European Foresight Platform
supporting forward looking decision making
www.foresight-platform.eu

# FESTOS – Foresight of Evolving Security Threats Posed by Emerging Technologies

**EFP Brief No. 225**

**Authors:** Burkhard Auffermann Burkhard.Auffermann@utu.fi
Aharon Hauptman haupt@post.tau.ac.il

**Sponsors:** European Union DG Research
**Type:** European Union foresight
**Organizer:** ICTAF – Interdisciplinary Center for Technology Analysis and Forecasting, Coordinator: Dr. Yair Sharan, sharany@post.tau.ac.il
**Duration:** 03/09-12/11 **Budget:** € 824.552 **Time Horizon:** 2035 **Date of Brief:** Feb 2012

## Purpose

New technologies can improve our quality of life greatly, but they may also have a "dark side". The objectives of FESTOS were to identify and assess evolving security threats posed by the potential abuse of emerging technologies and new scientific knowledge, on the one hand, and propose means to reduce the likelihood of such threats, on the other. Looking ahead to the year 2030, this foresight study scanned the horizon of different fields of technology. Possible means of prevention and policy measures were studied in the context of trade-offs between security needs and the freedom of research and knowledge.

## Emerging Technologies Pose New Threats to Security

The FESTOS project (Foresight of Evolving Security Threats Posed by Emerging Technologies) identified and assessed evolving security threats caused by the abuse or inadequate use of emerging technologies and areas of applied research. Looking ahead to the year 2035, FESTOS scanned the horizon of fields such as nanotechnology, biotechnology, robotics, new materials, and information technology, as well as capabilities that might emerge from converging technologies.

FESTOS identified and evaluated these potential threats on the horizon. Based on this scanning, FESTOS stimulated "out of the box", forward-looking thinking and constructed "threat scenarios". Finally, FESTOS recommended policy guidelines designed to minimise the probability of these evolving security threats materialising. Possible means of prevention and policy measures were studied in the light of trade-offs between security needs and the freedom of research and knowledge while taking into account shifts in the public perception of threats and related security issues.

### Three Pillars of the Project

FESTOS had three pillars:

1. To identify new, potentially threatening technologies.
2. To assess emerging threats and – based on a selected set of potential threats – to construct scenarios with appropriate early-warning indicators.
3. To draft preparatory measures and policy guidelines.

As all foresight studies, FESTOS did not aim to predict the future. Instead, the project sought ***to raise awareness and initiate a debate*** among and between scientists and policy-makers about the possible "dark sides" of future technologies.

### Technology Scanning

The FESTOS team carried out a horizon scanning of emerging technologies that might pose security threats in the future if these technologies are abused. Furthermore, an assessment of the potential threats was carried out. The first result was a structured description of around 80 "potentially threatening" technologies in the

six fields listed above. The next step was to evaluate the threat aspects of 33 selected technologies by means of an international expert survey in which 280 experts participated. The collection of technologies was not intended to be exhaustive but to stimulate further discussions and provide a basis for the subsequent analysis. As such, it can serve as a "dynamic data bank" of potentially "abusable" technologies.

### Determining the Nature and Severity of Threats

Subsequently, the results of the expert survey were analysed in terms of the likely time spans for the threats to materialise, prioritisation (relative impact of each technology), the nature and extent of the potential damages, as well as societal issues. This activity included ranking and selecting security threats for scenario construction. In methodological terms, the exercise included expert brainstorming sessions, a security assessment (including Ansoff filters and the STEEPV method), an analysis of the relevant signals of change and wild cards.

### Scenario Development

Four narrative scenarios based on the identified security threats from emerging technologies were developed. The aim of the scenarios was to depict possible futures that take into account the social dimension and the interdependency of different impacts. In a scenario workshop, five methods and procedures were used: wild cards, security climates, futures wheel, security café for impact analysis and brainstorming.

### Control and Prevention

The possible control of scientific knowledge to prevent unintended new security threats is a very sensitive issue in open democratic societies. FESTOS raised a debate on whether and how to control emerging science and technology developments in order to prevent abuse without slowing down the process of knowledge creation needed for innovation, progress and improving human life. Secondly, FESTOS analysed the problematic issue of controlled dissemination of scientific knowledge in the light of the inevitable trade-offs between security and freedom of research and knowledge creation. The methods used were an online survey of approximately 100 selected experts and representatives from various parts of society, followed by 5-10 semi structured in-depth interviews in each of the participating countries (Poland, Germany, Finland, UK and Israel) with selected key actors representing civil society and other relevant organisations, and, finally, an international workshop on control and prevention, with the participation of invited experts and representatives.

## Top Technology Threats and Threat Scenarios

### Three Types of Potential Threats

Examination of the diverse technologies led to identifying three broad categories of potential threats: The first category is the disruption of certain technological applications for malicious purposes (for example, jamming communications in intelligent collision avoidance systems in transportation). The second category concerns the increased availability of technologies that once were confined to the military or to unique, heavily funded laboratories and were prohibitively expensive. The third category concerns surprising malicious uses of new technologies developed for completely different, beneficial and civilian purposes. The most interesting for FESTOS seemed to be the third category, where we found the most unexpected threats, signals of change or surprising "wild cards".

### Ten New Top Priority Threats

The threat analysis resulted in a prioritisation of the threatening technologies with respect to their ***potential for malicious use*** (combining the easiness of putting them to malicious use and the severity of the threat). The resulting top ten technologies are:

1. Smart mobile phone mash-ups
2. Internet of things (IoT)
3. Cloud computing
4. New gene transfer technologies
5. Advanced artificial intelligence
6. Synthetic biology
7. Cyborg insects
8. Energetic nanomaterials
9. Radio-frequency identification (RFID)
10. Autonomous & semi-autonomous mini robots

Furthermore, the ***intensity of the potential threat*** (i.e. the overall threat to several spheres of society according to the experts) posed by the ten most relevant technologies was prioritised:

1. Advanced artificial intelligence
2. Human enhancement
3. Swarm robotics
4. Cyborg insects
5. Internet of things (IoT)
6. Water-catalysing explosive reactions
7. Future fuels and materials for nuclear technologies
8. AI-based robot-human interaction
9. Cloud computing
10. Programmable matter

For the time scale 2015 – 2020, the following potential "wild card technologies" were identified (i.e. technologies with high severity threats and a low likelihood of actual abuse): swarm robotics, brain implants, water-catalysing explosive reactions, future fuels, self-replicating nano-assemblers, medical nano-robots, ultra-dense data storage, meta-materials with negative light refraction index and synthetic biology.

### Four Scenarios for Threat Assessment

Four narrative scenarios for threat assessment and identification of indicators were produced:

*Scenario 1*: *Cyber-insects Attack!*
Swarms of cyber-insects attack people and animals.

*Scenario 2*: *The Genetic Blackmailers*
Individual DNA is misused for purposes of extortion.

*Scenario 3: At the Flea Market*
Intelligent everyday nanotechnology-based products can be set to self-destruct, which is triggered by a wireless signal.

*Scenario 4: We'll Change Your Mind...*
A terrorist group uses a virus to change the behaviour of a portion of the population for a certain period of time.

### Conflict between Security and Freedom of Research

With the aid of the expert survey and the interviews, the FESTOS team assessed the respondents' perceptions of the awareness, acceptance and effectiveness of control and prevention measures. The results show that control and prevention measures exist, mostly in the fields of ICT and biotechnology. On the basis of the national reports on the participating countries' security institutions, we can say that the main institutions engaged in control activities are governments, ministries and security agencies. Most of the control measures have a high or very high impact on scientific knowledge, especially the freedom of science, knowledge creation and dissemination. The experts consider media, including the Internet, to be a dangerous channel of dissemination. By contrast, the most accepted control measures are

1. education curricula including programmes aiming to raise the awareness of potential threats,
2. measures invented by the knowledge producer and
3. measures developed by the media to limit the publication of sensitive knowledge.

Codes of conduct, internal guidelines (bottom-up approach) and legal regulations are perceived as the most effective control measures.

## Policy Conclusions

### Continuation of Horizon Scanning of Emerging Technologies

There is a need for networking, international cooperation and broader expert panels to evaluate emerging technologies continuously with respect to possible unintended effects relevant to security. More detailed technological evaluations are required in the short-term, and it was suggested that at least sixty to eighty technologies need to be evaluated. FESTOS provides a starting point to cover all the risks and work towards a EU risk strategy in different areas of science and technology. In addition, there is a need to cooperate much closer with the EU patent office and with patent agencies around the world. It is furthermore very important to secure financing in Horizon2020 to allow continuing the horizon scanning work carried out in FESTOS.

### Academic Freedom in Democratic Societies and "Knowledge Control"

There is a tension between possible security dangers of technology R&D and academic freedom, and there seem to be only two "stronger" control measures that academics are willing to accept: internal guidelines in research organisations and codes of conduct. Codes of conduct are the preferred control mechanism in R&D.

### Ethical Control and Codes of Conduct

Since science and technology is globalised and develops at a fast pace, we can only have ethical control if there are international codes of conduct, to be developed by international organisations. Scientists need to understand the consequences of their research, and this needs to be handled at an international level. There seems to be a difference between democratic and non-democratic countries in this respect. In democratic countries, there is less of a threat that scientists might develop technologies that will be misused. In societies that are more closed and lack democratic institutions, scientists tend to continue their research even if they are aware that their invention might pose a threat to security. In any event, industry has a massive influence, including the ability to effectively lobby for its interests. Some of this could focus on safe researcher practices, codes of conduct etc. and assist in the creation of an international "control" environment.

### Project Assessment, Social Responsibility and Security by Design

It is highly desirable that the "dark side" is considered at the beginning of projects. Therefore, it is crucial to develop assessment criteria. It is more effective to build in design control measures during the design phases of the research than to turn to ethical assessment after the

research is completed. Such an anticipatory approach results in “security by design”.

### Networking: the Role of the State and the EU

Another critical element is “networking and networks”, which will be very important in the future. This aspect concerns how scientific organisations are networked to produce results for society. All innovations are based on knowledge, and we must develop knowledge-management systems to manage the dark sides as well. This requires an active role of the EU Commission and European Parliament.

### The Role of Education

There is a need to educate students as early as possible about threats and security issues during their studies at university. Knowledge about these control dilemmas should be added to the universities' curricula.

We also need early media training for children since they will encounter a number of challenges as they increasingly navigate an expanding digital universe. Such media proficiency is even more important since the digital universe can be unfamiliar or even unknown to their parents, who are “digital immigrants”. The future “digital natives” can only cope and shape the digital universe if they are properly informed and know how to protect themselves.

### Bottom-up vs. Top-down Approaches of Control

Actors and decision-makers, as they balance security needs, the requirements set by open democratic societies and the freedom of science, should take active measures against the possible dangers of the dark side of technologies. More promising than top-down measures are bottom-up proposals: Instead of legislation and coercive measures with rather questionable outcomes, the FESTOS team proposes to develop soft and optional measures. These measures, first of all, are based on self-regulation, self-control and the education of engineers and scientists. Codes of conduct, ethical guidelines and educational measures may initially be established on sub-state levels but must be developed into national, Europe-wide and global regimes. While self-regulation and education may be the means of choice in most cases, it has to be stressed that there are also exceptional cases, such as weapons of mass destruction, for instance. In these cases, there exist international regimes to regulate the prohibition of research and development of extremely dangerous technologies and, for the most part, the international community complies with the rules. An example is the ***Biological and Toxin Weapons Convention*** (BTWC), which was the first multilateral disarmament treaty banning the production of an entire category of weapons.

## FESTOS Consortium

The consortium of the project “Foresight of Evolving Security Threats Posed by Emerging Technologies” (FESTOS) consists of the following partners:

Interdisciplinary Centre for Technology Analysis and Forecasting (**ICTAF**) at Tel-Aviv University, Israel

Finland Futures Research Centre (**FFRC**), University of Turku, Finland

Centre for Technology and Society, Technical University of Berlin (**TUB**), Germany

Institute of Sociology (**IS**), University of Lodz, Poland

**EFP** Consulting (UK) Ltd, UK

## Sources and References

http://www.festos.org/