning systems could make disastrous moral decisions.
2. Malevolent persons could reconfigure such systems for terrorist or criminal use.
3. Knowledge about the decision making of such robots could be used by criminals to "trick" them.

**Sources for technology description:**

**Sources for threat indication:**

**Description of this technology in the FESTOS expert survey:**
The adoption of autonomous robots, in particular in military environments, leads to new problems of control. Autonomous decisions have to be based on ethical considerations. Recently, the development of ethical controls became a new field in computer science and philosophy. The application of autonomous systems in civilian (e.g. domestic) environments will lead to the use of such ethical control systems in new areas.

(Potential threats: Could one envision malfunctioning systems that make disastrous decisions or malevolent persons that reconfigure such systems for terrorist or criminal use?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2023</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>difficult (2.29)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>low severity (2.17)</td>
</tr>
</tbody>
</table>

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>17%</td>
<td>33%</td>
<td>83%</td>
<td>17%</td>
<td>50%</td>
<td>17%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood is constant over time. The most threatened societal sphere is people, followed by the environment. The political systems might also be sensitive to the threat.
5. Swarm Robotics

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description:

Similar to animal operations in nature in which the single player are not as intelligent as the swarm, robots with limited skills should act in a swarm to reach a sophisticated behaviour. One of the main experts in this field describes them as follows: "Swarm robotics is a novel approach to the coordination of large numbers of robots. It is inspired from the observation of social insects (ants, termites, wasps and bees) which stand as fascinating examples of how a large number of simple individuals can interact to create collectively intelligent systems. Social insects are known to coordinate their actions to accomplish tasks that are beyond the capabilities of a single individual: termites build large and complex mounds, army ants organize impressive foraging raids, and ants can collectively carry large preys. Such coordination capabilities are still beyond the reach of current multi-robot systems." (Sahin, 2005)

An application could be the exploration of an unknown area, or collaboration of different robots to move or accomplish a task which is too difficult for the single robot – like ants which work together to carry heavy objects. Today some experimental examples of swarm robots already exist. For example, the "I-Swarm" project at the Fraunhofer Institute in Karlsruhe or the "swarm-bot" project at the École Polytechnique Fédérale de Lausanne. Similar techniques are possible for flying robots as the Australian Center for Field Robotics has shown in their "Ubiquitous Networking Project".

The EC FP7 projects SYMBRION and REPLICATOR investigate and develop novel principles of adaptation and evolution for symbiotic multi-robot systems based on bio-inspired approaches and modern computing paradigms. These exploratory systems consist of super-large-scale swarms of robots, which can dock with each other and symbiotically share energy and computational resources within a single artificial-life-form. They can dynamically aggregate into one or many symbiotic organisms and collectively interact with the physical world via a variety of sensors and actuators. According to the projects vision, such bio-inspired robotic organisms can become self-configuring, self-healing, self-optimizing and self-protecting from both hardware and software perspectives. This leads not only to extremely adaptive, evolve-able and scalable robotic systems, but also enables robot organisms to reprogram themselves without human supervision and for new, previously unforeseen, functionality to emerge. In addition, different symbiotic organisms may co-evolve and cooperate with each other and with their environment.

Based on another EU project (I-SWARM) researchers envision that tiny (about 4 millimeters size) robots could be mass-produced in swarms and programmed for a variety of applications, such as surveillance, micro-manufacturing, medicine, cleaning, and more. In an effort to reach this goal, a recent study has demonstrated the initial tests for fabricating microrobots on a large scale.

The technique involves integrating an entire robot - with communication, locomotion, energy storage, and electronics - in different modules on a single circuit board. The researchers use conductive adhesive to attach the components to a double-sided flexible printed circuit board using surface mount technology. The circuit board is then folded to create a three-dimensional robot. As the researchers explain, a single microrobot by itself is a physically simple individual. But many robots communicating with each other using infrared sensors and interacting with their environment can form a group that is capable of establishing swarm intelligence to generate more complex behavior. According to the researchers, by mass-producing swarms of robots, the loss of some robotic units will be negligible in terms of cost, functionality, and time, yet still
achieve a high level of performance.
Interestingly, a German researcher has recently shown that robots which resemble natural creatures are accepted as "members" by a swarm or group of animals, and could lead them. The animals follow the artificial guide even to dangerous places like the surroundings of predators. The research showed that to guide a swarm or a group you need circa 5 - 10 % of whole. The researcher claims that the same principle applies to humans as well.

**Potential threat indications:**

Robot swarms can perform new kinds of attacks (on the ground as well as under water and in the air). For example, small networked flying robots which may be unobservable by automatic defense systems could coordinate an attack such that each robot carries a small dose of explosives but the combined effect is huge.

Besides, the swarms could be used to disrupt surveillance technologies. Similar knowledge to the above-mentioned German research could be used to guide crowds in panic – in a positive and negative ways.

Higgins (2009) provides three weaknesses of swarm robots, which raise security concerns: “In particular, swarms of robots potentially (i) employ different types of communication channels (ii) have special concepts of identity, and (iii) exhibit adaptive emergent behaviour which could be modified by an intruder.”(Higgins, 2009). Bio-inspired self-evolvable and self-configuring swarms may pose a threat in the future, if the self adaptation and self-reprogramming are intentionally employed for malicious behaviour of the swarm. The ability to relatively easily mass-produce tiny robots for swarms (as described above) may make the threats more concrete.

**Sources for technology description:**
EC FP7 projects SYMBRION and REPLICATOR: www.symbrion.eu
Wenn Menschen schwärmen: www.fv-berlin.de/pm_archiv/2009/33-schwaerme.html (in German)

**Sources for threat indication:**


**Description of this technology in the FESTOS expert survey:**

Swarm robotics is a novel approach to the coordination of large numbers of robots. It is inspired mainly by the observation of insects, which show how a large number of simple individuals can interact to create collectively intelligent systems. Based on the EU project I-SWARM researchers envision that tiny (about 4 millimeters size) robots could be mass-produced in swarms and programmed for a variety of applications, such as surveillance, micro-manufacturing, medicine, cleaning, and more.

(Potential threat: Is it possible that the self adaptation and self reprogramming are intentionally employed for malicious behavior of the swarm? Could the ability to easily mass-produce tiny robots for swarms make the threat even more concrete?)
FESTOS WP2  Final report on potentially threatening technologies  D2.3

FESTOS experts survey results:

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2030</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (2.89)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (3)</td>
</tr>
</tbody>
</table>

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>22%</td>
<td>11%</td>
<td>78%</td>
<td>78%</td>
<td>67%</td>
<td>67%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases in the long range. The most threatened societal spheres are people and infrastructure. Economy and the environment are significantly affected too.

Robotics: overall assessment

The expert survey results show that the field of Robotics will give rise to potential new threats in the coming years. Generally the threat likelihood increases with time. As expected, people are likely to be the most threatened sphere in society. Some technologies will have significant impact on values. Other spheres like environment or economy are likely to be impacted by part of the emerging technologies.
Chapter 7. Main Field: New Materials

7.1 New Materials: Introductory Overview

Emerging trends

Advances in Materials Science and Engineering have enormous impact on future manufacturing industries and new products. Moreover, the evolution of materials has shown that new materials or advanced materials processing can signal the birth or death of entire industries. New technological approaches and capabilities, in particular nanotechnologies, have enabled going down to the nanoscale and molecular states of materials and new ways to create, process, and eventually use them. In the last decades the materials sector is increasingly concerned with tailoring a growing list of ever more specialized materials for narrow niche applications. This trend is likely to continue, by utilizing innovative technologies.

High-performance alloys, nanocomposites, super-strength materials, new laminates, carbon nanotubes and other nanomaterials, a variety of special coatings, and new biological or bio-inspired materials are just a few examples of the richness of this field. Important areas are “smart materials” and "multi-functional materials" that respond in a desired manner to changing external conditions and are being developed for use in sophisticated structural as well as electronic, optical, magnetic, and biotech applications. A multifunctional material is a composite or hybrid of several distinct material phases in which each phase performs a different function. New functional materials will enable new enhanced system performance, for example adaptable performance, mission tailorability and morphing. With increasing complexity, multifunctional materials become not mere materials but sophisticated systems with controllable features, for example “artificial muscles” and “self-healing” materials, to name just two examples.

An exciting and imaginative future trend that deserves special attention is “programmable matter”. It's vision seems like science fiction and is inspired by science-fictional thinking. This vision was described in the magazine Nature by Wil McCarthy, an aerospace engineer and Science Fiction writer: “In the 22nd century, of course, any competent designer will simply define the shape and properties they require, including 'unnatural' traits such as super-reflectance, refraction matching (invisibility), and centuple bonds far stronger than diamond, then distribute the configuration file to any interested users.” McCarthy illustrated the outcomes in the following scenario: “4 July 2100. The flick of a switch: a wall becomes a window becomes a door. Any chair becomes a hypercomputer, any rooftop a power or waste-treatment plant. We scarcely notice; programmable matter pervades our homes, our workplaces, our vehicles and environments. There isn't a city on Earth — or Mars, for that matter — that isn't clothed in the stuff from rooftop to sub-basement. He gave the example of “quantum dot” (a nanocrystal particle with unique features) as a possibly building block: “The unique trait of a quantum dot, as opposed to any other electronic component, is that the electrons trapped in it will


arrange themselves as though they were part of an atom, even though there’s no
atomic nucleus for them to surround. Which atom they emulate depends on the
number of electrons and the exact geometry of the wells that confine them, and in
fact where a normal atom is spherical, such ‘designer atoms’ can be turned into
cubes, tetrahedra or any other shape, and filled with vastly more electrons than any
real nucleus could support, to produce ‘atoms’ with properties that simply don’t occur
in nature.\textsuperscript{26}

DARPA is not waiting till the 22-nd century, and is already funding Programmable
Matter research to create materials that can be programmed to self-assemble, alter
their shape to perform a desired function, and then disassemble. Among the
expected breakthroughs in this program are encoding information into chemistry, or
fusing materials with machines, and fabrication of mesoscale particles with arbitrary
complex shapes, composition, and function. Known also as “Info Chemistry”, this
emerging field combines chemistry, information theory, and programmability to build
information directly into materials.\textsuperscript{27}  Dr. M. R. Zakin, program manager for
Programmable Matter project, described a science-fiction-like scenario to illustrate
DARPA’s expectations: “In the future a soldier will have something that looks like a
paint can in the back of his vehicle. The can is filled with particles of varying sizes,
shapes and capabilities. These individual bits can be small computers, ceramics,
biological systems—potentially anything the user wants them to be. The soldier
needs a wrench of a specific size. He broadcasts a message to the container, which
causes the particles to automatically form the wrench. After the wrench has been
used, the soldier realizes that he needs a hammer. He puts the wrench back into the
can where it disassembles itself back into its components and re-forms into a
hammer.” That is the essence of programmable matter, according to Zakin. It means
distributing processing capabilities throughout the material: “You’re blurring the
distinction between materials and machines. Materials act like computers and
communications systems, and communications systems and computers act like
materials.”\textsuperscript{28} Such technological developments, if achieved, will have tremendous
impact on our lives. The DARPA project is aimed at defense applications, but the
research (carried out in leading universities like Harvard, MIT and Cornell) has high
potential for important civil applications ranging from aerospace to medicine.
Morphing materials can be used to change an aircraft’s wings in flight or in clothing
that alters its characteristics to keep users cool in the day and warm at night. One of
the possible future directions is programming adaptability into the material itself.
Such adaptability, for example, could produce electronic devices that can adapt to

\textsuperscript{26} ibid
\textsuperscript{27} DARPA’s Programmable Matter Initiative, 25 August 2009,

\textsuperscript{28} Programmable Matter Research Solidifies: Signal Magazine, June 2009,
neid=263
heat and dust in the desert and then shift to resist humidity and moisture in a jungle environment ²⁹.

**Terrorism threats**

Future materials with enhanced controllable features may be attractive for terrorist groups in various ways, from enhancing explosive properties to sophisticated concealment, camouflage, invisibility, protection of covert activities and more, development of new toxic chemicals and more. Terrorist groups have already shown their capability to develop and manufacture super-toxic lethal chemicals and highly contagious biological agents. This is enabled by scientific and technological developments in material science and is partly a result of open access to information, contributing also to the scientific and technological level of well-organized terrorist groups. The growing worldwide dissemination of knowledge mainly by means of the Internet enables quick global communication without the risk of being disclosed.

There exists a database of incidents involving chemical, biological, radiological and nuclear materials. The Centre for Non-Proliferation Studies at the Monterey Institute of International Studies, USA, marked about 400 relevant cases. Most of them are connected with chemical and biological materials combined with clearly shown terrorist motivation. Among chemicals, besides manufacturing toxic agents, the most effective are supertoxic lethal chemicals (standard chemical warfare agents, like GB and VX). Also, the misuse of stolen riot-control agents and toxic industrial chemicals like chlorine, phosgene, hydrogen cyanide, cyanogen chloride etc. can be considered for direct mass-casualty or mass incapacitation attacks (to evoke panic). Much wider possibilities in the choice of chemicals are given in indirect attacks (or threats of attacks), i.e. through contaminated water or food. Beside stable supertoxic agents (like VX, HD etc.) many other chemicals like persistent pesticides, cyanides, arsenous compounds, heavy metals, oil products etc. can be expected.

Biological agents of many types and origin, accessible from stores at medical and university institutes, can be taken in consideration, including the misuse of infectious materials from foci of proceeding epidemics, both human and animal, not to mention the manufacturing of certain toxins. Similarly, radio-nuclides from several peacetime sources including radioactive wastes, disseminated by various mechanisms, (including conventional explosives) could be used in terrorist attacks. Diverse views have been expressed concerning the possibility of nuclear terrorism. Even if the construction of nuclear explosive device seems theoretically very simple, large very qualified teams and very specific conditions are necessary to develop and manufacture such a device. Taking into consideration material and technological requirements, including safety for the developing and manufacturing teams themselves, this is generally considered as hardly possible without state involvement. From strategic reasons, R&D and many manufacturing steps in the nuclear arena belong to best guarded state secrecy, and localized in strongly guarded areas. Nevertheless, taking in consideration proceeding nuclear horizontal proliferation, extent of the respective parts of the military-industrial complex in growing number of countries, leaking of information, material and brains are not excluded.

In parallel to the continuous decrease of numbers of operational military nuclear devices, paradoxically the nuclear terrorism threat increases due to growing volume of fissile material from nuclear weapons decommissioned mainly according to above

²⁹ ibid
mentioned agreements (IMF, START-I) as well as due to the routine upgrading of nuclear arsenals. The most threatening materials in this area are weapon-grade plutonium, but more probably the highly enriched uranium (HEU) due to its extremely high amount and possibility to construct primitive types of nuclear explosive devices\textsuperscript{30}. While there has long been concern about nuclear materials being acquired by non-state groups, recent reports indicate that nuclear wastes may now or soon be available to terrorist groups. Large quantities of highly enriched uranium (HEU) that are poorly controlled and otherwise unaccounted in the former USSR and some other countries could be a very attractive source. HEU can, however, be readily diluted with natural uranium to a low-enriched level where it has high commercial value as proliferation-proof fuel for nuclear energetic reactors.

Countering the threat of terrorists' use of chemical, biological, radiological, and nuclear materials, or high-yield explosive devices (CBRNE), requires a wide range of materials technologies. The following paragraph refers to some current needs for technologies that emerge in order to respond to the challenges posed by terrorism threats. This may provide additional view on important directions in research. Furthermore, some experts expressed their opinion that technologies developed in order to cope with these threats could (almost "symmetrically") be utilised by terrorist organisations for malicious purposes.

In the following pages we describe selected new materials technologies, along with the assessment of their potential threats based on the FESTOS expert survey.

For completeness, we mention here materials topics that were described in the preliminary scanning (report D2.1) but not included in the expert survey:

- Camera made of polymer fibres – without lenses;
- Chemical reactions for transmitting information;
- Dielectric Resonators (new materials for filtering radio-frequencies);
- Ultra speed transistor and ultra-high-speed memory;
- Advanced materials and technologies using physical simulation and virtual process modelling;
- Laser technologies;
- Self-healing concrete for durable infrastructures;
- Development of advanced materials by using physical simulation and virtual process modeling;

\textsuperscript{30} New Threats for the 21st Century: Chemical, Biological, Radiological and Nuclear Terrorism, \url{www.wagingpeace.org/articles/2002/05/00_matousek_new-threats.htm}
7.2 Selected New Materials technologies and evaluation of associated potential threats

1. Metamaterials and Optical Cloaking

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Optics</td>
</tr>
</tbody>
</table>

**Description:**
Several novel scientific discoveries in optics, materials, and nanotechnology in the last decade enabled research groups to develop theoretical models of cloaking devices made out of "metamaterials" that can hide objects from our sight, or make them appear as other objects. David Smith (now at Duke University) and his colleagues were the first to make metamaterials with negative refractive index in 2000. In 2006, a US-British team of scientists has successfully tested an "invisibility cloak" for microwave frequencies in the laboratory. The team, lead by David Schurig (Duke University) and by John Pendry (Imperial College London), described a realization of a cloaking device: a copper cylinder that was hidden inside a cloak consists of 10 fibreglass rings covered with copper elements. The team then showed that the copper cylinder and the cloak were actually "invisible" to microwaves frequencies. The invisibility was still imperfect because of the approximations used and material absorption, but their results provide an example for an electromagnetic cloaking mechanism, and demonstrate the feasibility of such technologies. (A video about the experiment: www.dukenews.duke.edu/2006/10/cloakdemo.html)

In order to build a cloaking device, there is a need to engineer materials at the nano level. There are several techniques that can be considered, such as electron-beam lithography, interference lithography, nanoimprint lithography, and two-photon photopolymerization (see "sources for technology description"). Those technologies can not be used to create real cloaking device at a reasonable cost today, but they are constantly evolving.

Since 2006 there have been many research activities around this subject, and several theoretical approaches for developing cloaking devices in visible light frequencies were suggested. A recent article describes a feasible design of a "cloaking carpet" that hides an object from sight from above, and can be used for camouflage purposes. In May 2009, a group of Chinese researchers demonstrated a theoretical design of an illusion cloak that can make one object to look like another object, or to create an illusion of a hole inside a wall so one can see what is happening on its other side. All these developments show that ideas that were used in Science Fiction years ago can become reality thanks to new nano-engineering techniques, and are not so far in the future as we might expect.

In December 2010 a new, rather surprising achievement was published: MIT researchers have built a "carpet cloak" capable of hiding objects in the millimetre range over a broad range of visible frequencies from red to blue. Moreover, they've built it not out of metamaterials but out of calcite, an ordinary and relatively cheap optical material, using conventional optical lens fabrication techniques. This makes the cloak cheap and easy to build. The researchers demonstrated it by hiding a wedge of steel 38mm long and 2 mm high.

**Potential threat indications:**
Widespread optical cloaking technology will dramatically change warfare, terror and crime possibilities.
The possibility is not only to make an object (or person?) invisible, but also to make it look as...
something different (sophisticated active camouflage). This opens imaginative possibilities of abuse. If such technologies are practically and effectively realized, one can envisage that in the future there will be a need to revolutionize areas such as VIPs security, to implement a variety of sensors in homeland security applications that used to be based on human sight, etc.

Sources for technology description:
[13] An optical cloak made of dielectrics, Jason Valentine1, Jensen Li1, Thomas Zentgraf1, Guy Bartal1 and Xiang Zhang, NATURE MATERIALS, April 2009. Link: www.nature.com/nmat/journal/vaop/ncurrent/pdf/nmat2461.pdf
[14] Illusion optics: The optical transformation of an object into another object, Yun Lai, Jack Ng, Huan Yang Chen, De Zhu Han, Jun Jun Xiao, Zhao- Qing Zhang, C. T. Chan,
Sources for threat indication:
http://cobweb.ecn.purdue.edu/~photspec/press.htm
http://beta.technologyreview.com/blog/arxiv/23519/?nlid=2029

Description of this technology in the FESTOS expert survey:
Such specially engineered metamaterials could enable optical "cloaking", and creation of 'super-lenses' with a spatial resolution below that of the wavelength. It has been shown that cloaking devices made out of metamaterials can hide objects from sight in certain wavelengths, or make them appear as other objects.

(Potential threat: Could this technology enable "invisibility cloaking", or perfect camouflage, for malicious purposes of criminals or terrorists?)

FESTOS experts survey results:

| When will this technology be sufficiently mature to be used in practice? | 2030 |
| How easy will it be to use this technology for malicious purposes that might pose security threats? | somewhat difficult (2.5) |
| How severe is the potential security threat posed by this technology? | medium severity (2.95) |

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>8%</td>
<td>31%</td>
<td>75%</td>
<td>85%</td>
<td>23%</td>
<td>46%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases significantly in the long range. The most threatened societal spheres are infrastructures and people, followed by the economy. Interestingly, the potential impact on the environment and on political systems is not negligible as well – a result that is not obvious for this particular technology.
2. Future fuels and structural materials for nuclear technologies.

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
</table>

**Description:**
The development of safe and efficient nuclear reactors needs advanced materials to produce fuels and reactor’s structural materials. Expansion in new materials research was made possibly by applying intense pulsed neutron sources based on proton accelerators rather than a reactor. Application of this technology allowed to discover a majority of organic superconducting materials or materials with record-breaking magnetoresistive effects in metallic layered materials. Other discoveries include radiation-induced segregation as an important microstructural process in metals. Alloys for thermonuclear fusion reactor applications that limit erosion, provide self-sustaining protective coating to minimize energy loss, and inhibit transfer of impurities. Uranium silicide fuels for research and test reactors which require only low-enrichment and are therefore proliferation-resistant. Synthesis of new organic superconducting materials and structure-property relationships; record high superconducting transition temperatures for these materials were also established. New ceramic compounds for high-energy-density fuel cells, and for oxygen-permeable membranes used in converting methane to liquid fuels. New solid lubricants based on boric acid compounds. Synthesis of high-quality nanocrystalline diamond film that is exceptionally smooth and has superior tribological properties. This technology makes able to determine the mechanisms of irradiation-induced swelling of materials; predict the behaviour of fuel elements in reactor cores; investigate and clarify the coexistence of superconductivity and magnetism in single crystals; develop inelastic neutron scattering techniques to provide unique information on dynamics of solids and liquids; determine the structural, thermodynamics and phase relationships of many transuranium compounds; elucidate the depth of origin of sputtered atoms and the mechanisms of sputtered cluster emission (this was important for applications in many fields including geochemistry, cosmochemistry, and the superconducting industry). Also developed was neutron radiography and other non-destructive testing techniques that are used throughout the world.

**Potential threat indications:**
In the opinion of experts new nuclear technology materials can be abused and bring new threats because of potential utilisation for making nuclear (both fissile and dirty) bombs by terrorist groups. The actually attractive HTGR (high temperature) nuclear reactors as a technology to produce energy from CO₂, needs very sophisticated materials, which in turn might pose a threat.

**Sources for technology description:**
www.anl.gov/Science_and_Technology/History/Anniversary_Frontiers/mathist.html

**Sources for threat indication:**
Discussion at the Military University in Warsaw

**Description of this technology in the FESTOS expert survey:**
New materials and processes for safe and efficient nuclear reactors have been developed, such as organic superconductors, materials with special magnetoresistive effects, radiation-induced segregation, Uranium silicide fuels which require only low-enrichment, new solid lubricants, nanocrystalline diamond films, etc. These enable to determine the mechanisms of irradiation-induced swelling of materials, predict the behaviour of fuel elements in reactor cores, develop inelastic neutron scattering techniques, determine properties of trans uranium compounds, and more.
(Potential threat: Could such techniques make it easier for terrorists to build fissile or "dirty" nuclear bombs?)

**FESTOS experts survey results:**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2023</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>difficult (2.33)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (3.07)</td>
</tr>
</tbody>
</table>

**Societal spheres potentially threatened:**

<table>
<thead>
<tr>
<th></th>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0%</td>
<td>25%</td>
<td>92%</td>
<td>83%</td>
<td>83%</td>
<td>25%</td>
</tr>
</tbody>
</table>

**Interpretation:**
The threat likelihood increases with time. Most societal spheres (except values) are expected to be threatened by this technology, in particular people, infrastructures and the environment.
3. Crystalline polymers, polymer blends, multilayer assemblies.

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
Polyethylene is widely used in film applications due to its low cost and excellent processing ability. It would be a candidate for additional packaging applications if a broader spectrum of gas permeability and selectivity characteristics were achieved. A useful technology for controlling structure–property relationships and improving the performance of polymeric materials involves blending with suitable functional constituents. Poly(ethylene oxide) (PEO) possesses an unusually high selectivity for CO$_2$ over nonpolar gases such as O$_2$, N$_2$, and H$_2$. Whereas the CO$_2$ permeability of a polyethylene film is about 43 the O$_2$ permeability, this value rises to 163 for PEO. This characteristic makes PEO attractive for gas separation and atmosphere control applications. Polyethylene and PEO are incompatible in melt blends. Very important is to combine polyethylene and PEO through the synthesis of copolymers containing poly (ethylene oxide) side chains grafted to poly(ethylene-co-acrylic acid) (EAA). It also appears that the presence of carboxyl groups on the polyethylene improves the compatibility. When PEO was blended with polyethylene under conditions that oxidized the polyethylene, much better dispersion was achieved.

The spectrum of gas permeability and selectivity characteristics of ethylene-based polymers is obtained by combining EAA with PEO. To obtain films that differed substantially in their solid state morphology, EAA was combined with PEO as melt blends and as coextruded films with many alternating, continuous microlayers of EAA and PEO. The design and fabrication of ultrathin polymer layers are of increasing importance because of the rapid development new materials technology. Confined, two-dimensional crystallization of polymers presents challenges and opportunities due to the long-chain, covalently bonded nature of the macromolecule. Using an innovative layer-multiplying coextrusion process it is possible to obtain assemblies with thousands of progressively thinner polymer layers. When the thickness is confined to 20 nanometers, the PEO crystallizes as single, high-aspect-ratio lamellae that resemble single crystals. Unexpectedly, the crystallization habit imparts two orders of magnitude reduction in the gas permeability.

The potential applications: long term food preservation and pharmaceutical industry, military and police applications due to specific mechanical endurance of multilayer foils (bullet-proof vests).

**Potential threat indications:**
Polymer materials are an interest of military manufacturing due to reduction of gas permeability. This kind of materials can be abused by terrorist groups wanting to use gas resistive coatings. There are several counterterrorism and crime means based on using “war gases”. The resistive coatings and easy accessible filters can strengthen terrorists activity.

**Sources for technology description:**

**Sources for threat indication:**
Talks with experts at the Military University, Warsaw
Sources for relevant Foresight:


Description of this technology in the FESTOS expert survey:
Controlling structure–property relationships to improve the performance of polymeric materials involves blending with suitable functional constituents. For example, Poly(ethylene oxide) (PEO) possesses an unusually high selectivity for CO$_2$ over non-polar gases such as O$_2$, N$_2$, and H$_2$ – which makes it attractive for gas separation and atmosphere control applications. Special gas permeability and selectivity characteristics are obtained by combining appropriate materials and new processes. Applications range from long term food preservation to specific mechanical endurance of multilayer foils (e.g. for bullet-proof vests).

(Potential threat: Since such polymers are of military interest due to reduction of gas permeability, could they be attractive to terrorist groups that want to use gas resistive coatings?)

FESTOS experts survey results:

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>difficult (2.56)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.11)</td>
</tr>
</tbody>
</table>

![Graph showing the likelihood to pose a security threat from 2015 to 2035]

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>0%</td>
<td>82%</td>
<td>45%</td>
<td>45%</td>
<td>36%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases in the long range and then tends to decrease. The most threatened societal spheres are people, followed by infrastructures and the environment. The impact on the economy could be considerable as well.
### 4. Water catalyzing explosive reactions

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**

A new study has shown that water, in hot dense environments, plays an unexpected role in catalyzing complex explosive reactions. Water rarely, if ever, acts as a catalyst under ordinary conditions. Using first-principle atomistic simulations of the detonation of the high explosive PETN (pentaerythritol tetranitrate), the research team discovered that in water, when one hydrogen atom serves as a reducer and the hydroxide (OH) serves as an oxidizer, the atoms act as a dynamic team that transports oxygen between reaction centres.

They found that nitrogen loses its oxygen mostly to hydrogen, not to carbon, even after the concentration of water reaches equilibrium. They also found that carbon atoms capture oxygen mostly from hydroxide, rather than directly from nitrogen monoxide (NO) or nitrogen dioxide (NO₂). Meanwhile water disassociated and recombines with hydrogen and hydroxide frequently.

**Potential threat indications:**

Mixing fluid chemicals is the way to produce explosives e.g. on a board of the aircraft. If water component is added to the solid materials, it would be a way to produce explosives without necessity to mix fluids. This technology could be used by terrorists to construct bombs on the board of an aircraft or might be used in other situations bringing to the uncontrolled explosions (e.g. used by the desperate people, youth experimenting with chemicals etc).

**Sources for technology description:**


**Sources for threat indication:**

**Description of this technology in the FESTOS expert survey:**

Research has shown that water, in hot and dense environments, plays an unexpected role in catalysing complex explosive reactions.

(Potential threat: Could this mean that adding water to appropriate solid materials could enable the preparation of powerful explosives without necessity to mix fluids?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>2030</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2030</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>difficult (2.56)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (3.38)</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases with time. The most threatened societal spheres are clearly people and infrastructures. The impact on other spheres (except values) is not negligible.
## 5. Personal rapid prototyping and 3-D printing machines

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Description:

The RepRap (a short for Replicating Rapid-prototyper) project at the University of Bath (UK) is working towards creating a cheap and easy-to-use 3D printer that can construct plastic products after downloading a detailed description from a computer. The software will be free under the GNU General Public License. The printer can build any 3D plastic model that one can think of – from flower pots, self portrait statues and Lego bricks, to mechanical parts, motherboards and vehicle replacement parts.

The personal rapid prototyping machines use different raw materials: thermoplastics (Polylactic acid), Ceramic slurries (Silicon nitride), Silicone polymer, Wood's metal, Field's metal, and even Chocolate.

The technology is not new, but commercial machines costs are around €30,000 (in 2009). One of the project goals is to design the printer that will be able to self-copy, at a cost of €500 (materials only), so that private people and little communities will be able to use it. Today RepRap can make up to 60% of its parts, and the other parts are relatively cheap and available to the common private user. Researchers are planning to increase that 60% by enabling RepRap printers to build its own electric circuitry, and future programs include expanding to a wide variety of materials: ceramics, wax, metals, etc.

There are other project regarding personal rapid prototyping machines (see "Sources for technology description"); the unique property of the RepRap project is the design of a printer that can self-copy, and the use of GNU General Public License for the technology. Those properties are likely to speed up the spreading of the technology. The main driver for wide spread personal rapid prototyping machines is the price. According to the "Worldwide Guide to Rapid Prototyping": "With recent price cuts, it's possible to buy a Solido LOM-based machine for less than $10,000, or a Dimension, FDM-based uPrint system for less than $15,000. Buyers who are willing and able to build a kit can be in business today for just a few hundred dollars".

Future trends in the field of rapid prototyping include:
- Increased speed, by using faster computers, more complex control systems, and improved materials
- Improved accuracy and surface finish
- The introduction of non-polymeric materials, including metals, ceramics, and composites

Personal rapid prototyping machines can also effect the global economy – a wide spread use can have a major revenue drawback in several industrial sectors, a major effect on the Chinese growth rate, and can cause a wide-spread violations of intellectual property rights, and an environmental damage due to the increasing use of plastic materials.

### Potential threat indications:

#### Home-made weapons

Personal rapid prototyping machines can potentially be used for creating weapons. Polymers are widely used in guns, and criminals can design new types of cheap guns that only need several simple metal parts, or combine common metal parts with specially designed plastic parts. Future generations of personal rapid prototyping machines will be able to work with hard ceramic materials that will open new opportunities for weapons. Polymer weapons may also pass metal detectors without been detected.

Other indications about plastic guns can be found in the article "Is it possible to make an undetectable nonmetal gun?" at "sources for threat indication" section.
Besides guns, other plastic weapons can be manufactured as well. In an article published in Dec. 2008 in telegraph.co.uk, Head of Scotland Yard anti-knife project Operation Blunt 2, Commander Mark Simmons, said:

"We have had some finds of non-metallic knives. The numbers are not vast at the moment, and they do not start me thinking that there is a major new trend. We have seen some made out of carbon fiber, a type of hard plastic. A few of those have been found. People will be ingenious about this sort of thing, and there will always be individuals thinking of different ways around a new policing tactic".

3D printers may pose a real threat of easy production of non-metallic knives.

In the near future many kinds of such home-made weapons could be manufactured by teenagers using their parent's 3D printer and instructions downloaded from the internet. A massive amount of new types of weapons in the streets can potentially interfere with the rule of law and order.

**Fake products**

Personal rapid prototyping machines can be used by criminals for cheap manufacturing of fake products, creating new income sources for criminal organizations, and violating property rights.

**Sources for technology description:**

The RepRap project:
http://reprap.org/bin/view/Main/WebHome

Video of a talk by Adrian Bowyer:

Fab@home project: http://fabathome.org/wiki/index.php?title=Main_Page


**Sources for threat indication:**

Plastic knives used to evade metal detectors
www.telegraph.co.uk/news/newstopics/politics/lawandorder/3628285/Plastic-knives-used-to-evade-metal-detectors.html

Is it possible to make an undetectable nonmetal gun?
www.straightdope.com/columns/read/1202/is-it-possible-to-make-an-undetectable-nonmetal-gun
www.keepshooting.com/selfdefense/knives/blackpolymer.htm

Chameleon Weapons Defy Detection
www.defensetech.org/archives/002265.html

**Description of this technology in the FESTOS expert survey:**

Currently developed 3D printers can construct products after downloading a detailed description form a computer. Researchers envision a printer that will be able to self-copy, at a cost of €500 (materials only), and to use a wide variety of materials.

(Potential threat: Possible use for constructing "home-made" weapons? Or undetectable weapons? Or cheap manufacturing of fake products?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>difficult (2.89)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.71)</td>
</tr>
</tbody>
</table>

Societal sphere potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>0%</td>
<td>57%</td>
<td>71%</td>
<td>29%</td>
<td>29%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases with time in the next 20. The most threatened societal sphere is infrastructures, followed by people. The impact on the environment and the economy is not negligible.
6. Programmable Matter

### Description:
Programmable matter is a matter which has the ability to change physical properties such as shape, density, optical properties, and others in a response to user input or autonomous sensing. In Science Fiction there are many examples for the theoretical idea (e.g. "Star Trek", "Terminator 2", "Kiln People"), but in reality since the early 1990's scientists suggested several concepts of programmable matter that could be realised. In 2000 the Science Fiction writer and aerospace engineer Will McCarthy described the following vision in the journal Nature: “4 July 2100. The flick of a switch: a wall becomes a window becomes a door. Any chair becomes a hyper-computer, any rooftop a power or waste-treatment plant. We scarcely notice; programmable matter pervades our homes, our workplaces, our vehicles and environments”.

DARPA is currently funding a research program on programmable matter. Carnegie Mellon's website describes one of the projects: "The goal of the claytronics project is to understand and develop the hardware and software necessary to create a material which can be programmed to form dynamic three dimensional shapes which can interact in the physical world and visually take on an arbitrary appearance". The visionary goal of DARPA's program is to create materials that can be programmed to self-assemble, alter their shape to perform a desired function, and then disassemble. Among the expected breakthroughs in this program are encoding information into chemistry, or fusing materials with machines, and fabrication of mesoscale particles with arbitrary complex shapes, composition, and function. Known also as “InfoChemistry”, this emerging field combines chemistry, information theory, and programmability to build information directly into materials.

Dr. M. R. Zakin, DARPA's program manager, described a science-fiction-like scenario to illustrate DARPA's expectations: “In the future a soldier will have something that looks like a paint can in the back of his vehicle. The can is filled with particles of varying sizes, shapes and capabilities. These individual bits can be small computers, ceramics, biological systems—potentially anything the user wants them to be. The soldier needs a wrench of a specific size. He broadcasts a message to the container, which causes the particles to automatically form the wrench. After the wrench has been used, the soldier realizes that he needs a hammer. He puts the wrench back into the can where it disassembles itself back into its components and re-forms into a hammer.” That is the essence of programmable matter, according to Zakin. It means distributing processing capabilities throughout the material: “You're blurring the distinction between materials and machines. Materials act like computers and communications systems, and communications systems and computers act like materials”.

Such technological developments, if achieved, will have tremendous impact on our lives. The DARPA project is aimed at defense applications, but the research (carried out in leading universities like Harvard, MIT and Cornell) has high potential for important civil applications ranging from aerospace to medicine. Morphing materials can be used to change an aircraft’s wings in flight or in clothing that alters its characteristics to keep users cool in the day and warm at night. One of the possible future directions is programming adaptability into the material itself. Such adaptability, for example, could produce electronic devices that can adapt to heat and dust in the desert and then shift to resist humidity and moisture in a jungle environment.

Other interesting program is run by Intel, and according to their website "The malleable stuff could mimic the shape and appearance of a person or object being imaged in real time, and as the
originals moved, so would their replicas. These 3D models would be physical entities, not holograms. You could touch them and interact with them, just as if the originals were in the room with you.”

**Potential threat indications:**
If the visionary technological capabilities of programmable matter are achieved, such technology can be used by terrorists and criminal groups for example in order to create new types of weapons that can pass security checks at airports. Those weapons can be programmed to look like ordinary items, and then change their properties after boarding the airplane, for example transforming into a knife. In fact, it will enable a perfect camouflage of any object. Moreover, it would enable reconfigurable tools with perfect performance, including weapons, readily adaptable to changing conditions and mission requirements.

**Sources for technology description:**
www.nature.com/nature/journal/v407/n6804/full/407569a0.html

DARPA’s Programmable Matter Initiative, 25 August 2009,

Programmable Matter Research Solidifies: Signal Magazine, June 2009,
www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1964&zoneid=263

DARPA Wants a Shapeshifter
www.wired.com/dangerroom/2007/03/darpa_wants_a_s/

Universal ‘Rubik’s Cube’ Could Become Pentagon Shapeshifter

Intel teases shape-shifting programmable matter

**Description of this technology in the FESTOS expert survey:**

Materials that can be programmed to self-assemble, alter their shape and physical properties to perform a desired function, and then disassemble - in response to user input or autonomous sensing. Known also as “InfoChemistry”, this emerging field combines chemistry, information theory, and programmability to build information directly into materials.

(Potential threats: Could one imagine malicious use of easily reconfigurable tools with perfect performance, including weapons (that can pass security checks at airports), readily adaptable to changing conditions and requirements?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2030</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>difficult (2.29)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.79)</td>
</tr>
</tbody>
</table>

Interpretation:

The threat likelihood increases with time in the next 20 years or so. The most threatened societal spheres are people and infrastructures, followed to a lesser degree by the environment and the economy.

New materials: overall assessment

Many of the new materials technologies will mature in the coming first and second decades. They might result in significant future threats to several societal spheres. The societal spheres potentially threatened vary from one technology to the other. Most spheres might be sensitive to these new capabilities. Values are the least affected sphere with zero score in several cases. The threat likelihood over time in some cases shows a direction change in the third decade, from increase to decrease, hinting that probably protection and countermeasures will be available.
Chapter 8. Converging Technologies

8.1 Converging Technologies: Introductory Overview

Science and engineering are the primary drivers of global technological competition. Unifying science based on the unifying features of nature at the nanoscale provides a new foundation for knowledge, innovation, and integration of technology. Revolutionary and synergistic advances at the interfaces between previously separated fields of science, engineering and areas of relevance are poised to create Nano-Bio-Info-Cogno (NBIC) transforming tools, products and services.

The importance of the concept of converging technologies stems from the fact that Info technologies, biotechnologies, and nanotechnologies complement each other and have already begun to join forces with cognitive science. Synergism is also possible with social psychology and other social sciences. This convergence promises to transform every aspect of life. Current convergence at the nanoscale is happening due to the use of the same elements of analysis (that is, atoms and molecules) and of the same principles and tools, as well as the ability to make cause-and-effect connections from simple components to higher-level architectures.

A new challenge is building systems from the nanoscale that will require the combined use of nanoscale laws, biological principles, information technology, and system integration. Then, after 2020, one may expect divergent trends as a function of the system architecture. Several possible divergent trends are system architectures based on: guided molecular and macromolecular assembling; robotics; biomimetics; and evolutionary approaches.

The transforming effect of NBIC convergence on society is expected to be large, not only because of the high rate of change in each domain and their synergism with global effects on science and engineering, but also because we are reaching qualitative thresholds in the advancement of each of the four domains Nano, Bio, Info, Cogno.

The convergence is on the broad scale (including anthropology, environment, up to social studies), but the most dynamic component driving an accelerating path of change is the convergence of nanotechnology, modern biology, and the digital revolution. With proper attention to ethical issues and societal needs, these converging technologies could lead to a tremendous improvement in human abilities, societal outcomes, national productivity levels, and the quality of life – all enabled by revolutionary products and services. At the same time the converging tools make

---


32 Coherence and Divergence in Megatrends in Science and Engineering, 1999-2000 (Roco, 1999); Converging Technologies for Improving Human Performance (Roco and Bainbridge, 2003)
threats available and easy to create based on the utilization or misuse of these advanced technologies.

There are several reasons for the current interest in Converging Technologies. First, the fundamental knowledge of matter. Until now, we have known much less about the intermediate nanoscale. The basic properties and functions of material structures and systems are now defined and, more importantly, can be changed as a function of the organization of matter via 'weak' molecular interactions (such as hydrogen bonds, electrostatic dipole, van der Waals forces, various surface forces, electro-fluidic forces, etc.). The intellectual drive toward smaller dimensions was accelerated by the discovery of size-dependent novel properties and phenomena. However, we cannot yet visualize or model with proper spatial and temporal accuracy a chosen domain of engineering or biological relevance at the nanoscale. We are still at the beginning of this road.

A second reason for the interest in Converging Technologies is the promise for fundamentally new applications. Possible examples include chemical manufacturing using designed molecular assemblies, processing information using photons or electron spin, detecting chemicals or bioagents using only a few molecules, detecting and treating chronic illnesses by sub-cellular interventions, regenerating tissue and nerves, enhancing learning and other cognitive processes by understanding the “society” of neurons. Finally, a third reason for the interest is the fast pace of industrial prototyping and commercialization and the fact that governments around the world are pushing to develop Converging Technologies as rapidly as possible. Coherent, sustained R&D programs in the field have been announced by the U.S (the first and largest such program), Japan, Korea, EC, Germany, China, Taiwan, and others.

Converging science and engineering from the nanoscale might establish a mainstream pattern for applying and integrating nanotechnology with biology, electronics, medicine, learning and other fields. It includes hybrid manufacturing, neuromorphic engineering, artificial organs, expanding life span, enhancing learning and sensorial capacities. Science and engineering of nanobiosystems will become essential to human healthcare and biotechnology. The functions of the brain and nervous system are expected to be measured with relevance to cognitive engineering.

Life-cycle sustainability and biocompatibility might be pursued in the development of new products. Knowledge development in nanotechnology will lead to reliable safety rules for limiting unexpected environmental and health consequences of nanostructures. Control of contents of nanoparticles will be performed in air, soils and waters using a national network. The capabilities of Converging Technologies for systematic control and manufacture at the nanoscale are envisioned to evolve into “heterogeneous molecular nanosystems”, where each molecule in the nanosystem has a specific structure and plays a different role. Molecules will be used as devices and fundamentally new functions will emerge from their engineered structures and architectures. Designing new atomic and molecular assemblies is expected to increase in importance, including macromolecules “by design”, nanoscale machines, and directed and multi-scale self-assembling, exploiting quantum control, nanosystem biology for healthcare, human-machine interface at the tissue and nervous system level. Research will include topics such as: atomic manipulation for design of molecules and supramolecular systems, controlled interaction between light and matter with relevance to energy conversion among others, exploiting quantum control mechanical-chemical molecular processes, nanosystem biology for
healthcare and agricultural systems, and human-machine interface at the tissue and nervous system level. Other topics include:

- Energy conversion - photovoltaic conversion and direct conversion of thermal to electric energy are expected to be developed.
- Water filtration and desalination - using nanotechnology has a high promise, even though only scarce efforts are underway.
- Nano-informatics – specific databases and methods for characterizing and using of nanocomponents, materials and processes integrated at the nanoscale. Such databases might interface with existing knowledge and data sets and tools such as bio-informatics, human and plant genome.

The convergence of tools and know how will shorten the lead time to a wide range of products, applications and knowledge that will be available to all. Solutions and products will emerge for a wide area of applications: commodities, healthcare, as well as homeland security and military applications. These know how and available tools could be harmful in the hands of those who manipulate, misuse and/or abuse existing applications or utilize these technologies differently.

In the following pages we describe selected converging technologies, along with the assessment of their potential threats based on the FESTOS expert survey.
8.2 Selected Converging Technologies and associated potential threats

1. Nanotechnology-enabled brain implants

<table>
<thead>
<tr>
<th>S&amp;T Field: Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>Cognition</td>
</tr>
</tbody>
</table>

**Description:**

Various biomedical devices implanted in the central nervous system, so-called neural interfaces, already have been developed to control motor disorders or to translate willful brain processes into specific actions by the control of external devices. These implants could help increase the independence of people with disabilities by allowing them to control various devices with their thoughts (other candidate for early adoption of this technology is the military). Scientists at the University of Michigan have recently developed a nanotech coating for brain implants that helps the devices operate longer and could improve treatment for various diseases. In another recent research, scientists at the Lawrence Livermore National Laboratory have sealed silicon-nanowire transistors in a membrane similar to those that surround biological cells. These hybrid devices, which operate similarly to nerve cells, might be used to make better interfaces for prosthetic limbs, cochlear implants, and maybe also for brain implants.

The potential of nanotechnology application in neuroscience is widely accepted. Single-walled carbon nanotubes (SWCNT) have received great attention because of their unique physical and chemical features. Scientists have already developed a SWCNT/neuron hybrid system and demonstrated that carbon nanotubes can directly stimulate brain circuit activity. Thanks to the application of recent advances in nanotechnology to the nervous system, a novel generation of neuro-implantable devices is on the horizon, capable of restoring function loss as a result of neuronal damage or altered circuit function. The EU FP6 Neuronano project develops neuronal nano-engineering mainly by integrating carbon nanotubes with multi electrode array technology. The aim is a new generation biochips to help repair damaged central nervous system tissues.

Many safety and ethical issues have been raised in relation to brain implants. Like other brain-implants, implants with nano-elements may pose difficult problems regarding possible personality changes in the person. Important debates deals with the potential use of brain implants not for medical treatment but for enhancement of the brain functions of healthy persons, including "upgrading" of mental capabilities.

According to Andy Clark, a pro-enhancement philosopher at the University of Edinburgh in the UK, brain enhancements by 'clip-on' computer aids may soon become available for all. These could be anything from memory aids to the ability to "search" for information stored in your brain. "We'll get a flowering of brain augmentations, some seeping through from the disabled community," he says.

Such possibilities (even more than other visionary human enhancements) raise concerns that if radically improved brain capacities become reality in the (far?) future, humanity might split up in different "sub-species" which could even have difficulties understanding each other. Such consequences would challenge widely accepted basic principles of equality, autonomy and even non-violence.

According to a UK MOD think tank report:

*By 2035, an implantable information chip could be developed and wired directly to the user’s brain. Information and entertainment choices would be accessible through cognition and might...*
include synthetic sensory perception beamed direct to the user's senses".

### Potential threat indications:

If abused, enhancing brain implants could be used for thought/behaviour control of people, "brainwashing", causing social unrest, violence, etc. It could also equip criminals or terrorists with "super mental power".

### Sources for technology description:

Nanotechnology coming to a brain near you: www.nanowerk.com/spotlight/spotid=2177.php
Neuronano project: www.neuronano.net

### Sources for threat indication:


"Will designer brains divide humanity?", New Scientist, issue 2708, 13 May 2009

### Sources for relevant Foresight:


### Description of this technology in the FESTOS expert survey:

Biomedical **neural interface** devices implantable in the central nervous system have been developed to control motor disorders or to control prosthetic limbs or external devices. Scientists have demonstrated a direct stimulation of brain activity by a carbon-nanotube/neuron hybrid system. Future brain implants could be used for enhancement of the brain functions of healthy persons. According to a UK MOD think tank report: "By 2035, an implantable information chip could be developed and wired directly to the user's brain. Information and entertainment choices would be accessible through cognition and might include synthetic sensory perception beamed direct to the user's senses".

(Potential threat: Does this imply possible technological means for thought/behaviour control of people, or equipping future perpetrators with "super mental power"?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2030</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (2.73)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (3.07)</td>
</tr>
</tbody>
</table>

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Societal Sphere</th>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>67%</td>
<td>33%</td>
<td>93%</td>
<td>13%</td>
<td>20%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood rises with time. The most threatened societal sphere is people. As could be expected in such a sensitive topic, the experts foresee a very significant impact on values.
2. Brain-to-brain communication ("Radiotelepathy")

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cognition</td>
</tr>
</tbody>
</table>

**Description:**

Advances in brain-computer interface (BCI) may lead to so-called "radiotelepathy" or "synthetic telepathy", enabled by direct conversion of neural signals into radio signals and vice versa, and the placement of micro/nano radio transmitters and receivers within the tissue of a living brain. The famous physicist Freeman Dyson has estimated that a system of $10^5$ tiny transmitters inside a brain could observe and transmit in detail the activity of an entire human brain.

A step in this direction was taken in 2008, when a team of UC Irvine scientists has been awarded a $4$ million grant from the U.S. Army Research Office "to study the neuroscientific and signal-processing foundations of synthetic telepathy". According to news release of the university, "The brain-computer interface would use a non-invasive brain imaging technology like EEG to let people communicate thoughts to each other. For example, a soldier would “think” a message to be transmitted and a computer-based speech recognition system would decode the EEG signals. The decoded thoughts, in essence translated brain waves, are transmitted using a system that points in the direction of the intended target".

A British defense think-tank report envisages microchips that could be connected to brains, allowing for "synthetic sensory perception beamed directly to the user’s senses." According to the report, this technology could be used to download any amount of information, and could be used for communication, allowing for a sort of "computer-aided telepathy".

**Potential threat indications:**

Freeman Dyson speculated that Radiotelepathy could become powerful instrument of social change, used either for good or for evil purposes. It could foster mutual understanding and peaceful cooperation of humans all over the planet, or lead to tyrannical oppression and "enforced hatred" between different societies. One may envision "enforcing violence", advanced form of "brainwashing", etc.

According to a report by a think tank of the UK MOD:

"By 2035, an implantable information chip could be developed and wired directly to the user’s brain. Information and entertainment choices would be accessible through cognition and might include synthetic sensory perception beamed direct to the user’s senses. Wider related ICT developments might include the invention of synthetic telepathy, including mind-to-mind or telepathic dialogue. This type of development would have obvious military and security, as well as control, legal and ethical, implications."

**Sources for technology description:**

F. Dyson, "Radiotelepathy", the direct communication of feelings and thought from brain to brain, www.edge.org/q2009/q09_3.html

UC Irvine news release: “Scientists to study synthetic telepathy”

**Sources for threat indication:**

DCDC Global Strategic Trends (2006), UK MOD
www.dcdc-strategictrends.org.uk/viewdoc.aspx?doc=1

F. Dyson, "Radiotelepathy", the direct communication of feelings and thought from brain to brain,
www.edge.org/q2009/q09_3.html

UC Irvine news release: "Scientists to study synthetic telepathy"

Drummond, Katie : Pentagon Preps Soldier Telepathy Push,

Description of this technology in the FESTOS expert survey:
Advances in brain-computer interface (BCI) may lead to so-called "radiotelepathy" enabled by direct conversion of neural signals into radio signals and vice versa. In a US army-funded project, scientists at the University of California "study the neuroscientific and signal-processing foundations of synthetic telepathy".

(Potential threat: According to a report by a think tank of the UK MOD: "ICT developments might include the invention of synthetic telepathy [that] would have obvious military and security, as well as control, legal and ethical, implications."

FESTOS experts survey results:

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2030</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>difficult (2.25)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (2.56)</td>
</tr>
</tbody>
</table>

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>70%</td>
<td>60%</td>
<td>100%</td>
<td>10%</td>
<td>10%</td>
<td>40%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases with time. The most threatened societal spheres are people and values. No doubt there is an alert regarding future threat to values as we know them today.
### 3. Brain-Computer Interface – "Mind Reading" commercial gadgets

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

**Description:**

This entry is closely related to the previous one (Brain Machine Interfaces), but it focuses on already commercially available (or almost available) gadgets, which, in our opinion, deserves special attention.

There have been many advances in the area of neural interfaces, which have led to first commercial products. For example, researchers at the University of Wisconsin’s Neural Interfaces lab and other labs around the world have demonstrated systems that enable people with disabilities to operate Internet services such as Twitter, "by thought.”

The EPOC headset marketed by EMOTIV Systems is claimed to be the first Brain Computer Interface (BCI) device for the gaming market. The idea is to operate games by "thought control". The EPOC detects and processes real time brain activity patterns (small voltage changes in the brain caused by the firing of neurons) using a device that measures electric activity in the brain. This novel gadget has been met with excitement amongst many gamers. Emotiv's president, Tan Le, said that "BCI is undoubtedly the future for video games". Californian company NeuroSky has built a device that can detect emotions: the firm says it can tell whether you are focused, relaxed, afraid or anxious, for example. The firm is licensing its set-up to other companies, including Mattel, Nokia and Sega. Mattel plans to sell a game which involves players levitating a ball "using thought alone."

Toyota announced in June 2009 that it has developed a way of steering a wheelchair by detecting brain waves: The user wears a cap that can read brain signals, which are relayed to a brain scan electroencephalograph (EEG) on the electrically powered wheelchair, and then analyzed in a computer program.

**Potential threat indications:**

The threats are similar to those mentioned earlier in the entry on Brain Machine Interface. Naturally, the commercial availability raises more immediate concerns. One may consider a distortion in the double-way communication between users and the gadgets.

Such developments are potentially very attractive for hackers, and possibly other criminals and terrorists as well. Hacking such a device could enable influencing the user's actions, perhaps even thoughts. One expert interviewed by CNN said: "So add that up: a wireless, remote, brain reading/writing device that can scan, interpret, and communicate with someone across the room, without them even knowing it. Connect that to the Internet... and talk about brainwashing possibilities. What if some hacker could figure out how to write viruses to people's brains? It's actually a little scary."

"Neural devices are innovating at an extremely rapid rate and hold tremendous promise for the future," said computer security expert Tadayoshi Kohno of the University of Washington. "But if we don't start paying attention to security, we're worried that we might find ourselves in five or 10 years saying we've made a big mistake." What would happen if hackers start focusing on neural devices, such as the deep-brain stimulators currently used to treat Parkinson's and depression, or electrode systems for controlling prosthetic limbs? According to Kohno and his colleagues, who published their concerns July 1 in *Neurosurgical Focus*, most current devices carry few security risks. But as neural engineering becomes more complex and more
widespread, the potential for security breaches will mushroom. A recent article in Wired adds: “Some might question why anyone would want to hack into someone else’s brain, but the researchers say there’s a precedent for using computers to cause neurological harm. In November 2007 and March 2008, malicious programmers vandalized epilepsy support websites by putting up flashing animations, which caused seizures in some photo-sensitive patients.

**Sources for technology description:**

http://emotiv.com/


"Toyota technology has brain waves move wheelchair": www.physorg.com/news165487826.htm

"Twitter Telepathy: Researchers Turn Thoughts Into Tweets": www.wired.com/wiredscience/2009/04/braintweet

**Sources for threat indication:**


"Innovation: Mind-reading headsets will change your brain": www.newscientist.com/article/dn17009-innovation-mindreading-headsets-will-change-your-brain.html


"Hackers Assault Epilepsy Patients via Computer" www.wired.com/politics/security/news/2008/03/epilepsy

**Description of this technology in the FESTOS expert survey:**

Researchers have demonstrated systems that enable people with disabilities to operate Internet services such as Twitter, "by thought." The EPOC headset marketed by EMOTIV Systems is claimed to be the first Brain Computer Interface (BCI) device for the video gaming market. Toy manufacturers plan to sell a game which involves players levitating a ball "using thought alone." Toyota has developed a wheelchair steered by detecting brain waves.

(Potential threat: Could one speculate on malicious distortion in the double-way communication between users and the gadgets? Could hacking such a device enable influencing the user’s actions?)
FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>When will this technology be sufficiently mature to be used in practice?</td>
<td>2023</td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>difficult (2.33)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>low severity (2.42)</td>
</tr>
</tbody>
</table>

![Graph showing the likelihood to pose a security threat](graph.png)

**Societal spheres potentially threatened:**

<table>
<thead>
<tr>
<th>Societal Sphere</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values</td>
<td>50%</td>
</tr>
<tr>
<td>Political systems</td>
<td>33%</td>
</tr>
<tr>
<td>People</td>
<td>100%</td>
</tr>
<tr>
<td>Infrastructures</td>
<td>17%</td>
</tr>
<tr>
<td>Environment</td>
<td>8%</td>
</tr>
<tr>
<td>Economy</td>
<td>8%</td>
</tr>
</tbody>
</table>

**Interpretation:**
The threat likelihood is constant in time. The most threatened societal sphere is people. It is important to note the very high impact on values. Political systems could be affected too.
4. Cyborg Insects

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

**Description:**

Engineers are creating insects that can be controlled through electronics by implanting electrical stimulators that zap certain nerves or brain cells to trigger an impulse to move in the desired direction. The insects, which can be controlled by remote control or a pre-programmed chip, may soon be able to generate the electricity required to control them, prolonging their controllable life span.

A DARPA project aims to co-opt the way some insects communicate to give early warning of chemical attacks, locating disaster victims, monitoring for pollution and gas leaks, etc. Researchers have already created "insect cyborgs" by implanting them with electrodes to control their wing muscles. They plan is to create living communication networks by implanting a package of electronics in crickets, cicadas or katydids - all of which communicate via wing-beats. The implants will cause the insects in these OrthopterNets to modulate their calls in the presence of certain chemicals. The firm OpCoast, based in New Jersey, has been awarded a contract to develop a mobile communications network for insects. The electronics package can contain an acoustic sensor designed to respond to the altered calls of other insects. This should ensure the "alarm" signal is passed quickly across the network and is ultimately picked up by ground-based transceivers. Each network is likely to use hundreds or thousands of insects, though they could be spread far apart.

Early attempts in this area have been made in Japan in 2001, when researchers at Tokyo University unveiled the world's first electronically-guided cockroach. This so-called "Robo-roach", surgically implanted with a micro-robotic backpack that allowed controlling its movements. Working under a $5m grant from the Japanese government, the scientists have managed to implant tiny microchip backpacks onto the insects allowing them to be controlled with a remote handset. The pulse-emitting backpack sends signals to the host cockroach through electrodes, causing it to turn left, right, run forward or back.

The Japanese researchers envisioned then that within a few years similarly controlled insects will be carrying mini-cameras or other sensory devices to be used for a variety of sensitive missions - like crawling through earthquake rubble to search for victims or slipping under doors on espionage. One of the ideas for applications was creating "cyber locust" to protect agriculture from locusts (diverting the locust swarms by a "cyber locust").

One can imagine how advanced features in cyber-insects can be achieved with present and future capabilities offered by micro/nano technologies.

**Potential threat indications:**

Cyber-insects can be used also for harmful effects, in addition to obvious surveillance or espionage missions.

For example, swarms of insects may be directed at population areas; the insects may be bred for harmful purposes e.g. to transmit disease or to damage crops.
Sources for technology description:
"Cyborg crickets could chirp at the smell of survivors", New Scientist, 11 July 2009:
www.newscientist.com/article/mg20126884.200-cyborg-cockroaches-could-power-own-electric-brains.html
www.guardian.co.uk/Archive/Article/0,4273,4321358,00.html

Sources for threat indication:

Description of this technology in the FESTOS expert survey:
Insects controlled through implanted electrical stimulators. By connecting electrodes and radio antennas to the nervous systems of insects, researchers were already able to make them take off, dive and turn on command. Researchers envision living communication networks (for sensing, surveillance, etc) by implanting electronics in insects. Advanced capabilities could be offered by micro/nano technologies.

(Potential threat: Could cyborg insects be used by perpetrators for harming people, spying or other malicious activities?)

FESTOS experts survey results:

<table>
<thead>
<tr>
<th>When will this technology be sufficiently mature to be used in practice?</th>
<th>2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td>somewhat difficult (3.33)</td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td>medium severity (3.08)</td>
</tr>
</tbody>
</table>

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>17%</td>
<td>8%</td>
<td>92%</td>
<td>92%</td>
<td>67%</td>
<td>42%</td>
</tr>
</tbody>
</table>

Interpretation:
The threat likelihood increases with time. The most threatened societal spheres are people and infrastructures, followed by a considerable impact on the environment and the economy.
5. Human enhancement

<table>
<thead>
<tr>
<th>S&amp;T Field:</th>
<th>Nanotech</th>
<th>Biotech</th>
<th>ICT</th>
<th>Robotics</th>
<th>New Materials</th>
<th>Converging Technologies</th>
<th>Other</th>
</tr>
</thead>
</table>

Description (as presented in the expert survey):

NBIC, the convergence of nano, bio, info technologies and new technologies based on cognition science, offer potential for unprecedented enhancement of human performance: not only better health but alteration and augmentation of physical and mental abilities, and drastic life extension. Fast interface between the human brain and machines may transform work, ensure military superiority, and enable new modes of interaction between people. Some envision even that human and machine intelligence will converge over the coming century (the Cyborg vision).

Potential threat indications (as presented in the expert survey):

Are such drastic changes threatening the human species, as some experts warn? Could specific changes be ill-used by perpetrators?

Sources for technology description:
Human enhancement study, European Parliament, STOA report, 2007

FESTOS experts survey results:

<table>
<thead>
<tr>
<th>Question</th>
<th>2030</th>
<th>Somewhat difficult (2.63)</th>
<th>Medium severity (3.13)</th>
</tr>
</thead>
<tbody>
<tr>
<td>When this technology be sufficiently mature to be used in practice?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How easy will it be to use this technology for malicious purposes that might pose security threats?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How severe is the potential security threat posed by this technology?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

likelihood to pose a security threat (from 1 - very unlikely, to 5 - very likely)

Societal spheres potentially threatened:

<table>
<thead>
<tr>
<th>Values</th>
<th>Political systems</th>
<th>People</th>
<th>Infrastructures</th>
<th>Environment</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>81%</td>
<td>69%</td>
<td>94%</td>
<td>38%</td>
<td>6%</td>
<td>38%</td>
</tr>
</tbody>
</table>

33 This topic was not included in the preliminary scanning (report D2.1)
Interpretation:
The threat likelihood increases with time. The most threatened societal spheres are people and values. The political systems are highly affected as well. The dramatic impact on values in such a sensitive topic should be stressed.

Converging Technologies: Overall Assessment

The main observation is that Converging Technologies will have a significant impact on values. Most technologies are expected to mature only after 2020, deep into the century. The likelihood of threats is increasing with time. People are the main sphere threatened. In certain cases the political system will be at risk which is also an important finding, more evident in the Converging Technologies field than in other fields.
Chapter 9. Technologies and potential threats – integrative assessment

In this chapter we present integrative results from the expert survey (for more details please see the expert survey report D2.2).

In the survey respondents were asked to assess each technology with regard to several aspects: Timing of maturity, easiness of malicious use, severity of threat, likelihood of posing a security threat (in different timeframes) and the most threatened societal spheres. They were also asked to indicate their level of knowledge about each technology: expert, knowledgeable, or familiar.

9.1 Maturity timeframes

For each technology the respondents were asked: "When will this technology be sufficiently mature to be used in practice?"

The following explanation was provided: "Sufficiently mature": The technology was at least demonstrated and validated outside the laboratory, through testing of prototypes. (This is similar to TRL-5 or higher, on the "Technology Readiness Scale" used in many technology assessment studies)

Table 9.1 and Figure 9.1 describe the distribution of the estimated time of maturity for the various technologies covered by the expert survey. The time frame spans from 2010 to 2035. The stars in Fig. 9.1 mark the median year, which is usually considered in such surveys as "the most probable year" (in our case, the most probable year in which each technology will be sufficiently mature to be used in practice).

The column "later or never" indicates the percentages of respondents that think that the specific technology under consideration will mature later than 2035, or will never practically mature. The column N presents the number of responses for each technology.

---

* Expert: Specialist knowledge in this area, through current/recent research work. Knowledgeable: Considerable knowledge in this area, through past work or current engagement in adjoining areas. Familiar: Knowledge based on reading relevant publications or listening to experts.
Table 9.1: Maturity timeframes – detailed distribution of responses

<table>
<thead>
<tr>
<th>Technology</th>
<th>Now - 2015</th>
<th>2016 - 2020</th>
<th>2021 - 2025</th>
<th>2026 - 2035</th>
<th>Later or never</th>
<th>median</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet of Things</td>
<td>33.3%</td>
<td>50.9%</td>
<td>10.5%</td>
<td>1.8%</td>
<td>3.5%</td>
<td>2018</td>
<td>57</td>
</tr>
<tr>
<td>RFID</td>
<td>72.2%</td>
<td>13.9%</td>
<td>5.6%</td>
<td>2.8%</td>
<td>5.6%</td>
<td>2012</td>
<td>36</td>
</tr>
<tr>
<td>Smart mobile</td>
<td>84.4%</td>
<td>12.5%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>3.1%</td>
<td>2012</td>
<td>32</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>84.4%</td>
<td>15.6%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>2012</td>
<td>32</td>
</tr>
<tr>
<td>Ultra-dense data storage</td>
<td>26.3%</td>
<td>63.2%</td>
<td>10.5%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>2018</td>
<td>19</td>
</tr>
<tr>
<td>Artificial Intelligence</td>
<td>27.7%</td>
<td>21.3%</td>
<td>19.1%</td>
<td>14.9%</td>
<td>17.0%</td>
<td>2018</td>
<td>47</td>
</tr>
<tr>
<td>AI-based robot-human interaction</td>
<td>15.8%</td>
<td>21.1%</td>
<td>42.1%</td>
<td>5.3%</td>
<td>15.8%</td>
<td>2023</td>
<td>10</td>
</tr>
<tr>
<td>Autonomous toy robots</td>
<td>28.6%</td>
<td>57.1%</td>
<td>0.0%</td>
<td>7.1%</td>
<td>7.1%</td>
<td>2018</td>
<td>14</td>
</tr>
<tr>
<td>Artificial limbs</td>
<td>22.2%</td>
<td>55.6%</td>
<td>11.1%</td>
<td>11.1%</td>
<td>0.0%</td>
<td>2018</td>
<td>9</td>
</tr>
<tr>
<td>Ethical control of robots</td>
<td>14.3%</td>
<td>28.6%</td>
<td>14.3%</td>
<td>14.3%</td>
<td>28.6%</td>
<td>2023</td>
<td>7</td>
</tr>
<tr>
<td>Swarm robotics</td>
<td>0.0%</td>
<td>22.2%</td>
<td>11.1%</td>
<td>66.7%</td>
<td>0.0%</td>
<td>2030</td>
<td>9</td>
</tr>
<tr>
<td>Molecular manufacturing</td>
<td>10.0%</td>
<td>20.0%</td>
<td>40.0%</td>
<td>10.0%</td>
<td>20.0%</td>
<td>2023</td>
<td>10</td>
</tr>
<tr>
<td>Self-replicating nanoassemblers</td>
<td>0.0%</td>
<td>16.7%</td>
<td>8.3%</td>
<td>33.3%</td>
<td>41.7%</td>
<td>2030</td>
<td>12</td>
</tr>
<tr>
<td>Medical nanorobots</td>
<td>9.1%</td>
<td>9.1%</td>
<td>0.0%</td>
<td>54.5%</td>
<td>27.3%</td>
<td>2030</td>
<td>11</td>
</tr>
<tr>
<td>Tailored nanoparticles</td>
<td>57.9%</td>
<td>42.1%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>2012</td>
<td>19</td>
</tr>
<tr>
<td>Energetic nanomaterials</td>
<td>28.6%</td>
<td>50.0%</td>
<td>7.1%</td>
<td>0.0%</td>
<td>14.3%</td>
<td>2018</td>
<td>14</td>
</tr>
<tr>
<td>Molecular nanosensors</td>
<td>46.2%</td>
<td>38.5%</td>
<td>7.7%</td>
<td>7.7%</td>
<td>0.0%</td>
<td>2018</td>
<td>13</td>
</tr>
<tr>
<td>Brain implants</td>
<td>0.0%</td>
<td>13.3%</td>
<td>20.0%</td>
<td>40.0%</td>
<td>26.7%</td>
<td>2030</td>
<td>15</td>
</tr>
<tr>
<td>Brain-to-Brain</td>
<td>0.0%</td>
<td>11.1%</td>
<td>0.0%</td>
<td>66.7%</td>
<td>22.2%</td>
<td>2030</td>
<td>9</td>
</tr>
<tr>
<td>Cyborg insects</td>
<td>15.4%</td>
<td>30.8%</td>
<td>30.8%</td>
<td>7.7%</td>
<td>15.4%</td>
<td>2023</td>
<td>13</td>
</tr>
<tr>
<td>Brain computer interface</td>
<td>25.0%</td>
<td>25.0%</td>
<td>25.0%</td>
<td>16.7%</td>
<td>8.3%</td>
<td>2023</td>
<td>12</td>
</tr>
<tr>
<td>Human enhancement</td>
<td>5.9%</td>
<td>17.6%</td>
<td>17.6%</td>
<td>47.1%</td>
<td>11.8%</td>
<td>2030</td>
<td>17</td>
</tr>
<tr>
<td>Metamaterials &amp; Optical Cloaking</td>
<td>4.0%</td>
<td>32.0%</td>
<td>8.0%</td>
<td>4.0%</td>
<td>52.0%</td>
<td>2030</td>
<td>25</td>
</tr>
<tr>
<td>Water catalyzing chemical reactions</td>
<td>4.0%</td>
<td>20.0%</td>
<td>24.0%</td>
<td>4.0%</td>
<td>48.0%</td>
<td>2030</td>
<td>25</td>
</tr>
<tr>
<td>Programmable matter</td>
<td>8.0%</td>
<td>16.0%</td>
<td>12.0%</td>
<td>16.0%</td>
<td>48.0%</td>
<td>2030</td>
<td>25</td>
</tr>
<tr>
<td>3-D printing</td>
<td>30.8%</td>
<td>19.2%</td>
<td>7.7%</td>
<td>15.4%</td>
<td>27.0%</td>
<td>2018</td>
<td>26</td>
</tr>
<tr>
<td>Future fuels</td>
<td>16.0%</td>
<td>8.0%</td>
<td>32.0%</td>
<td>4.0%</td>
<td>40.0%</td>
<td>2023</td>
<td>25</td>
</tr>
<tr>
<td>Crystalline polymers</td>
<td>34.6%</td>
<td>11.5%</td>
<td>26.9%</td>
<td>3.8%</td>
<td>23.0%</td>
<td>2023</td>
<td>26</td>
</tr>
<tr>
<td>Synthetic biology</td>
<td>15.4%</td>
<td>34.6%</td>
<td>23.1%</td>
<td>11.5%</td>
<td>15.4%</td>
<td>2018</td>
<td>26</td>
</tr>
<tr>
<td>DNA-protein interaction</td>
<td>19.0%</td>
<td>28.6%</td>
<td>19.1%</td>
<td>4.8%</td>
<td>28.6%</td>
<td>2023</td>
<td>21</td>
</tr>
<tr>
<td>Gene transfer</td>
<td>50.0%</td>
<td>25.0%</td>
<td>12.5%</td>
<td>0.0%</td>
<td>12.5%</td>
<td>2012</td>
<td>24</td>
</tr>
<tr>
<td>iPSC cells</td>
<td>5.9%</td>
<td>23.5%</td>
<td>29.4%</td>
<td>11.8%</td>
<td>29.4%</td>
<td>2023</td>
<td>17</td>
</tr>
<tr>
<td>Bio-mimicking for fluid mixing</td>
<td>13.3%</td>
<td>6.7%</td>
<td>13.3%</td>
<td>26.7%</td>
<td>40.0%</td>
<td>2030</td>
<td>15</td>
</tr>
</tbody>
</table>
Figure 9.1 – Maturity timeframes
The technologies under consideration can be roughly divided into four groups according to their estimated (median) time of maturity:

**Short term (now – 2015):**
Radio-frequency identification (RFID), smart mobile phone technologies mash-ups, cloud computing, tailored nanoparticles, and new gene transfer technologies.

**Medium term (2016 – 2025):**
Internet of things (IoT), ultra-dense data storage, advanced Artificial Intelligence, autonomous & semi-autonomous mini robots (toys and amateur objects), AI-based robot-human interaction and co-existence, ethical control of robots, robotic artificial limbs, energetic nanomaterials, molecular manufacturing, molecular nanosensors, future fuels, crystalline polymers, cyborg insects, personal rapid prototyping and 3-d printing machines, synthetic biology, DNA-protein interaction, Induced Pluripotent Stem Cells, Brain-Computer Interface ("Mind Reading" commercial gadgets),

**Long term (2026 - 2035):**
Self-replicating nanoassemblers, medical nanorobots, Nanotechnology-enabled brain implants, Human enhancement/augmentation based on NBIC convergence, Programmable matter, processes and structural materials for nuclear technologies, water catalysing explosive reactions, Bio-mimicking for fluids mixing at extremely small scales, metamaterials and "optical cloaking", swarm robotics.

From Table 9.1 it is evident that in some cases there is a significant difference between respondents' estimations of the maturity time. For instance, about 16% of the experts think that "AI-based robot-human interaction and co-existence", "synthetic biology" and "cyborg insects" will be sufficiently mature before 2015, while the same percentage of experts estimate that this will happen after 2035 (or never). Marked differences are also seen in other technologies, in particular "DNA-protein interaction", "iPC cells", and 3-D printing. In some cases the percentage of experts who think that the technology will mature after 2035 or never is very high, especially with regard to "metamaterials and optical cloaking" (52%), "programmable matter" (48%) and "water catalyzing chemical reactions" (48%).

Naturally, for many new and emerging technologies the uncertainty regarding their time of maturity is high and therefore significant disagreement between experts is not surprising. Such a gap might be narrowed in future survey rounds (such multi-round "Delphi" survey methodology is a common practice in foresight studies). We should also be cautious with respect to these findings in cases in which the number of responses was relatively low.

**9.2 Severity of Threat and Easiness of Use for Malicious Purposes**

The experts were asked to assess the severity of the potential threats of each technology on a scale of 1-5 (5 = most severe). Then they were asked how easy will it be to use each technology for malicious purposes (1=not easy at all, 5=very easy). It was explained in the questionnaire that "easy" means that the technology is easily available/affordable/adaptable or "disruptable", and that "malicious" refers mainly to
terrorism and crime. Columns A and B in the following table present the average values of experts' responses for each technology.

Evidently, some technologies are easy to use for malicious purposes but their actual threat is not very severe while others pose severe threat but are difficult to use (see also Fig.9.4 below).

A possibly useful way to rank the technologies is by using the combination (e.g. multiplication) of values A (easiness of malicious use) and B (severity of threat), which we interpret as the actual potential of abuse: see column C in Table 9.2. The technologies in Table 9.1 are ordered by their "potential of abuse" (column C) as reflected by the experts opinions, from the highest potential (smart mobile phone mash-ups) to the lowest potential (iPS cells). For more details regarding this method of ranking/prioritization please see the FESTOS deliverable D3.3: "Integrated Security Threats Report".

**Table 9.2: Severity of threats, easiness of malicious use, and potential of abuse**

<table>
<thead>
<tr>
<th>Technology</th>
<th>A: How easy will it be to use this technology for malicious purposes that might pose security threats?</th>
<th>B: How severe is the potential security threat posed by this technology?</th>
<th>C: Multiplication of A and B: Potential of abuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Smart mobile</td>
<td>3.69</td>
<td>3.49</td>
<td>12.88</td>
</tr>
<tr>
<td>2. IoT</td>
<td>3.61</td>
<td>3.49</td>
<td>12.60</td>
</tr>
<tr>
<td>3. Cloud computing</td>
<td>3.29</td>
<td>3.53</td>
<td>11.61</td>
</tr>
<tr>
<td>4. Gene transfer</td>
<td>3.52</td>
<td>3.22</td>
<td>11.33</td>
</tr>
<tr>
<td>5. Artificial intelligence</td>
<td>3.21</td>
<td>3.43</td>
<td>11.01</td>
</tr>
<tr>
<td>6. Synthetic biology</td>
<td>3.16</td>
<td>3.40</td>
<td>10.74</td>
</tr>
<tr>
<td>7. Cyborg insects</td>
<td>3.33</td>
<td>3.08</td>
<td>10.26</td>
</tr>
<tr>
<td>8. Energetic nanomaterials</td>
<td>3.00</td>
<td>3.33</td>
<td>9.99</td>
</tr>
<tr>
<td>9. RFID</td>
<td>3.14</td>
<td>3.03</td>
<td>9.51</td>
</tr>
<tr>
<td>10. Autonomous robots</td>
<td>3.36</td>
<td>2.83</td>
<td>9.51</td>
</tr>
<tr>
<td>11. AI robots</td>
<td>3.00</td>
<td>2.94</td>
<td>8.82</td>
</tr>
<tr>
<td>12. Swarm robotics</td>
<td>2.89</td>
<td>3.00</td>
<td>8.67</td>
</tr>
<tr>
<td>13. Water catalyzing</td>
<td>2.56</td>
<td>3.38</td>
<td>8.65</td>
</tr>
<tr>
<td>14. Brain implants</td>
<td>2.73</td>
<td>3.07</td>
<td>8.38</td>
</tr>
<tr>
<td>15. Ultra-dense</td>
<td>3.05</td>
<td>2.72</td>
<td>8.30</td>
</tr>
<tr>
<td>16. Human enhancement</td>
<td>2.63</td>
<td>3.13</td>
<td>8.23</td>
</tr>
<tr>
<td>17. Nanoassemblers</td>
<td>2.75</td>
<td>2.92</td>
<td>8.03</td>
</tr>
<tr>
<td>18. 3-D printing</td>
<td>2.89</td>
<td>2.71</td>
<td>7.83</td>
</tr>
<tr>
<td>19. Metamaterials</td>
<td>2.50</td>
<td>2.95</td>
<td>7.37</td>
</tr>
<tr>
<td>20. Tailored nanoparticles</td>
<td>2.53</td>
<td>2.89</td>
<td>7.31</td>
</tr>
</tbody>
</table>
Table 9.2 shows that according to the experts' opinion the following top 10 technologies are leading in terms of potential of abuse – they exhibit severe threat potential and could be rather easily used for malicious purposes:

- Smart mobile mash-ups
- Internet of things (IoT)
- Cloud computing
- Gene transfer
- Advanced AI
- Synthetic Biology
- Cyborg insects
- Energetic nanomaterials
- RFID
- Autonomous & Semi-Autonomous Mini Robots: Toys and Amateur Objects

These technologies should get thus special attention, in particular those which are expected to mature in the relatively near future.

It is interesting to present the severity of potential threats and the easiness of use for malicious purposes, versus the foreseen times of maturity. This is shown in Fig. 9.2 and 9.3 below.

In Fig. 9.4 we plot the severity of threat vs. easiness of malicious use. Comparing figures 9.2 and 9.3, one can see that some of the technologies are conspicuous in both figures: relatively mature technologies that pose high severity threat and are easy to use for malicious purposes.
Figure 9.2: Severity of threat vs. time of maturity
The technologies can be divided as follows into three groups by their severity of threat, based on the average severity values resulting from the survey:

**Low severity (1 – 2.5, bottom quartile):**

Robotic artificial limbs, ethical control of robots, molecular manufacturing, molecular nanosensors, brain-computer interface, crystalline polymers, iPS cells, and biomimicking for fluid mixing.

**Medium severity (2.51 – 3.355, 2\textsuperscript{nd} and 3\textsuperscript{rd} quartiles):**

Ultra-dense data storage, autonomous mini robots, medical nanorobots, brain-to-brain communication, programmable matter, tailored nanoparticles, personal rapid prototyping and 3-d printing, future fuels processes and materials for nuclear technologies, RFID, AI-based robot-human interaction, swarm robotics, nanoassemblers, energetic nanomaterials, brain implants, cyborg insects, human enhancement based on NBIC convergence, gene transfer, metamaterials with negative refraction index.

**High severity (3.356 – 5, top quartile):**

Internet of things (IoT), Smart mobile phone technologies mash-ups, cloud computing, advanced Artificial Intelligence, Water catalysing explosive reactions, Synthetic biology.
Figure 9.3: Easiness of use for malicious purposes vs. time of maturity
Figure 9.4: Severity of threat vs. easiness of malicious use
9.3 Likelihood to actually pose a security threat in the future

The experts were asked to assess the likelihood that each technology will actually come to pose a security threat, in different timeframes, from now till after 2035 (including the likelihood that the technology will never pose such threat). The likelihood was assessed on a scale of 1 to 5 (1= very unlikely, 5=very likely).

It should be noted (as explained in the questionnaire) that in certain cases a technology can be used for malicious purposes even before it is sufficiently mature to be used in practice for regular purposes. This might occur with technologies and products that are in a phase of prototype testing, are lacking safety regulations or do not comply with formal standards and so on.

The results (in terms of average likelihoods) are shown in Table 9.3 below.

In the subsequent figures 9.5 to 9.11 we map the severity of threats vs the likelihood to actually pose a threat, in the different time-frames under consideration.
### Table 9.3 Likelihood of posing a threat in different time intervals

<table>
<thead>
<tr>
<th>Technology</th>
<th>Now-2015</th>
<th>2016-2020</th>
<th>2021-2025</th>
<th>2026-2035</th>
<th>After 2035</th>
<th>Never</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT</td>
<td>2.57</td>
<td>3.11</td>
<td>3.6</td>
<td>3.51</td>
<td>3.23</td>
<td>1.46</td>
<td>54</td>
</tr>
<tr>
<td>RFID</td>
<td>2.75</td>
<td>3.06</td>
<td>3.18</td>
<td>3.03</td>
<td>3</td>
<td>2</td>
<td>36</td>
</tr>
<tr>
<td>Smart mobile</td>
<td>3.06</td>
<td>3.33</td>
<td>3.44</td>
<td>3.15</td>
<td>2.96</td>
<td>2.08</td>
<td>31</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>3</td>
<td>3.1</td>
<td>3.14</td>
<td>3.04</td>
<td>2.89</td>
<td>1.78</td>
<td>32</td>
</tr>
<tr>
<td>Ultra-dense</td>
<td>1.83</td>
<td>2.5</td>
<td>2.88</td>
<td>3.12</td>
<td>3.24</td>
<td>2.15</td>
<td>18</td>
</tr>
<tr>
<td>Artificial intelligence</td>
<td>2.07</td>
<td>2.56</td>
<td>3.13</td>
<td>3.43</td>
<td>3.71</td>
<td>1.71</td>
<td>46</td>
</tr>
<tr>
<td>AI robots</td>
<td>1.59</td>
<td>2</td>
<td>2.25</td>
<td>2.65</td>
<td>2.94</td>
<td>1.46</td>
<td>17</td>
</tr>
<tr>
<td>Autonomous robots</td>
<td>1.71</td>
<td>2.36</td>
<td>3.07</td>
<td>3.14</td>
<td>3.36</td>
<td>1.67</td>
<td>14</td>
</tr>
<tr>
<td>Artificial limbs</td>
<td>1.22</td>
<td>2.22</td>
<td>2.67</td>
<td>2.78</td>
<td>2.67</td>
<td>2.25</td>
<td>9</td>
</tr>
<tr>
<td>Ethical control</td>
<td>1.57</td>
<td>1.86</td>
<td>1.86</td>
<td>1.71</td>
<td>2</td>
<td>1.67</td>
<td>7</td>
</tr>
<tr>
<td>Swarm robotics</td>
<td>1.33</td>
<td>1.44</td>
<td>1.89</td>
<td>2.56</td>
<td>2.89</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Molecular manufacturing</td>
<td>1.38</td>
<td>1.88</td>
<td>2.44</td>
<td>3</td>
<td>3</td>
<td>2.25</td>
<td>9</td>
</tr>
<tr>
<td>Nanoassemblers</td>
<td>1.1</td>
<td>1.1</td>
<td>1.67</td>
<td>2.11</td>
<td>2.73</td>
<td>2.43</td>
<td>11</td>
</tr>
<tr>
<td>Medical nanorobots</td>
<td>1</td>
<td>1.25</td>
<td>1.78</td>
<td>2.44</td>
<td>3.11</td>
<td>1.63</td>
<td>9</td>
</tr>
<tr>
<td>Tailored nanoparticles</td>
<td>2.56</td>
<td>3.11</td>
<td>3.18</td>
<td>3.06</td>
<td>3.07</td>
<td>1.56</td>
<td>18</td>
</tr>
<tr>
<td>Energetic nanomaterials</td>
<td>2.2</td>
<td>2.91</td>
<td>3.3</td>
<td>3.9</td>
<td>3.78</td>
<td>1.17</td>
<td>11</td>
</tr>
<tr>
<td>Molecular nanosensors</td>
<td>1.38</td>
<td>1.88</td>
<td>2.44</td>
<td>3</td>
<td>3</td>
<td>2.25</td>
<td>9</td>
</tr>
<tr>
<td>Brain implants</td>
<td>1</td>
<td>1.64</td>
<td>2.07</td>
<td>2.46</td>
<td>2.85</td>
<td>1.56</td>
<td>15</td>
</tr>
<tr>
<td>Brain-to-Brain</td>
<td>1</td>
<td>1.11</td>
<td>1.44</td>
<td>2</td>
<td>2.56</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>Cyborg insects</td>
<td>1.42</td>
<td>2.38</td>
<td>2.92</td>
<td>3.08</td>
<td>3.17</td>
<td>1.2</td>
<td>13</td>
</tr>
<tr>
<td>Brain computer interface</td>
<td>1.7</td>
<td>1.9</td>
<td>2.11</td>
<td>2.2</td>
<td>2.22</td>
<td>1.2</td>
<td>12</td>
</tr>
<tr>
<td>Human enhancement</td>
<td>1.07</td>
<td>1.69</td>
<td>2.07</td>
<td>2.67</td>
<td>3.13</td>
<td>1.39</td>
<td>16</td>
</tr>
<tr>
<td>Metamaterials</td>
<td>1.21</td>
<td>1.99</td>
<td>2.56</td>
<td>3.33</td>
<td>3.82</td>
<td>1.39</td>
<td>19</td>
</tr>
<tr>
<td>Technology</td>
<td>1.44</td>
<td>2.01</td>
<td>2.69</td>
<td>2.94</td>
<td>3.58</td>
<td>1.81</td>
<td>17</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>Water catalyzing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programmable matter</td>
<td>1.51</td>
<td>1.95</td>
<td>2.41</td>
<td>3.14</td>
<td>3.40</td>
<td>2.27</td>
<td>17</td>
</tr>
<tr>
<td>3-D printing</td>
<td>2.13</td>
<td>2.68</td>
<td>3.18</td>
<td>3.53</td>
<td>3.56</td>
<td>1.49</td>
<td>20</td>
</tr>
<tr>
<td>Future fuels</td>
<td>1.47</td>
<td>2.07</td>
<td>2.78</td>
<td>3.38</td>
<td>3.71</td>
<td>1.76</td>
<td>17</td>
</tr>
<tr>
<td>Crystalline polymers</td>
<td>2.12</td>
<td>2.40</td>
<td>2.99</td>
<td>3.54</td>
<td>3.38</td>
<td>1.18</td>
<td>17</td>
</tr>
<tr>
<td>Synthetic biology</td>
<td>1.91</td>
<td>2.59</td>
<td>3.14</td>
<td>3.64</td>
<td>4.15</td>
<td>2.13</td>
<td>22</td>
</tr>
<tr>
<td>DNA protein</td>
<td>1.81</td>
<td>2.08</td>
<td>2.73</td>
<td>3.07</td>
<td>3.20</td>
<td>3.03</td>
<td>18</td>
</tr>
<tr>
<td>Gene transfer</td>
<td>2.23</td>
<td>2.94</td>
<td>3.41</td>
<td>3.41</td>
<td>3.47</td>
<td>2.38</td>
<td>22</td>
</tr>
<tr>
<td>iPS cells</td>
<td>1.21</td>
<td>1.31</td>
<td>1.69</td>
<td>1.86</td>
<td>2.31</td>
<td>2.08</td>
<td>16</td>
</tr>
<tr>
<td>Bio-mimicking</td>
<td>1.35</td>
<td>1.60</td>
<td>1.72</td>
<td>1.89</td>
<td>2.26</td>
<td>1.54</td>
<td>13</td>
</tr>
</tbody>
</table>
Figure 9.5 Severity of potential threat vs likelihood to pose a threat: Now-2015
Figure 9.6 Severity of potential threat vs likelihood to pose a threat: 2016-2020
Figure 9.7 Severity of potential threat vs likelihood to pose a threat: 2021-2025
Figure 9.8 Severity of potential threat vs likelihood to pose a threat: 2026-2035
Figure 9.9  Severity of potential threat vs likelihood to pose a threat: After 2035
It might be of interesting to present a comparison between the severity of the potential threats and the maximum of the likelihood average value along the whole time interval (Fig. 9.11). The maximum values can be interpreted as representing the likelihood that the technology might pose a security threat in general, no matter when. Technologies which appear in the upper right quartile of the figure are those which have high likelihood to pose a highly severe security threat.

Technologies in this group include the Internet of Things (IoT), RFID, smart mobile phone technologies mash-ups, cloud computing, advanced Artificial Intelligence, tailored nanoparticles, energetic nanomaterials, cyborg insects, metamaterials and "optical cloaking", water catalysing explosive reactions, synthetic biology, human enhancement and new gene transfer technologies.

**Potential "wild card" technologies**

On the other hand, looking at technologies with low likelihood (less than 3.0) to actually pose a threat combined with high (more than 3.0) severity of threat could point to potential so-called "wild cards" (low-likelihood but high impact events), that may also imply a need for special attention. For example, based on Fig. 9.6 we can identify potential "wild card technologies" for the timeframe 2016 -2020. These are presented below in Fig. 9.10, in which for completeness we also added their foreseen time of maturity.

![Figure 9.10 Potential "Wild Cards" for the timeframe 2016-2020](image)

(low-likelihood high-severity technologies in fig 9.6)
Figure 9.11 – Severity of potential threat vs maximum likelihood to pose a threat
The change of threat likelihood over time

It is interesting to observe the change over time of the average values of perceived likelihood of each technology to actually pose a security threat. This dynamics is shown in Figures 9.12 – 9.17.

For most of the technologies the likelihood to pose a threat rises with time, but in some cases it declines in later stages, presumably because the experts envision that in a certain time technologies or other means will be effectively applied to prevent the realisation of the threat or to counter it.

![Figure 9.12 Likelihood to pose a threat - ICT](image)

![Figure 9.13 Likelihood to pose a threat - Robotics](image)
Figure 9.14 Likelihood to pose a threat – Nanotechnology

Figure 9.15 Likelihood to pose a threat – Converging technologies
9.4 The impact on society: different societal spheres that might be affected

In the last question of the survey the experts were asked to evaluate to which of the following spheres of society will each technology actually pose a security threat (multiple choice):

- People (individuals, groups, mass populations)
- Infrastructures (energy, airports, communications, etc.)
- Economy (e.g. industries, banks)
- Environment
- Political system
- Values

In the following table 9.4 we summarise the respondents' answers. The percentages indicated are the fraction of the respondents that chose each possibility; because of the multiple choice option the sum of percentages across each technology can be between zero (no threat at all) and 600% (maximal effect on all spheres).

* The following explanation of "values" was given in the questionnaire: Human values tell people what is good/bad, desirable/undesirable, etc. Values are changing over time. Threats posed by new technologies might lead to changes of values. For example, omnipresent video surveillance or the control of individual behavior using RFID's might lead to changes of values with respect to the democratic nature of the society. Another example for changing values might be a political decision to use or NOT to use a specific technology which enhances security but limits personal rights. Specific future technologies could challenge the perception of what is "positive" and "negative" in such technologies – and consequently may lead to drastic changes of value systems with respect to technology (an example could be "swarm robotics" and its surveillance and control capabilities).
Table 9.4: Societal spheres potentially threatened by various technologies

<table>
<thead>
<tr>
<th>Technology</th>
<th>Economy</th>
<th>Environment</th>
<th>Infrastructures</th>
<th>People</th>
<th>Political systems</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT</td>
<td>66%</td>
<td>22%</td>
<td>80%</td>
<td>93%</td>
<td>24%</td>
<td>29%</td>
</tr>
<tr>
<td>RFID</td>
<td>54%</td>
<td>9%</td>
<td>63%</td>
<td>91%</td>
<td>23%</td>
<td>31%</td>
</tr>
<tr>
<td>Smart mobile</td>
<td>41%</td>
<td>13%</td>
<td>56%</td>
<td>94%</td>
<td>34%</td>
<td>31%</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>90%</td>
<td>10%</td>
<td>65%</td>
<td>81%</td>
<td>32%</td>
<td>19%</td>
</tr>
<tr>
<td>Ultra-dense</td>
<td>89%</td>
<td>17%</td>
<td>33%</td>
<td>78%</td>
<td>39%</td>
<td>6%</td>
</tr>
<tr>
<td>Artificial intelligence</td>
<td>67%</td>
<td>38%</td>
<td>76%</td>
<td>82%</td>
<td>51%</td>
<td>31%</td>
</tr>
<tr>
<td>AI robots</td>
<td>41%</td>
<td>41%</td>
<td>59%</td>
<td>88%</td>
<td>35%</td>
<td>41%</td>
</tr>
<tr>
<td>Autonomous robots</td>
<td>43%</td>
<td>36%</td>
<td>71%</td>
<td>93%</td>
<td>14%</td>
<td>29%</td>
</tr>
<tr>
<td>Artificial limbs</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>89%</td>
<td>11%</td>
<td>33%</td>
</tr>
<tr>
<td>Ethical control</td>
<td>17%</td>
<td>50%</td>
<td>17%</td>
<td>83%</td>
<td>33%</td>
<td>17%</td>
</tr>
<tr>
<td>Swarm robotics</td>
<td>67%</td>
<td>67%</td>
<td>78%</td>
<td>78%</td>
<td>11%</td>
<td>22%</td>
</tr>
<tr>
<td>Molecular manufacturing</td>
<td>50%</td>
<td>88%</td>
<td>38%</td>
<td>75%</td>
<td>25%</td>
<td>13%</td>
</tr>
<tr>
<td>Nanoassemblers</td>
<td>55%</td>
<td>82%</td>
<td>55%</td>
<td>73%</td>
<td>18%</td>
<td>0%</td>
</tr>
<tr>
<td>Medical nanorobots</td>
<td>18%</td>
<td>46%</td>
<td>9%</td>
<td>100%</td>
<td>9%</td>
<td>18%</td>
</tr>
<tr>
<td>Tailored nanoparticles</td>
<td>16%</td>
<td>84%</td>
<td>21%</td>
<td>100%</td>
<td>0%</td>
<td>11%</td>
</tr>
<tr>
<td>Energetic nanomaterials</td>
<td>25%</td>
<td>58%</td>
<td>83%</td>
<td>92%</td>
<td>25%</td>
<td>0%</td>
</tr>
<tr>
<td>Molecular nanosensors</td>
<td>20%</td>
<td>30%</td>
<td>20%</td>
<td>100%</td>
<td>40%</td>
<td>0%</td>
</tr>
<tr>
<td>Brain implants</td>
<td>7%</td>
<td>20%</td>
<td>13%</td>
<td>93%</td>
<td>33%</td>
<td>67%</td>
</tr>
<tr>
<td>Brain-to-Brain</td>
<td>40%</td>
<td>10%</td>
<td>10%</td>
<td>100%</td>
<td>60%</td>
<td>70%</td>
</tr>
<tr>
<td>Cyborg insects</td>
<td>42%</td>
<td>67%</td>
<td>92%</td>
<td>92%</td>
<td>8%</td>
<td>17%</td>
</tr>
<tr>
<td>Brain computer interface</td>
<td>8%</td>
<td>8%</td>
<td>17%</td>
<td>100%</td>
<td>33%</td>
<td>50%</td>
</tr>
<tr>
<td>Human enhancement</td>
<td>38%</td>
<td>6%</td>
<td>38%</td>
<td>94%</td>
<td>69%</td>
<td>81%</td>
</tr>
<tr>
<td>Metamaterials</td>
<td>46%</td>
<td>23%</td>
<td>85%</td>
<td>69%</td>
<td>31%</td>
<td>8%</td>
</tr>
<tr>
<td>Water catalyzing</td>
<td>42%</td>
<td>58%</td>
<td>92%</td>
<td>83%</td>
<td>33%</td>
<td>0%</td>
</tr>
<tr>
<td>Programmable matter</td>
<td>45%</td>
<td>64%</td>
<td>73%</td>
<td>73%</td>
<td>18%</td>
<td>18%</td>
</tr>
<tr>
<td>3-D printing</td>
<td>75%</td>
<td>33%</td>
<td>58%</td>
<td>75%</td>
<td>17%</td>
<td>8%</td>
</tr>
<tr>
<td>Future fuels</td>
<td>25%</td>
<td>83%</td>
<td>83%</td>
<td>92%</td>
<td>25%</td>
<td>0%</td>
</tr>
<tr>
<td>Crystalline polymers</td>
<td>36%</td>
<td>45%</td>
<td>45%</td>
<td>82%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Synthetic biology</td>
<td>23%</td>
<td>69%</td>
<td>15%</td>
<td>100%</td>
<td>23%</td>
<td>31%</td>
</tr>
<tr>
<td>DNA protein</td>
<td>17%</td>
<td>75%</td>
<td>8%</td>
<td>100%</td>
<td>8%</td>
<td>25%</td>
</tr>
<tr>
<td>Gene transfer</td>
<td>27%</td>
<td>82%</td>
<td>0%</td>
<td>82%</td>
<td>9%</td>
<td>27%</td>
</tr>
<tr>
<td>iPS cells</td>
<td>9%</td>
<td>18%</td>
<td>0%</td>
<td>82%</td>
<td>0%</td>
<td>27%</td>
</tr>
<tr>
<td>Bio-mimicking</td>
<td>13%</td>
<td>50%</td>
<td>13%</td>
<td>100%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>
From table 9.4 we can learn that some of the technologies potentially threaten several societal spheres while others affect fewer spheres.

In-depth analysis* of the survey results such as in the table 9.4 is presented in the FESTOS deliverable D3.3, based on task 2 in WP3. Here we only show for each societal sphere the number of technologies regarded as threatening by more than 50% of the respondents (Fig. 9.18). As can be seen in figure 9.18, almost all the addressed technologies pose potential threats to people. ICTs could also threaten the economy and infrastructures, new materials affect mainly the environment and infrastructures, nanotechnologies and biotechnology affect mainly the environment, and converging technologies can also affect the political systems and values.

![Figure 9.18: The number of technologies that pose a threat to each of the societal spheres](image)

**9.5 Some observations and insights from respondents' comments**

The survey respondents were encouraged to comment (in free text) on the technology fields, on specific technologies, and on the survey in general. 46 experts chose to take this opportunity (full texts can be found in Appendix A).

In general, the impression from the comments is that the respondents feel that the issues addressed by FESTOS are very important and most of the technologies included in the survey are indeed relevant and deserve attention. Perhaps the following comment of one respondent underlines the value of the expected FESTOS outcomes: *"In all these emerging technologies we need to change our vision of..."*

---

*Including STEEPV analysis: implications related to Society, Technology, Economy, Environment, Politics and Values*
security, considering the potential threats to the well-being of our society from the very beginning".

Quite surprisingly, some comments underline the insufficient awareness (by experts!) of potential security threats, and hence the importance of FESTOS. It seems that the survey itself has already contributed to raising awareness, at least for some experts. One expert wrote: "Going over your questions I suddenly realized how smilingly innocent technologies can pose severe security threats in the near future. Being a relatively experienced individual, yet unaware of the above, I would say now that the public is not informed about such threats... Thank you for enlightening me..."

A few additional technologies were proposed for considerations, most of them in the ICT field: Semantics in image processing, image recognition, experience feedback, image mining (combined with data mining and text mining), knowledge engineering, knowledge discovery in databases, semantic web, social computing. According to one expert, certain transportation technologies are worth consideration as well.

Several respondents wrote that the main threats in the ICT field are more to privacy and civil liberties than to security, and stressed the potential abuse not by criminals but also by governments or other organizations.

Some experts think that although the addressed technologies are new, the potential threats are not, because similar malicious uses are already possible by existing technologies. This was said, for example, about ultra-dense data storage and RFIDs, or about certain nanotechnologies that according to some opinions are no more dangerous than "old" chemistry technologies.

Certain nanotechnologies, in particular nanoassemblers and molecular manufacturing, are regarded as "too speculative" by some respondents. However, there is clear disagreement about such technologies. While one expert claims that molecular manufacturing is "too speculative to deserve attention at the moment", another one says that it is "no more dangerous than organic chemistry", and a third one thinks that the same technology "could be dangerous by scaling down the resources and facilities needed to manufacture other risky technologies [...] enabling creative malefactors to invent entirely new categories of threats there is no general preparedness or recognition of". Similarly, while many respondents stress the potential threats of tailored nanoparticles ("a nice weapon for a terrorist", in the words of one expert), other experts think that the perceived dangers are overestimated ("to pose serious threats huge amounts are needed and these will be covered by normal oversight and regulation").

Many experts stressed the well known fact that all technologies are inherently prone to potential misuse, and that the necessary regulations usually lag behind the technologies. One respondent warned that "As soon as big money is involved it becomes impossible to get objective information. Therefore the dangers must be estimated in advance... Otherwise it will be too late". Moreover, risk policy is problematic because, as one expert put it, "Society tends to misestimate risks, and be very over-confident about its estimates. Certain minor risks are exaggerated, while others are regarded as silly."


10. Conclusions

"I suddenly realized how smilingly innocent technologies can pose severe security threats in the near future. Being a relatively experienced individual, yet unaware of the above, I would say now that the public is not informed about such threats."

A responding expert, FESTOS expert survey

In the present report we have summarised the activities carried out in FESTOS Workpackage 2: "Horizon scanning of emerging technologies and scientific developments, which may pose security threats in the future". The result is a set of selected new/emerging technologies with a significant threat potential in the sense of abuse by terrorist or criminal organisations, as evaluated by means of an expert survey. The list is obviously not intended to be exhaustive. Rather, it is intended to stimulate further discussions and to provide a basis for a subsequent analysis, where the potential threats are classified, assessed and discussed in more detail (in FESTOS WP3). Moreover, we regard the list as a dynamic bank of technologies with indications of potential security threats, which may be useful even beyond FESTOS and after the project is completed.

Studying various technologies, three broad categories of potential threats could be identified: The first one is the disruption of certain emerging technological applications for malicious purposes. For example, jamming the communications in intelligent collision avoidance systems in transportation, or any hacking of computer systems and causing damage by disrupting their proper functioning. This category, although it may seem straightforward, is increasingly important with the continuously growing dependence of our society on technologies, at the level of both critical infrastructures and everyday life. Just thinking about the envisioned "Internet of Things", where everything around us is interconnected, raises serious concerns about this new "opportunity" for hacking, disruption and abuse.

The second category concerns the increased availability and proliferation of technologies that once were strictly confined to the military sector or to unique heavily funded laboratories, and as such were prohibitively expensive. For example, commercial off-the-shelf (COTS) components that enable terrorists to create their own SIGINT (signal intelligence) systems, or equipment capable of generating damaging electromagnetic pulses (EMP). Even some materials for chemical or biological terrorism may fall into this category, as the underlying knowledge, relevant materials and laboratory equipment become widely accessible. Examples of technologies in this category were included in the preliminary scanning (report D2.1). Due to scope limitations these technologies were not investigated in the expert survey, but undoubtedly they deserve attention.

The third category concerns malicious and surprising uses of new technologies that are being developed for completely different, beneficial purposes. For instance, employing small (but sophisticated) toy robots for terror attacks, utilising internet-
based networked games to recruit new members to hostile organisations, or using synthetic biology to engineer bacteria that, for example, instead of producing fuel consume it.

All the three categories are important for addressing emerging security threats posed by new technologies. Nevertheless, the most interesting for FESTOS seems to be the third category, where we may probably find the most unexpected potential threats, perhaps signals to surprising "wild cards". Some possible wild cards (namely low-likelihood but high-severity threats of maliciously used technologies) have been already indicated in the FESTOS expert survey.

In the FESTOS worldwide expert survey we have elicited experts' opinions about the threat potential of selected emerging technologies, following a preliminary scanning of a broad range of potentially threatening technologies. In addition, the survey addressed general attitudes to technology-related threats, as important input to the analysis of "security climates" in WP4.

The results of the survey provide the experts' estimates about:

- The time frame in which each technology will be sufficiently mature to be used in practise
- The severity level of the potential security threat posed by each technology
- The easiness level of malicious use of each technology
- The likelihood of each technology to actually pose a security threat in the future, in different time-frames (from now till after 2035)
- Which societal spheres are mostly affected by security threats that might be posed by each technology

Interesting free-text comments submitted by experts in the survey underline the insufficient awareness (even by experts!) of potential security threats stemming from emerging technologies, hence the importance of FESTOS. Several comments indicate that the respondents feel that the issues addressed by FESTOS are highly important and most of the technologies in the survey are indeed relevant and deserve attention.

The information gathered in the survey can serve as a valuable base for further analysis. The results provide additional dimension to the preliminary horizon scanning as well as important inputs to the subsequent analysis and categorisation of threats performed in WP3. The in-depth analysis (including ranking and evaluation of threats from various perspectives) is presented in D3.2 ("Categorised security threats in foresight perspective") and in D3.3 ("Integrated Security Threat Report").
Appendix A – Full text of selected respondents' comments

The respondents of the survey were encouraged to write free-text comments on each of the fields, on each of the technologies, and general comments about the survey. 46 respondents wrote some comments. We quote here selected comments (with minimal necessary editing).

Comments on additional potentially threatening technologies (not included in the survey):

- I would include Web 2.0 and Botnets.
- Knowledge Engineering, Knowledge Management, semantic web, experience feedback Wireless threats monitoring systems
- Topics not included in the survey: e.g. cyber-security, denial of service, social computing Potential threats of emerging technologies in environmental use of GMO to treat pollution, sewage, etc. Using transgenic food, producing of transgenic organisms from bacteria to animals without proper security
- Some interesting transportation technologies worth an analysis.
- semantics in image processing, image recognition experience feedback, image mining combined with datamining and textmining
- I see great potential danger in the possible manipulation and use of knowledge discovery techniques on huge private data about persons and firms. These technologies can be a great advantage for criminals, terrorists, etc. Unfortunately, our democratic rules avoid to be efficient in front of these people and organizations.

ICT
General comments:

- We will find security holes in nearly every software/hardware which is developed, economic pressure will set fun and usage more important than security. Each of the technologies above will be used at one time in a destructive way. You claim terrorists to be dangerous but the loss of privacy by data crawling companies and states, loss of freedom are much more dangerous. If our political system slowly changes to a surveillance society I would count this as harmful. None is able to tell which security holes will be used in which upcoming technologies to achieve what kind of destruction. I do not feel able to break down complicated estimations to a number from 1 to 5. Most of the technologies noted above will change the social world we live in (getting used to states and companies knowing intimate details about my live, social pressure to use smart phones etc.) and in this changed world other threats will show up. It is simply not important which technology will give the backdoor. And you missed the whole field of social networks and a generation of internet kids growing up, states which try to set up local laws to fight the global internet, companies trying to restrict the net and the freedom and privacy of users to keep their hands on music, movies, texts and more. The big threats are not single technologies but the social impact and stress of upcoming technologies.
• Danger of many different IT applications converging to provide an
undemocratic state with extraordinary surveillance and intrusion capabilities.
• Problems are: absence of regulatory mechanisms, hacking of websites, entry
of outside elements with spurious data.
• This field is advancing much faster, especially in e-commerce and e-financial
services, than either the regulatory responses or the public's understanding of
what risks are involved.
• This field poses a privacy threat. If not implemented carefully, we could have
challenges with profiling based on what items we are wearing/carry with us,
traceability (depending on reader density and interoperability). The
technology is not very transparent.

Comments on specific technologies:

IoT

• The main problem of the Internet of Things is the direct influence that it has in
the physical world. Attacks that target home PCs nowadays (DDoS, zombie
networks,...) could be used to target real-world elements, causing major
damage to all the elements of our society. All the elements of the IoT must be
thoroughly studied in order to define a new security approach that could be
used as a foundation to avoid security breaches.
• The technology is already in use in small scales, also in homes. However,
there are no precautions for power surges.
• A major problem may become state preparations and use (for armed conflict
or phases just below). This applies also for RFIDs
• This technology enables ubiquitous surveillance. Governments or groups with
access to the infrastructure can monitor large populations, and security
exploits can allow others the same power. Since ubiquitous monitoring makes
many privacy and security precautions impossible (e.g. secret passwords),
this has potentially serious effects.

Radio-frequency identification (RFID) and "RFID-dust"

• RFID is just one form of identity technology, where objects gain a detectable
and traceable identity. Mature identity technology enables tracking of people
and objects, with potential integrity concerns.
• Possible erosion of democratic freedoms.
• RFID Technology does not pose a new threat. However, it does not provide a
solution for existent threats since its purpose is mainly to provide tracking
features on objects or even people. If we consider that there will always be a
way to hack RFID data, there will always be chances to abuse these data.
However, this fact does not pose a new threat since the same kind of threats
exists no matter if RFID technology is present or not. Following one of the
examples provided: "Using RFID readers to locate valuable goods and select
potential victims", this kind of malicious activities are currently done through
discrete surveillance of the areas where goods are stored and potential
victims. Surveillance and open source intelligence (OSINT) can provide all the
information required to locate valuable goods and victims and it is less
expensive (it needs no RFID equipment or hacking software) and also less
risky. Reading a RFID tag might require to be close to tagged good or person. However, knowing in what kind of house a potential victim lives, what kind of car he has and what his job is can be obtained in a much more discrete manner, far away from the potential target. Similar reasoning can be used with the rest of the examples provided. In short, RFID does not pose a new threat; it just makes perpetrators adapt their methods.

- There are 2 basic types of RFID: 1) semiconductor chip based demanding energy for operation 2) passive SAW-tags, only reflecting signals. The first are incomparably more dangerous, since they demand >1W radiation power by each "reader", while SAW-tag readers radiate 100times lower power (10mW). Massive use of semiconductor tags will result in high level of background EM radiation, especially in public places, such as supermarketes.

Smart mobile telephone technologies mash-ups

- Danger might stem from the ubiquitous diffusion of smart phones and their ease of use and the likely emergence of distributed applications (so that e.g. a group with malicious intentions might exploit one of these to get intelligence etc.)
- The primary threat will be through the equivalent of phishing scams, exploiting the complexity of upload/download to lure the unsuspecting. In addition to this the targeting of such devices by hackers will be an increasing problem.
- While smartphones and OSINT (Open Source Intelligence) could be used maliciously, they also have strong potential good effects (distributed outbreak monitoring, ad hoc coordination, surveillance of government and other centres of power). The transition to a society of distributed monitoring and new values can be disruptive and might be interpreted by governments as malicious use.
- There are already some reasonable technology-based security solutions for this domain, but they are far less mature, understood or implemented than security solutions for PC-based Internet. The public is basically unaware of the risks or solutions and is not being educated adequately. Governments need to intervene at the level of regulating security solutions and also providing education campaigns in order to encourage uptake of security technologies.
- The usage of smart phones (and their future evolutions) in relations to other mentioned domains (e.g. IoT) might pose specific challenges, thinking about the possibility that they would act as very common "remotes" or "listening post" for any kind of manipulation -- this might be even more serious considering e.g. that phones might be hacked by third parties

Cloud Computing

- Cloud Computing should not be used in infrastructures and very important fields like economy and political systems.
- Cloud computing involves risks due to centralization to certain datacenters. It is of limited security importance because malicious use that doesn't attack on the datacenter level will be traceable to a customer.
Ultra-dense Data Storage
- Losses of data occur all the time and are a serious problem, but it is not the data storage that is the risk.
- A major problem may become state preparations and use (for armed conflict or espionage)
- The threats to data storage have been existing along with archiving. The security threat is therefore the same as any data loss or theft, only the amount gets larger. It does mean that the threat grows with the amount of storage.

Advanced Artificial Intelligence
- AI is nowadays only in used under human supervision, not as stand-alone autonomously deciding entity. It is, however easier to make malware than safe usage. For example, now even the simplest computer virus is a threat, and it is more difficult to protect against it than to make one.
- If we maliciously use future AI technology, it will cause serious problems since AI will have more powerful intelligence than human beings in the future. If we will be able to produce a perfect AI system and if some somebody with malicious intent have it, it might cause a serious security threat such that in SF movies. Fortunately (?), it will be very difficult to produce a perfect AI system even after 20 years. However, even for current level of AI system, there exists certain possible security threats. Actually, we will be able to protect them by the AI technology.
- The problem is not simple AGI (Artificial General Intelligence), which certainly can pose some security risks (e.g. malicious data mining, automated crime), but above human intelligence. Whether such AGI can be created is uncertain, but if it can the consequences are potentially "extreme". There exist plausible theoretical arguments why such systems would pose an existential risk to humanity and the biosphere. The risk here is not from deliberate malicious use, but rather that the AGI behaves in a "malicious" (not necessarily intentionally designed malicious) way.
- The problem is not an AI being too intelligent but people willing to believe what computers tell them.
- Unpredictable behavior: AI could in principle decide on eradicating humankind. Particular problems if used by states in preparations for armed conflict.
- Data privacy is perhaps the most urgent problem with this technology. Also the military use of this technology should be strictly forbidden.

Robotics
- Robots in public area based on adjustable autonomy, HRI, networked robots, cooperative localization and cooperative decision-making should attract more academic and industrial entities.
- "Robots soldiers" is one of the most frightening applications of this technology. Also the temptation to replace human beings with robots for eldercare is worrying. Social robotics should be limited by ethical considerations.

Nanotechnology

General Comments:
Nanoassemblers and nanorobots are mainly of interest for novelists
Mostly a pipe dream.
Generally speaking users of different nanotechnologies should be informed on potential risk connected with their application.
Potentially huge benefits especially in areas such as nanomedicine. But there are no more threats than have always existed, say, in synthetic organic chemistry
Very incomplete list of technologies
Concerns about toxicity - human health, occupational health, environment and ecosystems; and about economic priorities (too many nano consumer products, too few nanomaterials for sustainability and energy).

Comments on specific technologies:

Molecular Manufacturing
- Too speculative to deserve much attention at the moment
- Unlikely to be different from ordinary chemistry.
- This is no more dangerous than organic chemistry has always been
- Asking for 'threat' may be a misleading. This technology is about production methods, not about applications.
- Nanomanufacturing could be dangerous by scaling down the resources and facilities needed to manufacture other risky technologies, by creating first-mover advantages or arms races and especially by enabling creative malefactors to invent entirely new categories of threats there is no general preparedness or recognition of.

Self-replicating nano-assemblers
- Macroscale assemblers are potentially as dangerous as nanoscale assemblers, especially if they are stealthy and can reproduce in unobserved parts of the environment. Preparedness for replicating threats or warfare is low.
- Too speculative to deserve much attention at the moment
- It very much depends on the application of this technology
- This is more of a science fiction scare than real

Medical Nanorobots
- The threat is the same as any hazardous spread of viruses and bacteria.
- Medical nanorobots are essentially ICT-enabled medical devices taken to the next level. The main threats are privacy, over-diagnosis and control of populations by controlling their health systems.
- This is more of an opportunity than a threat.
- This nanotechnology is more realistic. Applications however will have to be tested in clinical trials.

Tailored nanoparticles
- Industrial application of different types of nanoparticles (carbon nanotubes, fullerenes, mineral nanofillers and so on) is still growing. However their users as a rule are not informed on very real detrimental effects of the particles on human organisms. Also nanoparticles used as drug carriers could exert a detrimental effect on human body.
• It is important to make sure that the nanoparticles can not cause unwanted damage. It is not possible to test nano-properties with the test methods used for e.g. toxicity, instead appropriate test methods need to be developed based on risk analyses conducted.

• Tailoring properties of nanoparticles allow to tailor physical properties of new materials and in consequence to tailor parameters of new generation of devices

• NPs especially if made of toxic material can pose a threat as they could be used in a similar way to gas based toxins.

• This technology offers far more of opportunity than a threat

• These particles can be used in the same way as a chemical/ biological/ radiological aerosol. They can be easily disseminated and stay in the air for a considerable time. A nice weapon for a terrorist. However, the threat must not be overestimated: difficult to produce, not very toxic (compared to “conventional” CBR-agents) and essentially long term effects. This means not much immediate damage as wanted by terrorist groups for propaganda purposes.

• NP are used already and their use will increase. To pose serious threats huge amounts are needed and these will be covered by normal oversight and regulation.

• While nanoparticles might accidentally cause harm, deliberate “nanotoxins” appear relatively inefficient. Some potential misuses could involve targeting particular organs or “blackmail” where infected people have to obey or some chemical signal will trigger a dangerous conformation change of the particles they have ingested.

• Producers of nanoparticles and companies offering different types of nanotechnologies should be obliged to inform their users as well as common members of societies on a potential risk connected witha progress in the area.

• A lot more should be spent on toxicology research as nanotech develops.

Energetic nanomaterials

• Enhanced explosives and incendiaries make terrorism slightly worse, but given the potential for current substances (especially non-monitored ones like thermite) nanomaterials doesn’t change the game.

• This is no more dangerous than many of the detonators and explosives that have been available in the past 50 years….in fact maybe less so because the stuff is harder to make!

• Nanomaterials fabrication is not easy, in most parts expensive and requires some chemical expertise - but all that can be had in the black market as the advent of meth and its derivaties show.

• 'Energised' is a vague term. All nanoparticles are in some sense energised because of their enormous surface area relative to mass.

Molecular sensors (sensors with molecular precision)

• Ubiquitous surveillance is a serious political risk.
• Sensors could create a significant military advantage. Probably too sophisticated for criminals.
• Sensor technology will not impose any foreseeable threats to any of the above.
• Just like theranostics is proposed as a way of personalising treatment to individual characteristics so molecular sensing could in principle be used to target toxins to individuals with particular biochemical makeup.
• This is a technology that actually reduces threats to security.
• Maybe biggest threat from use by governments.

Biotechnology
Comments on specific technologies:

Synthetic Biology
• It really has knock-on effects across all the above because if it is used to generate pandemic disease organisms which are then liberated then clearly industry will grind to a halt hospitals overwhelmed and so on.

New gene transfer technologies
• A perfect soldier as a result of gene engineering.

Induced Pluripotent Stem Cells (iPS cells)
• How do we know what is good for the human genome? How do we know "what sort of people should there be?" Are there any limits to reproductive freedom? And if we are to set the limits who are the "we" to it? I predict a serious transformation of our value systems.

New Materials
General comments:
• On the whole should be beneficial in creating strong lightweight materials, and intelligent materials, which will assist sustainability - low energy use, low waste, catalysis of production feeds (efficiency) etc. Toxicity may be an issue, especially at the disposal stage.
• Regarding the structural materials for nuclear applications, many efforts are done, especially for nuclear waste conditioning. One can worry about the relevance of the models used regarding the long durations involved. The task is not simple but it is the first time that such a long term problematic is addressed and people as to be reassured.
• Some materials like Bi replacing the Pb-additions to soldering materials are also environment- and human tissues degradable substance. Moreover, gas- and liquid media used in technology of e.g. Mg-alloy applied in aircraft- and automotive industries are very dangerous, too. Regarding the environment protection, such problems, like recycling of metal-alloys made structural elements and new solar cell- and crystallographic electrical cell (patented myself, recently) are subjects of research activity of my home Institute.
• My interest concerns multilayers produced by such technologies as: PVD, CVD, thermal spraying processes.
• In general it is always important to consider new materials different properties as opposed to more traditional materials. Test methods are in many cases developed for a certain type of material and application. This could e.g. be test methods for safety valves that used to be mounted on metallic material but are now mounted on composite materials with highly different thermal properties.
• An additive manufacturing enables the fabrication of 3-D physical metal/ceramic fully dense components of arbitrary shapes, with the use of service (or new) materials to generate functionalities (for example corrosion resistance) required for target applications. The great advantage of this technique is a possibility to fabricate components with functional graded structure (for example: gradient of chemical composition, phase structure, microstructure) in order to generate new functionalities that are not possible or too costly while using conventional processes. Nowadays, high performance components from metals (alloys) and metal/ceramic composites can be fabricated by using rapid prototyping techniques. It is usually 3D additive manufacturing by using laser engineered net shaping (LENS) or laser selective sintering (LSS). However, only LENS technique enables to obtain fully dense components with excellent mechanical properties. This technique is an excellent tool for design and fabrication of functionally graded materials (including multifunctional). It can be used to fabricate, enhance and repair high performance metal/ceramic components. By using this technique you can fabricate fully dense components from stainless steel, titanium and nickel alloys, metal/ceramic composites as well as refractory metals (alloys). However, you need also modern surrounding facilities for powder characterization and X-ray tomography of components as well as testing mechanical properties. The LENS system costs about 1 Million US dollars. So it is very expensive now. In the future the laser system can be cheaper that is why it may cost less. Moreover, miniaturization is going very fast and this system can be smaller and more friendly (easier) in using.

Comments on specific technologies:

Metamaterials with negative light refraction index
• This technology concerns so far nano-objects and narrow-band frequencies... Perfect invisibility for large scale objects in the whole visible spectrum is, in my opinion, very unlikely in the medium term future.
• This technology may lead to the production of invisible devices (cars, boats etc.) which could be very dangerous if used by terrorists.

Water catalysing explosive reactions
• Can revere actual safety standards and unable functioning of many infrastructures.

Programmable matter
• Can be used in a crime activities to mask crime material evidence.
Personal rapid prototyping and 3-D printing machines

- 3D printing will enable custom parts to be made with little evidence that it is being done. They may find application in dangerous devices and in shielding them from detection.
- The technology can simplify terrorist attack or crime groups activity planning

Dielectric Resonators for filtering radio-frequencies

- The technology can disturb or even demolish communication systems.

Future fuels, processes and structural materials for nuclear technologies

- Future fuels supposed to be more effective and more dangerous in case of explosion. Thus, it could be used as accessible explosives.
- Nuclear technologies are very difficult to be implemented by limited groups of individuals. They must be implemented in the countries having enough technological and economic potential. It is expected that access to nuclear technologies will continuously be limited due to international regulations, anti-proliferation treaties and if started, eventually destroyed if any threat might occur in a future.

Crystalline polymers, polymer blends, multilayer assemblies

- The material can be used to prolong malicious materials e.g. explosives, and as such can pose a threat
- PVD, CVD and thermal spraying are now used technologies and strongly influence on the industry and common life.
- Nanopolymers and composites could gradually replace the 'metallic' materials economy - transport, machinery etc - supporting a sustainable economy.

Converging Technologies

Comments regarding the field in general:

- The biggest danger here is the increasing gap between the haves and the have-nots. Wars have been fought over less.

Comments regarding specific technologies:

Nanotechnology-enabled brain implants

- BCI might harm or affect users, but it is unlikely to potentiate them so much they would become significantly better perpetrators.
- As any technology - new or old - the nanotechnology-enabled brain implants open both positive and negative options. The most obvious positive ones are health-improving opportunities, while the negative options are threats to the privacy and decision-making of the people involved. It is therefore up to those handling these technologies to undertake the positive or the negative avenue.

Brain-to-brain communication ("Radiotelepathy")

- The technology of decoding the human EEG signals (who wants to say something) and the use of a computer-based speech recognition system for
telepathy, which is under the study) seems to be the wrong way: this technology is not necessary for telepathy. Thus this particular technology is hardly a threat. However if telepathy is understood in the process of this study it can be the greatest threat for security.

- This technology would plausibly increase the capacity for planning, coordination and execution of a wide variety of tasks, including malicious ones. However, it is likely that the coordination improvements among law enforcement outweigh the coordination improvements among criminals.

Cyborg Insects

- There is probably a greater threat from "un-cyborged" insects used as bioweapons. Cyborg insects (and other forms of semi-autonomous drones) could be used to distribute toxins and bioweapons.

Brain-Computer Interface – "Mind Reading" commercial gadgets

- There already exists misuse of the technology, despite it not being functional today. Various "brain fingerprinting" and fMRI methods are being sold to law enforcement and legal systems as reliable deception detectors without any evidence. Proper mind reading is hard, but misunderstanding or over-interpreting the signals is easy.

Human enhancement/augmentation based on NBIC convergence

- The threat is inherent rather than intentionally directed against someone in particular
- Who has access to this technology will have serious power; without some sort of ethical guidelines and/or regulation, the power will easily become corrupted.
- In order to pose a significant risk enhanced people need to be significantly more capable than their peers. This is unlikely due to rapid technology diffusion. However, the transition towards enhancement is rife with risks of criminal markets (black markets for enhancements in areas where banned), economic/legal conflicts over the rights to enhance or what labor restrictions there will be on enhancement, social shifts due to life extension etc. The potentially most dangerous form of enhancement might be genetic recompilation making people guaranteed immune to viral diseases, giving certain groups lower thresholds to engage in biowarfare.
- The neurons of the brain and their enhanced connection have no moral values which is necessary to the security of human existence. As a dualist I do not reduce mind to brain and think that undeveloped mind with poor moral level and overdeveloped brain with enhanced neuronal work can lead to the human catastrophe.

General remarks about the survey

- The questions about risk perception assume there is a general level of over- or under-estimation. Rather, society tends to misestimate risks, and be very overconfident about its estimates. Certain minor risks are exaggerated, while others are regarded as "silly". This makes risk policy problematic.
• As soon as big money is involved it becomes impossible to get objective information. Therefore the dangers must be estimated in advance... Otherwise it will be too late.

• The issue of threats stemming from new technologies has no salience yet in the public domain which may be a virtue since its malicious use restricts itself. However this will not remain so. Just as the threats from the internet became evident and open only after its use had increased exponentially and gained widespread acceptance the same will apply for all the other new technologies as well. There may be therefore a merit in this trajectory as it will give sufficient time to create public awareness of the negatives.

• Most of the threats have to do with environmental damage and/or erosion of privacy and citizen freedoms.

• The key issue is trust between individuals and governments. Every technology may be a benefit or a threat to individuals.

• Any kind of technology field can be abused and pose a threat, as any kind of regulation can be abused, as any kind of policy can be abused... Any process defined by human beings will never be perfect and thus there will always be room for abuse or misuse. Technology is an odd discipline because it is often ahead of people needs (as a matter of fact, in many cases technology drives people needs) while regulations and policies are usually behind of people needs (people needs drive regulations and policies). Technology will always be ahead of polices, regulations and in many cases ahead of people needs. However, these tools (i.e. policies and regulations) should be used to shape the way new and emerging technologies are used, providing mechanisms to prevent abuse, reduce its likelihood or at least minimize its impact in order to guarantee that new and emerging technologies bring benefits to people and that their use does not pose a threat. There are a very limited number of technologies that pose a real threat, in most cases it is technology abuse or misuse what poses a clear and present threat. Policies and regulations should aim at avoiding this kind of technology abuse/misuse while promoting beneficial technology applications.

• I cannot predict the future likelihood of each threat but one should remember that in parallel to any new problem we develop new solutions.

• I am not very comfortable with the questions. How should I answer the question: do people over- or underestimate threats...? They highly overestimate in some fields, highly underestimate in others. This is very different to the median, as both over- and underestimation are threats by themselves. Some of these estimations can be easily corrected by informing people better, others are so hard to explain that you have to be an expert to give a proper estimation and so on. Some of peoples estimations have high (social) impact, others are more “I don't care”. This is only an example. There are several questions where I do not see how to give a correct answer as the question itself does not fit, and that answers may be misinterpreted. I am pretty sure that each of the new technologies listed will have security holes, which will be used for something and this will somehow affect life, so I had to give high ratings. But I do not think the world will fall apart tomorrow due to new technologies (what you could believe if you read my answers).
• Going over your questions I suddenly realized how smilingly innocent technologies can pose severe security threats in the near future. Being a relatively experienced individual, yet unaware of the above, I would say now that the public is not informed about such threats. This actually may not be that bad - not giving these ideas to the wrong people, or creating panic at this point. I do not know the situation in governments. I found the questions in the first part a bit too general. It would have been helpful to answer the questions in the first part of the survey after the second, more specific one. Perhaps even twice, before and after. My answers would have been significantly different. Thank you for enlightening me, I wish I would have been more informed and therefore more helpful.

• The problem is not in technologies which will be I think very useful, but in the fact that they are mainly developed by firms or labs working for defence or security agencies, without any control or public awareness. Commercial applications for immediate profit are also a threat. Scientists should not accept to be manipulated by those who pay for the research, but their careers are at risk then.

• If you support optimum education, then there will be no threat higher than in other fields

• The problem is that materialist position in science does not allow a scientist to see the alternative explanation of a human based on two substances: mind and brain. The pure biological approach to a human with disregard to spiritual needs is the greatest danger to human security because it strips a human of humanity and allows him to treat himself and others as a means (for better performance) but not as an end worth of respect which is not moral as Kant says.

• Synthetic Biology needs to be scrutinised; However, a lot of the additives that are put into food for colour, flavouring, processing etc.....need also to be dealt with in a more consistent manner

• In all these emerging technologies we need to change our vision of security, considering the potential threats to the well-being of our society from the very beginning.

• An important factor in attaining a high security is safety, i.e. it is important to make sure that the new technologies and materials are robust and safe.

• No wrongdoing can be fully prevented. From old ages till today crimes and alike are part of our life. Yet, throughout history, civilized human societies have made continuous progress by developing and adapting novel procedures and technologies. Therefore, it is up to these civilized societies to be aware that not everybody is kind and cooperative and to respond with no hesitation and utmost determinations when wrongdoings appear at the horizon.

• It is difficult to estimate nowadays the positive-negative balance of the future technologies, but I am sure that they must be investigated and introduced.

• I think that threats will be there for any system. The problem is for the users to be informed and make appropriate use of technologies. Policy makers must take continuous care for the security and safety of used systems.
• I was not aware of the threats that emerging technologies may generate. I am more interested in the technologies. I think that security issues can be solved once they become widely usable.

• Nothing to worry about for the next decade, possibly never. Nanotechnology is just another branch of chemistry/physics and is not per se a threat.

• The potential threats listed in the ICT section are of a different kind and it is not possible to use the same scale and evaluation for them. What is a "very significant" damage potentially caused by some new technology? Is it a humanity extermination (if we remember science fiction books and movies) by AI-enhanced robots, potential vulnerability of all the internet passwords that might be broken by combining computational powers in cloud computing or a damage that can cause to a person some trojan-virus-infected smart shirt from internet-of-things? These all are different types of damages and we might consider them being not actually of the same importance for the society.