Foresight of Evolving Security Threats
Posed by Emerging Technologies

SEVENTH FRAMEWORK PROGRAMME

FESTOS Alerts

Examples of Potentially Threatening Technologies and Policy Implications

New technologies may give rise in the future to unexpected security threats if abused by criminals or terrorists. FESTOS aims to assess such threats, to propose preventive means and to stimulate discussion on the freedom of research vs. potential dangers.

> "*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*

Imagine a device that makes objects invisible, or a teaspoon that reassembles itself into an insect-like robot, or “bio-kits” for programming living organisms. Science fiction? Not if you imaginatively scan the horizon of emerging technologies. How attractive would such techno-marvels be for future perpetrators?

The following pages (based on FESTOS deliverable D2.3) briefly present 10 examples out of 33 emerging technologies recently examined in the FESTOS horizon scanning and expert survey. For each technology the following aspects were assessed:

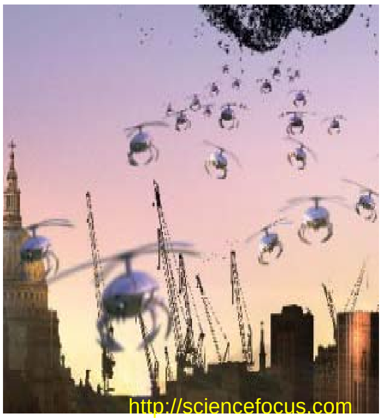
- *When will this technology be sufficiently mature to be used in practice?*
- *How easy will it be to use it for malicious purposes? (1=not easy at all, 5=very easy)*
- *How severe is the security threat posed by this technology? (1=very low severity, 5=very high severity)*
- *The likelihood that the particular technology 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 will it pose a security threat?*

FESTOS horizon scanning covered a wide range of technologies in various fields: from molecular sensors through metamaterials to brain implants and "radio-telepathy"; from cloud computing through "cyborg-insects“ to medical nanobots. Based on the threat assessment some preliminary technology-specific *policy implications* are suggested.

For detailed assessment of 33 potentially threatening technologies please see deliverable D2.3. Narrative scenarios based on selected threats are described in D4.2. The knowledge control dilemma is discussed in D5.2. Final policy recommendations are included in deliverable D6.1.

FESTOS alert: Swarm Robotics

Swarm robotics is a novel approach to the coordination of large numbers of robots, inspired mainly by insects, which show how a large number of simple individuals interact to create collectively intelligent systems. Researchers envision that tiny robots could be mass-produced in swarms and programmed for a variety of applications e.g surveillance, micro-manufacturing, medicine, or cleaning. EU FP7 projects SYMBRION and REPLICATOR develop novel principles of adaptation and evolution for multi-robot systems. This may lead not only to adaptive, evolve-able and scalable systems, but also may enable robot swarms to reprogram themselves without human supervision and new, previously unforeseen, functionality to emerge.

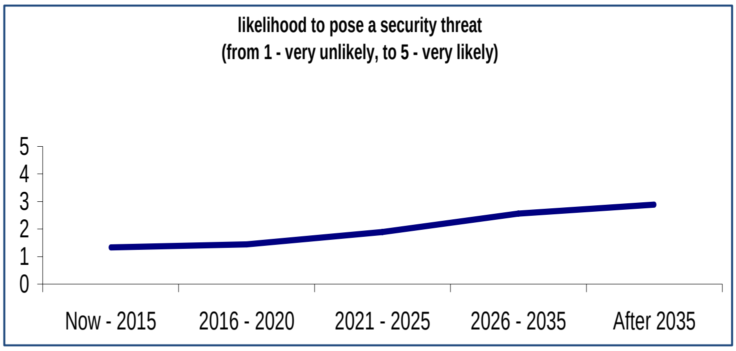


http://sciencefocus.com

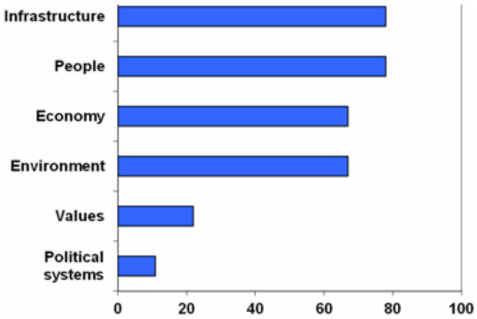
Foresight of Potential Threats:

Robot swarms may pose a threat in the future, if the self adaptation and self-reprogramming are employed for malicious behaviour of the swarm. They could perform new kinds of coordinated attacks in which for example each robot carries a small dose of explosives, combined together to cause a large damage. The ability to relatively easily mass-produce tiny robots for swarms may make such threats more concrete.

Time of sufficient maturity: 2030	Easiness of abuse: 2.9	Threat Severity: 3



Societal Spheres Threatened:



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

Policy Implications:

- Research and development of measures to identify such entities and neutralize them if necessary
- Research for methods that would enable remote-control of swarm robots, as well as measures to prevent hacking, signal disruption and unauthorized use
- Enhancement of research towards 'swarm intelligence' with special attention to embedding special safeguards
- International agreements on capabilities of robot swarms (e.g. minimum size, quantity, functions), and control over the availability of this technology
- Research on impact of masses of small robots on environment, health, transport and other areas of life

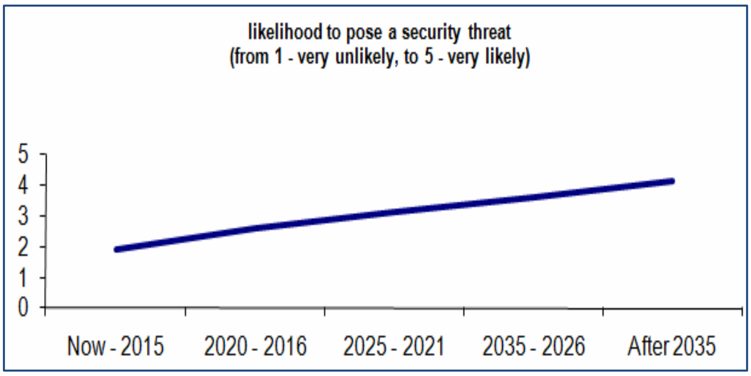
FESTOS alert: Synthetic Biology

Synthetic biology involves large-scale rewriting of genetic codes to create metabolic machines with singular purposes. The vision is to turn synthetic biology into a kind of engineering discipline, with similarly standardized parts – a collection of interchangeable genetic components. Hence, synthetic biology means *in vitro* building of natural biological agents and new artificial agents combinations, from basic building blocks of life. Cells could be programmed as precisely as computers, and indeed might function as tiny machines.

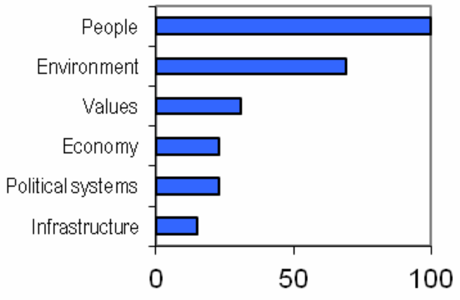
Foresight of Potential Threats:

Such technologies in wrong hands could facilitate production of current and new biological warfare agents, without special need of large biotech production facilities. Engineered organisms could be released into the environment with orders to attack. "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.

Time of sufficient maturity: 2018	Easiness of abuse: 3.2	Threat Severity: 3.4



Societal Spheres Threatened:



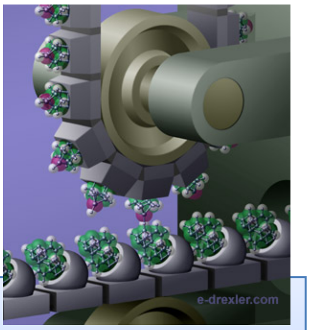
The threat likelihood increases with time. The most threatened societal spheres are people and the environment. In addition, attention to the potential impact on values should be paid.

Policy Implications:

- Raising awareness to potential threats associated with abuse of biotechnologies to create or modify biological organisms in such ways that pose inherent risks of bio-terror
- Developing effective ways to control instrumentation and knowledge dissemination, in the areas of bioengineering and synthetic biology, which pose obvious threats of creating cheaper and widely accessible tools for bioweapons
- Additional foresight study on potential (surprising) implications, for example, development of "ethnic" bio-weapons

FESTOS alert: Molecular Manufacturing

By Nanotechnology-enabled Molecular Manufacturing various desired products could be assembled "bottom up", namely atom by atom or molecule by molecule, possibly in small "nanofactories".



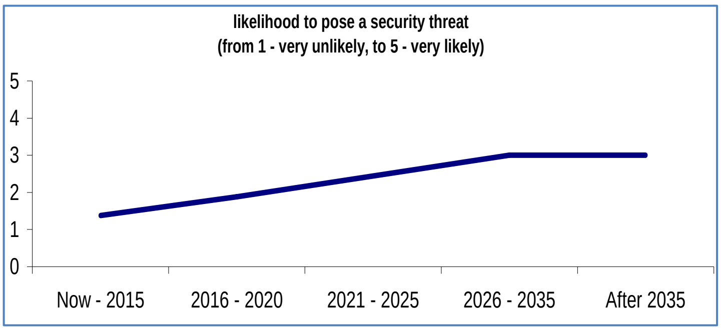
Foresight of Potential Threats:

Mulecular manufacturing could be used to create new hazardous materials, or new types of weapons. If versatile and sufficiently small “nanofactories” are developed, such items could be created anytime anywhere, including in sensitive locations places where no weapons are allowed. 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…"

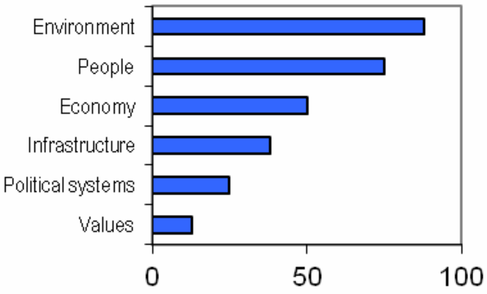
Time of sufficient maturity: 2023

Easiness of abuse: 2.5

Threat Severity: 2.5



Societal Spheres Threatened:



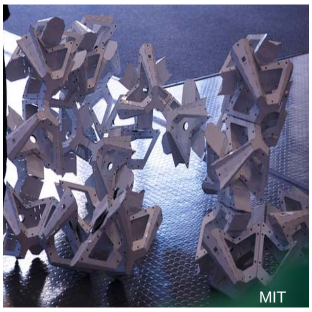
The threat likelihood is increasing with time. The most threatened societal spheres are the environment, followed by people. Impact is envisioned on the economy and infrastructures as well.

Policy Implications:

- Conducting more in-depth research on the potential effects of molecular manufacturing
- Enhanced activity in R&D of detection of new material and methods of identification of unknown materials
- Applying security-by-design means tailored to molecular manufacturing devices (“nanofactories”)
- Developing special nanosensors to detect harmful materials in various environments

FESTOS alert: Programmable Matter

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” or “Claytronics” this emerging field combines chemistry, information theory, and programmability to build information directly into materials.



MIT

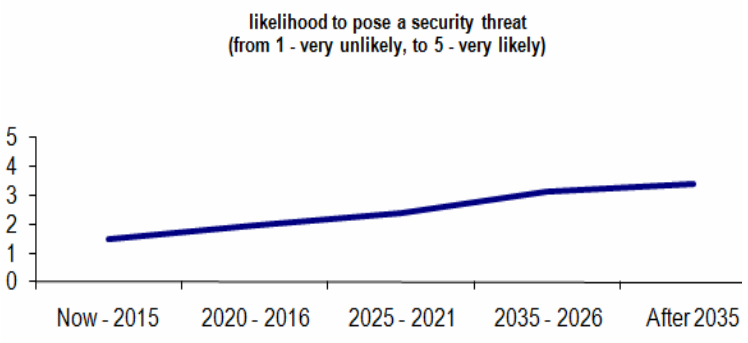
Foresight of Potential Threats:

One can imagine malicious use of easily reconfigurable tools with perfect performance, including weapons (that could be programmed to look like ordinary items and pass security checks), readily adaptable to changing conditions and requirements and enabling a perfect camouflage of any object.

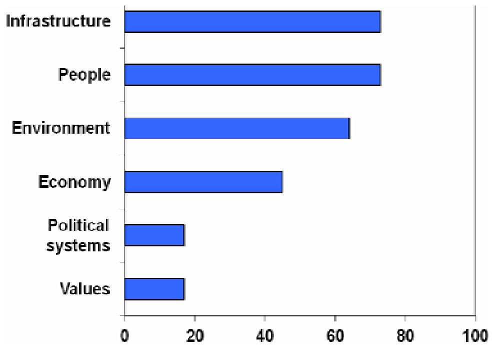
Time of sufficient maturity: 2030

Easiness of abuse: 2.3

Threat Severity: 2.8



Societal Spheres Threatened:



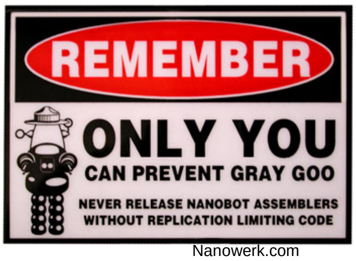
The likelihood to actually pose a security threat increases in the next 25 years or so. The most threatened societal spheres are people and infrastructures, followed to a lesser degree by the environment and the economy.

Policy Implications:

- Supporting R&D towards detection technologies that would be able to detect or identify non-metal weapons and other dangerous objects
- Developing new methods of security checks to cope with new threats of perfect camouflage. Advanced methods for identifying malicious intentions would be helpful.
- Research on possible tailored countermeasures for programmable matter, *e.g.* "self destruction" code/signal in case of unauthorised use

FESTOS alert: Self-replicating Nano-assemblers

Nanoassemblers are an important potential outcome of the vision of molecular nanotechnology, possibly leading to molecular manufacturing. Nanoassemblers could self-replicate exponentially, and they would autonomously assemble almost anything, molecule by molecule.
Uncontrolled "runaway replication" has been described in fictional/speculative scenarios of futuristic nanotechnology.


REMEMBER
ONLY YOU
CAN PREVENT GRAY GOO
NEVER RELEASE NANOBOT ASSEMBLERS
WITHOUT REPLICATION LIMITING CODE

Nanowerk.com

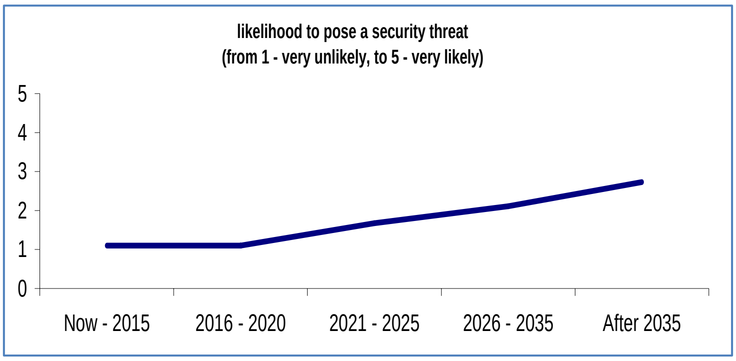
Foresight of Potential Threats:

While uncontrolled "runaway replication" is considered by experts as highly unlikely and can be prevented by appropriate safeguards, one can not preclude intentional malicious design of such devices for wrongdoings.

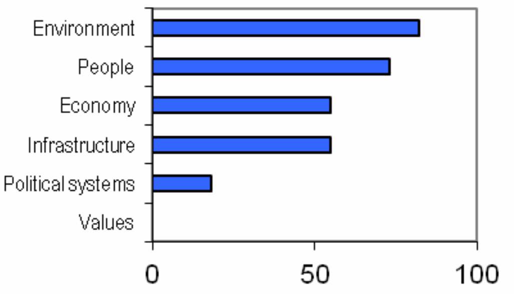
Time of sufficient maturity: 2030

Easiness of abuse: 2.75

Threat Severity: 2.9



Societal Spheres Threatened:



The likelihood of the threat is increasing over time.
The most threatened societal spheres are people and the environment, followed by infrastructures and the economy.

Policy Implications:

- Conducting research on possible self-replicating materials, biological and non-biological, which might include prions (the proteins that cause *mad cow disease*) as well as other materials that do not follow the biological paradigm
- R&D on potential safeguards that could prevent uncontrolled self-replication
- Tracking and regulating genetic engineering of bacteria for commercial purposes
- Investing in *meta-research* to understanding of cellular mechanisms related to manufacturing of “engineered” molecules.

FESTOS alert: Nanotechnology-enabled Brain Implants

Various biomedical devices implanted in the central nervous system could control motor disorders or 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, and might find use in the military as well. Debates still abound regarding the potential use of brain implants for enhancement of the brain functions of healthy persons, including an "upgrading" of mental capabilities.

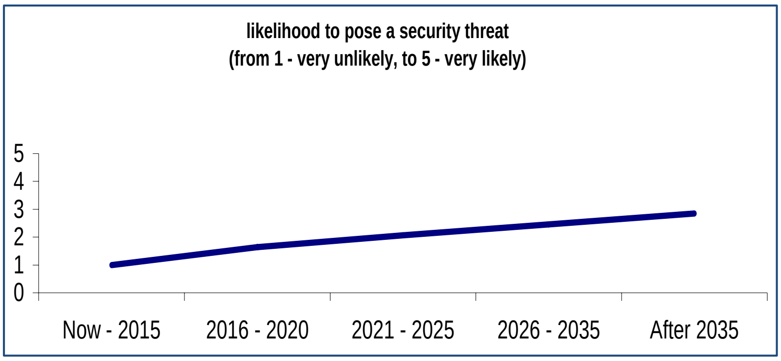
Foresight of Potential Threats:

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".

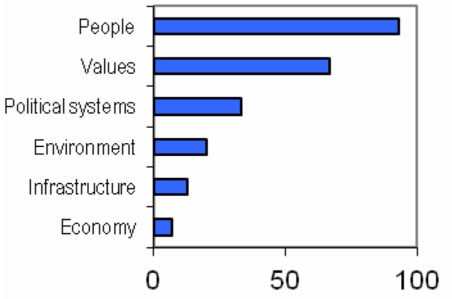
Time of sufficient maturity: 2030

Easiness of abuse: 2.7

Threat Severity: 3



Societal Spheres Threatened:



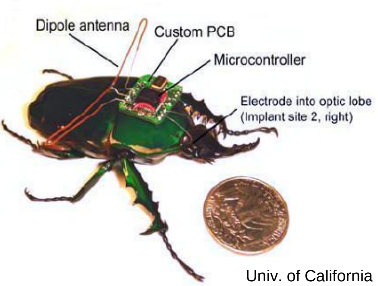
The threat likelihood rises with time. The most threatened societal sphere is people. As could be expected in such a sensitive topic, the experts foresee a very significant impact on values. Political systems could be affected as well.

Policy Implications:

- Research towards identification of people with malicious intentions should be enhanced
- Research of systems to support the identification of potential aggressors should be part of the R&D program
- Studies and social research of values in the era of wide use of sophisticated implants should be promoted
- Research on built-in safeguards/countermeasures tailored to brain implants

FESTOS alert: Cyborg Insects

Insects controlled through implanted electronics connected to the nervous system. Researchers envision living insect-based communication networks (for sensing, surveillance, etc). Another suggested application is protecting agriculture from locusts (diverting the locust swarms by a "cyber locust"). Advanced capabilities could be offered by micro/nano technologies.



Univ. of California

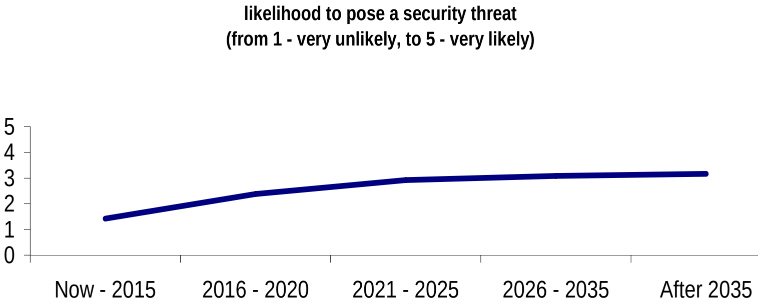
Foresight of Potential Threats:

It is conceivable that cyborg insects could be used by perpetrators for harming people, spying or other malicious activities. Swarms of such insects could be directed at agricultural areas for harmful purposes e.g. to damage crops.

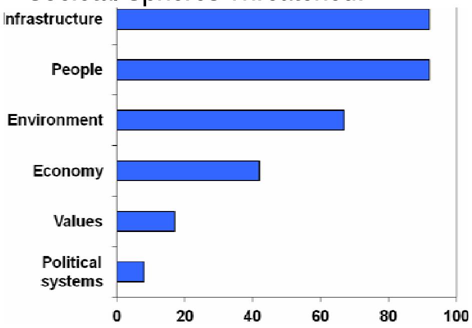
Time of sufficient maturity: 2023

Easiness of abuse: 3.3

Threat Severity: 3.1



Societal Spheres Threatened:



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.

Policy Implications:

- R&D on measures for identification of cyborg insects and for their neutralization if necessary.
- Study on implications of potential combination of swarm robotics with cyborg insects; Enhancement of research towards 'swarm intelligence' with special attention to embedding special safeguards
- Research for methods that would enable remote-control of cyborg insects with embedded measures to prevent hacking and signal disruption

FESTOS alert: Smartphone technologies mash-ups

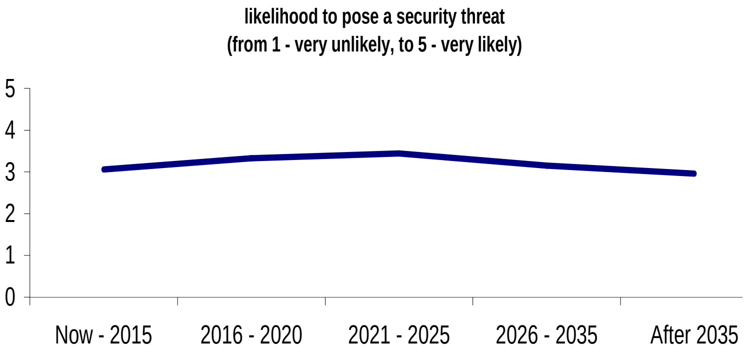
New cellphones are equipped with video cameras, GPS, Internet connectivity, and more. As these capabilities are “mashed up” (i.e., brought together in new combinations and in tandem with new Internet-based services), including emerging "Augmented Reality“ features and various sensors, they turn the cellphone into an extremely versatile communications and surveillance device.

Nokia

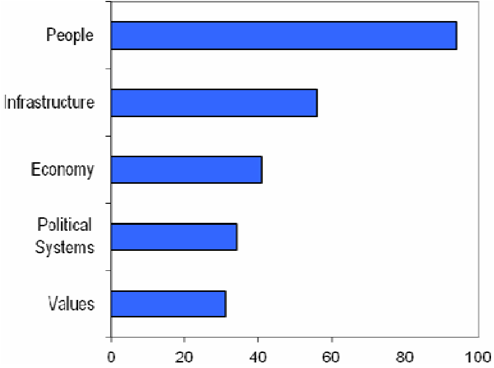
Foresight of Potential Threats:

New mobile phones could enable “Open Source Intelligence” to be carried out discretely and without any special equipment. A smartphone with a video camera and a GPS device would enable a terrorist or a criminal to easily collect location-based video imagery of a possible target area. New combinations with advanced Augmented Reality and other features could be even more useful for planning and executing malicious actions.

Time of sufficient maturity: 2012	Easiness of abuse: 3.7	Threat Severity: 3.5



Societal Spheres Threatened:



The threat likelihood is relatively high in the coming years and is expected to decrease in the next decade. The most threatened societal spheres are people and infrastructures, followed by the economy. It should be noted that the threats to political systems and to values are also considerable.

Policy Implications:

- More in-depth studies are needed on specific threats posed by abuse of the next generations of smartphones
- R&D on built-in safeguards tailored to smartphones, taking into account the easiness of abuse as revealed by the FESTOS survey
- Research on possible countermeasures such as remote de-activation of certain smartphone functions (e.g. Augmented Reality features, sensors)

FESTOS alert: Cloud Computing

Cloud computing 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. Cloud computing was defined by Gartner as one of the "top 10 strategic technologies" for 2011

cloudcomputingoffers.com

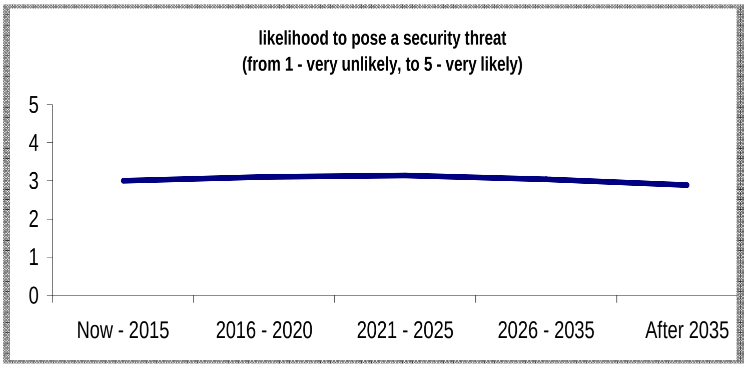
Foresight of Potential Threats:

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

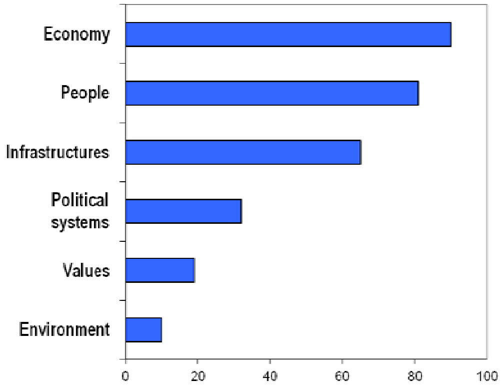
Time of sufficient maturity: 2012

Easiness of abuse: 3.3

Threat Severity: 3.5


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

Societal Spheres Threatened:



The threat likelihood is slightly decreasing in the long range.
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.

Policy Implications:

- More in-depth studies on specific threats posed by potential abuse of various Cloud Computing applications
- Developing Cloud Computing-specific security-by-design principles
- R&D on potential safeguards that could be embedded in Cloud Computing systems
- Regulations for responsible development and use of Cloud Computing systems

FESTOS alert: Internet of Things

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 where people are surrounded by various interconnected devices, unobtrusively embedded in their surroundings and easily accessed via intuitive interfaces. Computers are everywhere but they recede into the background and become "invisible". Such intelligent environment is expected to seamlessly respond to the presence and needs of individuals.

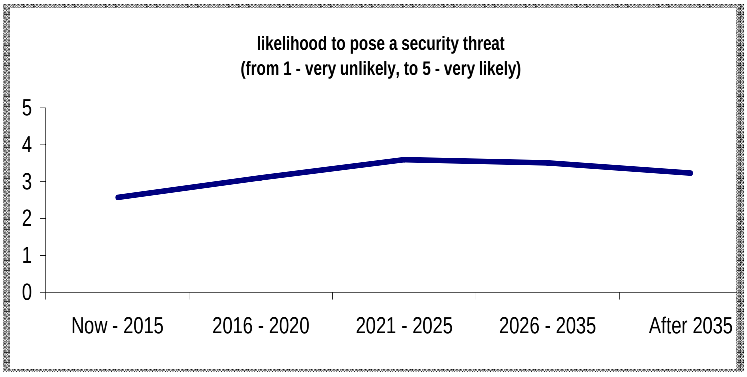
Foresight of Potential Threats:

Experts have warned that the security risks are first of all related to privacy. Will these technologies offer new opportunities for hacking, identity theft, disruption, and other malicious activities? As soon as the ordinary citizen becomes dependant on systems interconnected through IoT, the simple act of shutting them down by terrorists could create chaos.

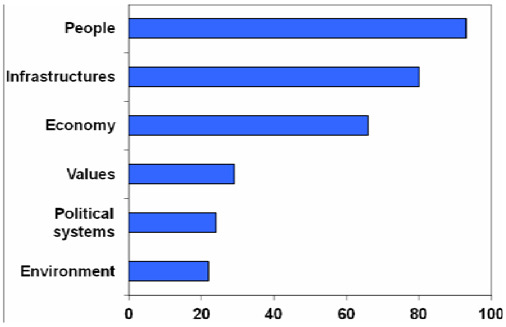
Time of sufficient maturity: 2018

Easiness of abuse: 3.6

Threat Severity: 3.5



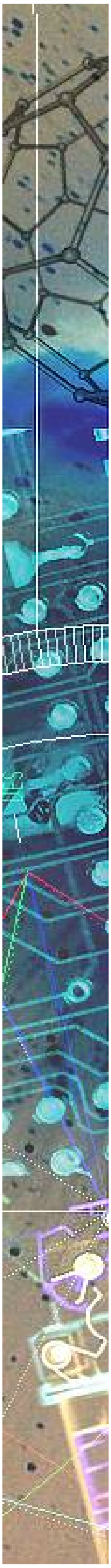
Societal Spheres Threatened:



The threat will increase over time with slight decrease in the long range. The most threatened societal spheres are people and infrastructures, followed by economy. However, it should be noted that the threat to values should not be underestimated.

Policy Implications:

- R&D on safeguards based on quantum technologies for communication between 'things', thus making the system "unhackable" (possibly under the FET program), and on safeguards that could be embedded in various components/layers of the IOT systems
- Developing IOT-specific security-by-design principles
- More in-depth studies on specific threats posed by potential abuse of IoT applications
- Research on portable devices that would be able to shut down all network activity in certain places
- Identification of selected high officials in critical positions that, as a precaution, would have to be disconnected from certain uses of the Internet of Things



The FESTOS consortium:

Interdisciplinary Center for Technological Analysis and Forecasting at Tel Aviv University, Israel

University of Turku, Finland

University of Lodz, Poland

EFPC (UK) Ltd.

Center for Technology and Society, Technische Universität Berlin, Germany

FESTOS contacts:
www.festos.org
Dr. Yair Sharan, sharany@post.tau.ac.il

> *"Unless we invent new threats, we won't be able to prevent them."*
> *Karlheinz Steinmüller*