Emerging Technologies and Evolving Security Challenges in the Coming Decades

Security in Futures – Security in Change, Turku, 3/6/2010

Yair Sharan, Aharon Hauptman

Interdisciplinary Center for Technology Analysis and Forecasting (ICTAF) at Tel-Aviv University

ICTAF

Interdisciplinary Center for Technology Analysis and Forecasting

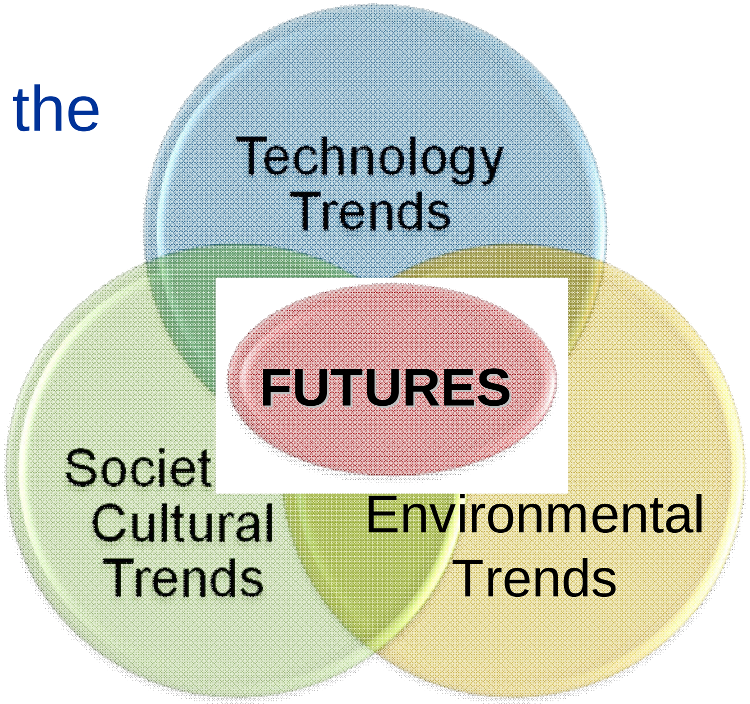
- Based at Tel-Aviv University (TAU)
- Independent non-profit organization
- Interdisciplinary
- Broad spectrum, high level core staff
- Management of external expert teams

ICTAF's Mission

■To be Israel's leading institute in *Technology Assessment and Foresight*

■To assist policy-makers in forward-looking planning

■To harness the knowledge of TAU for the benefit of the economy and society



Introduction

- Besides their huge contribution to quality of life, scientific progress and new technologies have intrinsic dangers
- Abuse is one of the dangers posed by emerging technologies
- Threats include crime, terrorism, man made catastrophes…
- New terrorist profile: larger number of potential terrorists and supporters with high levels of technical & scientific knowledge

More reasons to be worried

- Narrowing gaps between civilian and military products/applications.
- Miniaturization and cost reduction of military technologies facilitate terrorism (easier procurement, theft, concealment…)
- Potentially dangerous technical information available on the net

- Global networks of terrorists interconnected by the Internet
- Difficult to control and prevent sensitive knowledge dissemination in free societies

The Dark Side

Prof. Leonard Kleinrock, UCLA (Internet Pioneer, the Dan David prize winner):

The Internet is a perfect formula for employing the dark side of technology -

- Easy
- Quick
- No cost
- Anonymous

"We didn't think about it (the dark side) while developing it…"

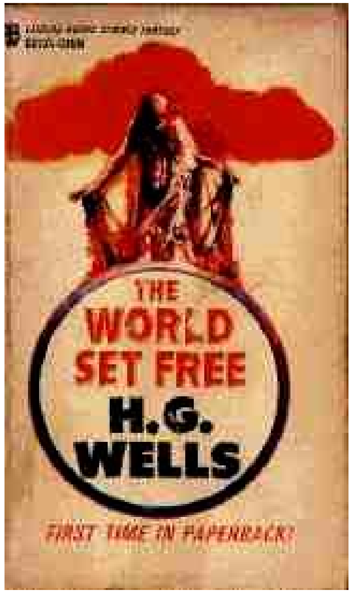
Tel-Aviv, 11 May 2010

The Foresight of H.G. Wells

*"…these **atomic bombs**…were strange even to the men who used them…"*

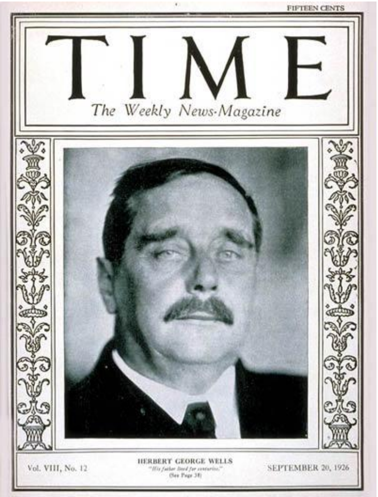
"…a man could carry about in a handbag an amount of latent energy sufficient to wreck half a city."

H. G. Wells, "The World Set Free", 1913



"Will there be no Foresight until those bombs begin to rain upon us?"

H.G. Wells, *WANTED - PROFESSORS OF FORESIGHT!*
BBC, 19 November, 1932

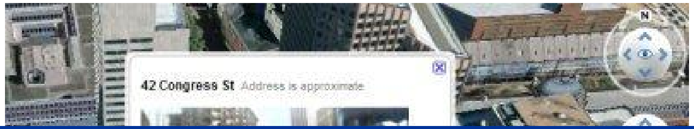


FP7 Project FESTOS: Foresight of Evolving Security Threats Of emerging Technologies

Terrorists use "Google Earth/ Street View"

An Indian Court has been called to ban Google Earth because it helped planning the terror attacks that killed more than 170 people in Mumbai

(Times Online, December 9, 2008)



Would a project like FESTOS in 1998 (or before) envision such a threat?

FESTOS challenge: to identify the future equivalents of "Google Earth" in 2019 - 2029…, and propose preparedness means.

www.festos.org

ICT threats

The Internet's nearly infinite connections represent ***"unprecedented vulnerabilities to espionage and covert attack."***

Cetron, M., O. Davies, "Ten Critical Trends for Cybersecurity", The Futurist, Sept-Oct 2009

Terrorists could break into computer systems and launch an attack on a nuclear state – triggering a catastrophic chain of events. ***"This may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb themselves"****.*

A study by the International Commission on Nuclear Non-proliferation and Disarmament (ICNND), 2009

ICT threats

- Attack of infrastructure control systems (Energy, transportation, water)

- Attacks on air navigation facilities in bad visibility conditions

- Targeted attacks by HED (High Explosive Device) and electronic warfare against critical civilian communication infrastructures (for example, flight control facilities at civilian airports at peak traffic hours).

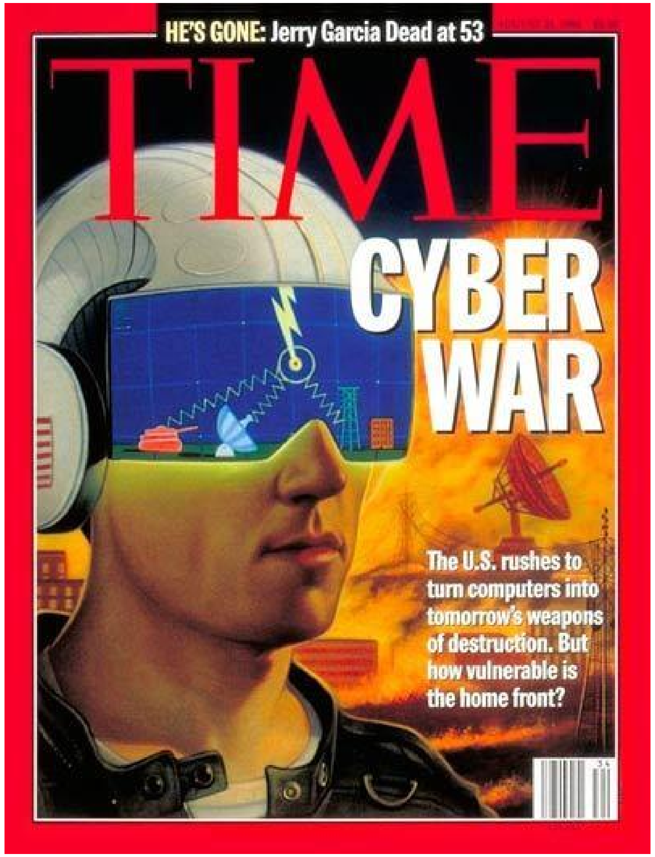
ICT threats

“None is immune to cyber-attack… Countries have become "critically dependent" on technology for commerce, finance, health care, emergency services and food distribution,"
"The next world war could happen in cyberspace”

H. Toure, Secretary-general of ITU, Sept 2009

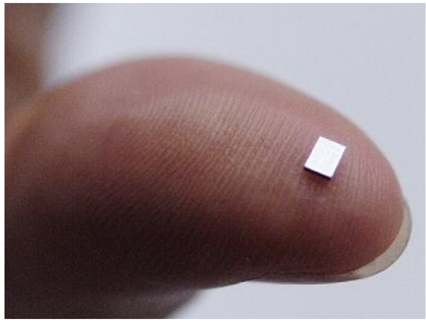
*Breaches in e-commerce are already running to **hundreds of billions**.*

C. Solari, Alcatel-Lucent's VP on quality, security and reliability


HE'S GONE: Jerry Garcia Dead at 53
TIME
CYBER WAR
The U.S. rushes to turn computers into tomorrow's weapons of destruction. But how vulnerable is the home front?

RFID – specific threat

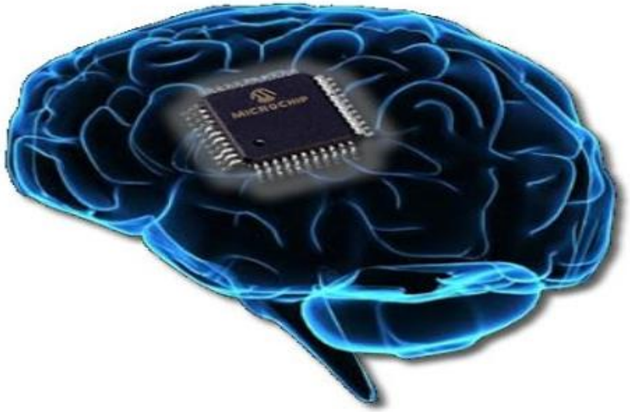
If all products have RFIDs, robbers might use RFID readers to select potential victims by obtaining information about purchased expensive items.



Implants – specific threat

Dr. M. Gasson from the University of Reading - the first person in the world to be infected by a computer virus.

“Huge implications for implantable computing devices such as heart pacemakers and cochlear implants…



As the implants technology develops, they become more vulnerable to computer viruses

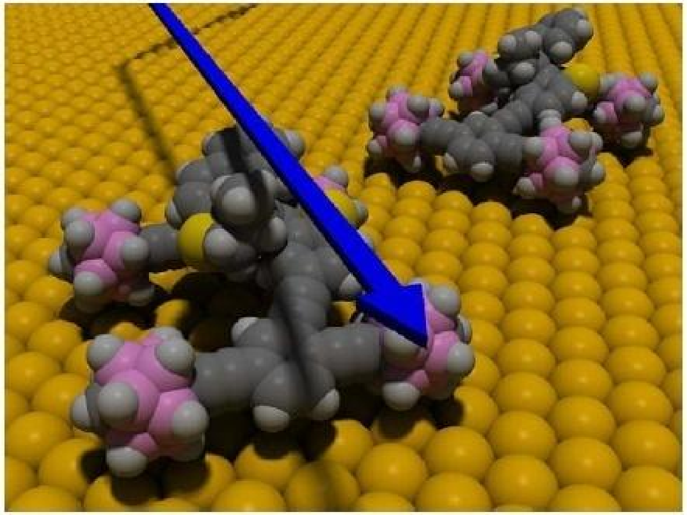
ScienceDaily (May 26, 2010)

Nanotechnologies highlights

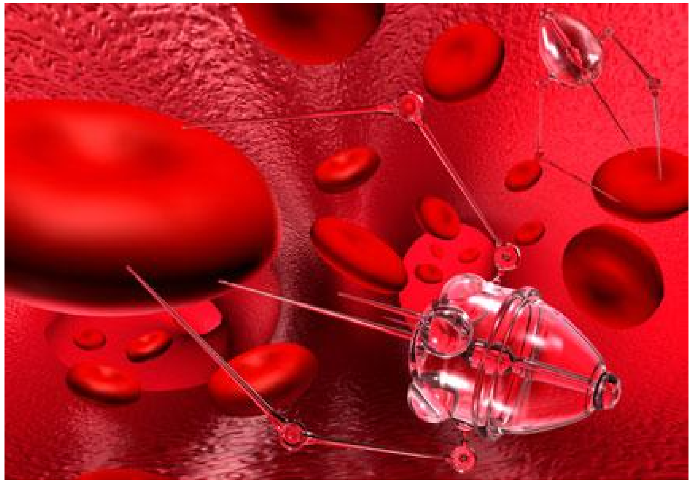
Manipulating matter on the nanoscale

Examples of applications:

- Superstrong lightweight materials
- Highly efficient photovoltaic and fuel cells
- Molecular electronics,
- Targeted drug delivery systems
- “Lab on a chip”
- Nanotechnology-based propellants, explosives
- Biocompatible implants…



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



More futuristic: Molecular assemblers and (self-replicating?) nanobots.

Highly energetic nanoparticles

- Nanoparticles react much more effectively (large surface-to-volume ratio)

- New molecules with high energy density could be created by molecular nanotechnology methods

- More lethal explosives, more efficient propellants (e.g. for home-made long-range rockets)

- Sending powerful explosives in envelopes by post…

More Nanothreats

- Metalless weapons made of undetectable nanocomposites
- “Artificial viruses” and other forms of "Nano-weapons“
- Networks of almost invisible tracking sensors ("smart dust"),

► Terrorists or criminals use "clouds of nano-machines capable of excreting multiple forms of toxic chemicals and biological hazards in airports”

► “stealthy new means of mass-killing”

(Millennium Project, 2009)

Biotechnology threats

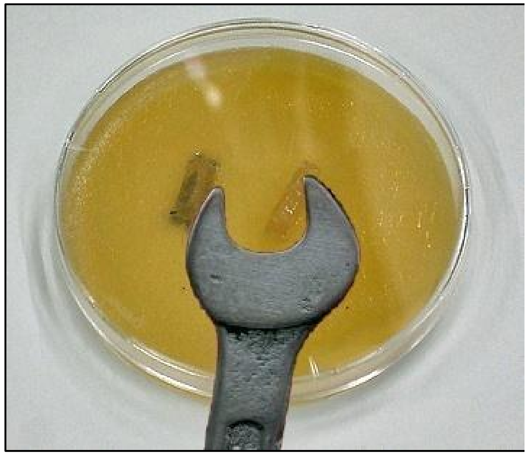
- Creation / Purchase of biowarfare agents (microbes, viruses, and toxins) **using available commercial / scientific products.**
- Creation of new bio-agents and toxins, using synthetic biology and structural chemistry methods.

  - Unknown agents, undetectable.

  - Antibiotics resistance.

Synthetic Biology

The vision: “biobricks” – interchangeable genetic components. Programming living organisms in the same way a computer scientist programs a computer”



Craig Venter’s vision: ***"an operating system for biologically-based software.“***

Latest news:

“another step in the quest to create synthetic life, by synthesizing an entire bacterial genome and using it to take over a cell.”

“the first self-replicating species we’ve had on the planet whose parent is a computer.”

New York Times, 20/5/2010

Synthetic Biology threats

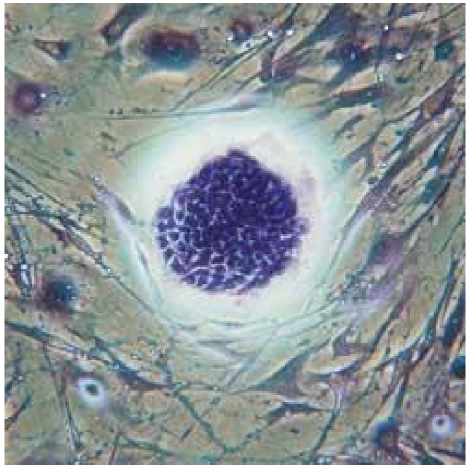
Bio-hacking
Bio-terror

"Ultimately synthetic biology means cheaper and widely accessible tools to build bioweapons, virulent pathogens and artificial organisms that could pose grave threats…"

Report by Ottawa-based ETC Group (one of the advocacy groups that want a ban on releasing synthetic organisms pending wider societal debate and regulation)

Induced Pluripotent Stem Cells (iPS cells)

In July 2009 scientists turned skin cells from adult mice into iPS cells - functionally equivalent to embryonic stem cells.



Potential threats:

“Rogue scientists might attempt to clone humans."
"With just a little piece of your skin, anyone could have your child -- even an ex-girlfriend or neighbor…. with a little practice, any IVF clinic in the world could probably figure out how to get it to work."

(Dr. Robert Lanza, a stem cell researcher)

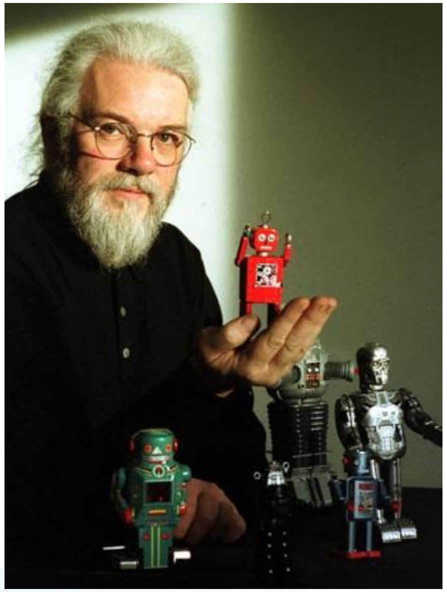
Imagine criminals using this to fabricate fictitious fraternity suits against billionaires…

Robotics Threats

Smarter, smaller, cheaper robots increase the danger that they will become available to terrorists

“It may not be long before robots become a standard terrorist weapon to replace the suicide bomber.”

“it wouldn’t require a lot of skill to make autonomous robot weapons.”
(N. Sharkey, Sheffield Univ,. UK)



Threats of small toy robots

Toy and amateur robots should be limited (by law) in mobility, size and sensing/actuating capability.
J. Altmann

“Covertly enter offices or houses – even through the crack under the door, or through an open window… Small robots could 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.“

J. Altmann

Robotic swarms

Coordination of large numbers of robots, inspired by swarms of insects, birds, etc.

SYMBRION

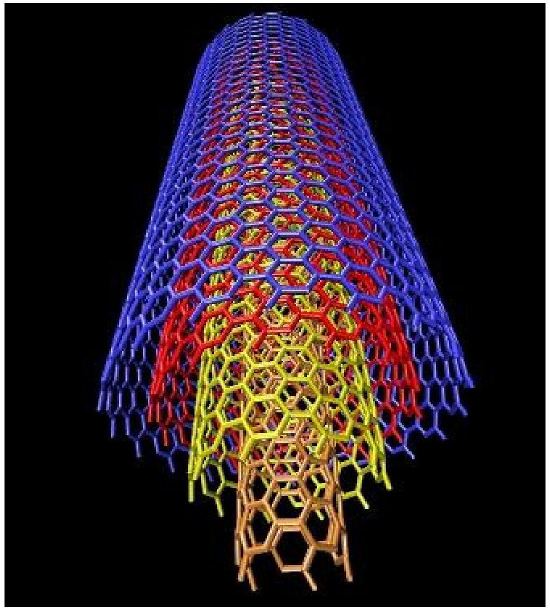
EC projects:
”I-Swarm”, ”Swarm-bot”
“SYMBRION” and “REPLICATOR.

I-SWARM envisions tiny (4 mm) robots mass-produced in swarms and programmed for surveillance, micromanufacturing, medicine, cleaning, etc.

Potential threats:
New kinds of attacks. Each robot carries a small dose of explosives but the combined effect is huge.
Self adaptation and self-reprogramming could be intentionally employed for malicious behaviour of the swarm
The ability to relatively easily mass-produce tiny robots for swarms may make the threats more concrete.

New Materials – Highlights

New technological capabilities have enabled going down to the nanoscale and molecular states of materials and new ways to create, process, and use them.

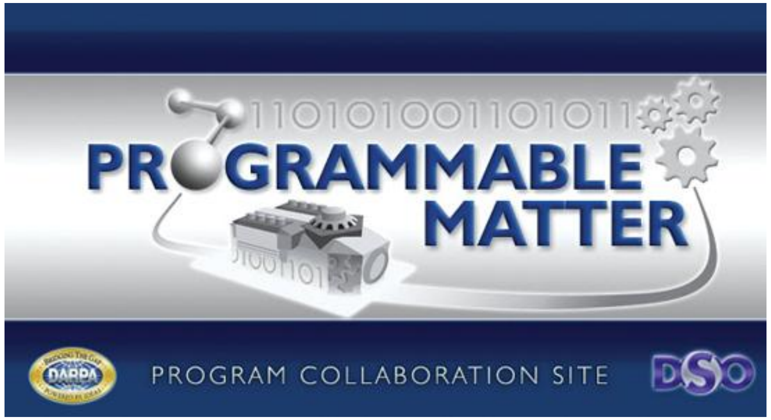


Examples of the richness of this field:

- High-performance alloys,
- nanocomposites,
- super-strength materials,
- carbon nanotubes and other nanomaterials,
- new biological or bio-inspired materials,
- “smart materials” and "multi-functional materials" that respond in a desired manner to changing external conditions.

Programmable Matter: Potential (speculative?) threats

DARPA funds research to create materials that can be programmed to self-assemble to perform a desired function, and then disassemble.



Threats?

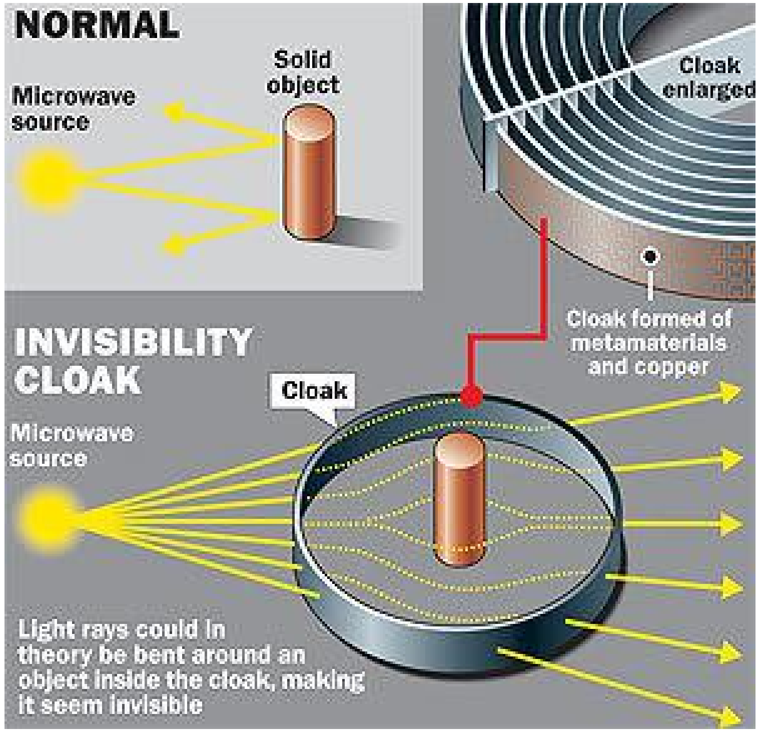
- New types of weapons that can pass security checks: Programmed to look like ordinary items, and than transform into a weapon?

- A perfect camouflage of any object?

- Reconfigurable tools with perfect performance, including weapons, readily adaptable to changing conditions and mission requirements.

Metamaterials; “Invisibility Cloaking”

“Metamaterials" (with negative refractive index) can hide objects from sight, or make them appear as other objects.


NORMAL
Microwave source
Solid object
Cloak enlarged
Cloak formed of metamaterials and copper
INVISIBILITY CLOAK
Cloak
Microwave source
Light rays could in theory be bent around an object inside the cloak, making it seem invisible

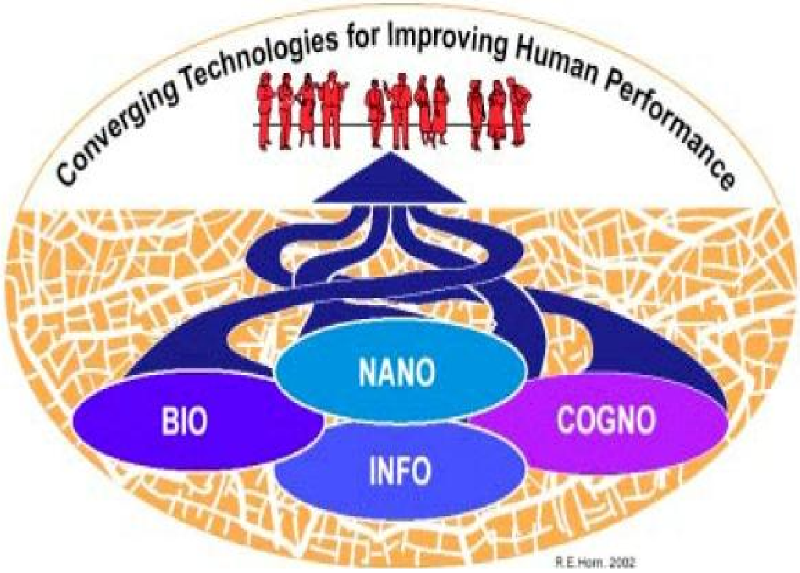
Potential threats:

Making an object (or person?) invisible, or looking as something different (sophisticated active camouflage). Imaginative possibilities of abuse…

Converging Technologies: NBIC

Info, bio, nano complement each other and have begun to join forces with cognitive science.
Synergism is also possible with psychology and other social sciences. This convergence promises to transform every aspect of life.

(A. Nordmann, "Converging Technologies – Shaping the Future of European Societies", EC HLEG Report, 2004)

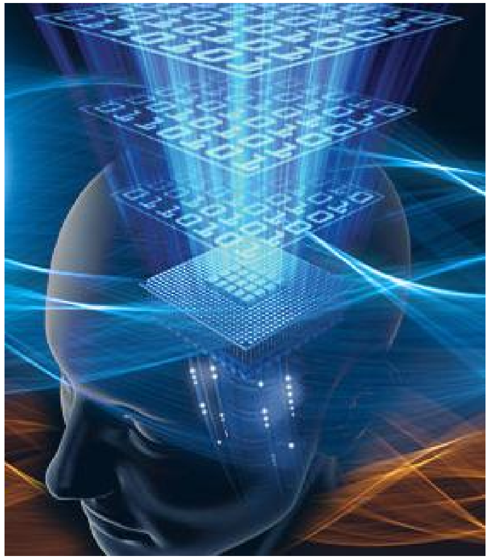


CT include neuromorphic engineering, artificial organs, enhancing learning and sensorial capacities.
Nanobiosystems may become essential to human healthcare.
The functions of the brain and nervous system are expected to be measured (and enhanced?) with relevance to cognitive engineering.

Nanotechnology-enabled brain implants and “synthetic telepathy”

Neural interfaces have been developed to control motor disorders or control of external devices by “thought power”.

UK MOD think tank report:
"By 2035, an implantable info chip could be developed and wired directly to the user’s brain. […] *synthetic telepathy, including mind-to-mind or telepathic dialogue.”*



Potential Threats:

“Enforcing violence", advanced form of "brainwashing", thought/behavior control of people, causing social unrest, violence, etc.
Recruitment of suicidal candidates

Remote control of humans?

“Shaking The World: Galvanic Vestibular Stimulation as a Novel Sensation Interface”

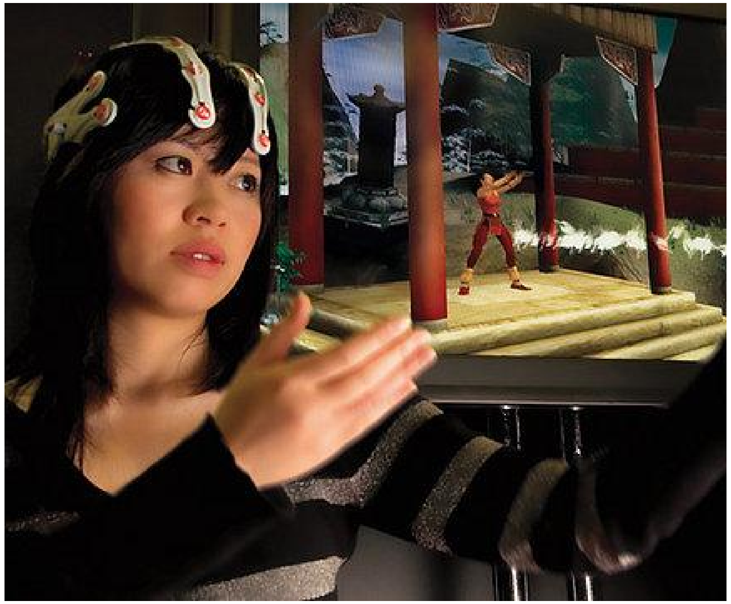
Weak Current Moves Your Balance.

“it would be useful for crowd control to have people walk in the same direction and sway to avoid collisions” (Source: NTT)

Brain-Computer Interface – "Mind Reading" commercial gadgets

- 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".

- Toyota announced in June 2009 that it has developed a way of steering a wheelchair by brain waves.



BCI: Potential threats

Distortion in the communication between users and gadgets. Hacking such a device could enable influencing the user's actions, perhaps even thoughts.

Expert interviewed by CNN: *“…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?“*

A recent article in Wired:
Why anyone would want to hack into someone else’s brain?
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.

CATEGORIES OF POTENTIAL THREATS

1. Disruption: hacking of systems and disrupting their proper functioning:

■ Jamming the communications in collision avoidance systems.
■ The "Internet of Things", where everything is interconnected, poses new "opportunity" for hacking and abuse.

This straightforward category is increasingly important with our growing dependence on technologies.

2. Availability & proliferation of technologies that once were confined to the military or to unique laboratories, and were prohibitively expensive:

■ Commercial off-the-shelf (COTS) components for “poor man’s SIGINT”
■ Equipment for generating EMP
■ Some materials for chemical or biological terrorism (as the underlying knowledge and lab equipment become widely accessible)

CATEGORIES of POTENTIAL THREATS

3. Surprising abuse of new technologies developed for completely different, beneficial purposes:

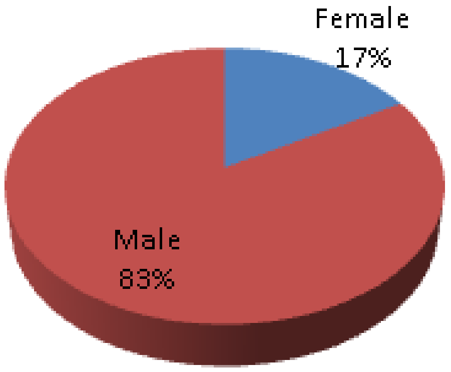
- Small (but sophisticated) toy robots
- Networked games - to recruit new members to hostile organisations
- Synthetic biology - to engineer bacteria that instead of producing fuel consume it

Category 3 is the most interesting:

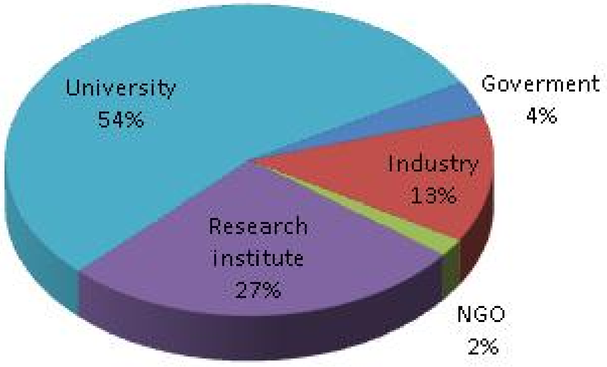
Most unexpected potential threats - signals to "wild cards".

FESTOS Expert Survey

Gender

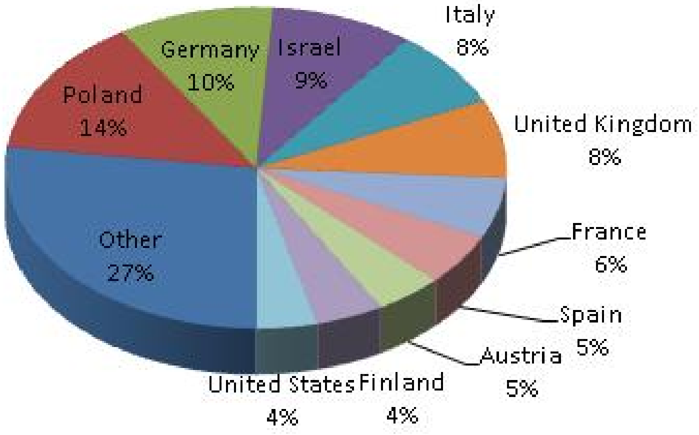


Affiliation

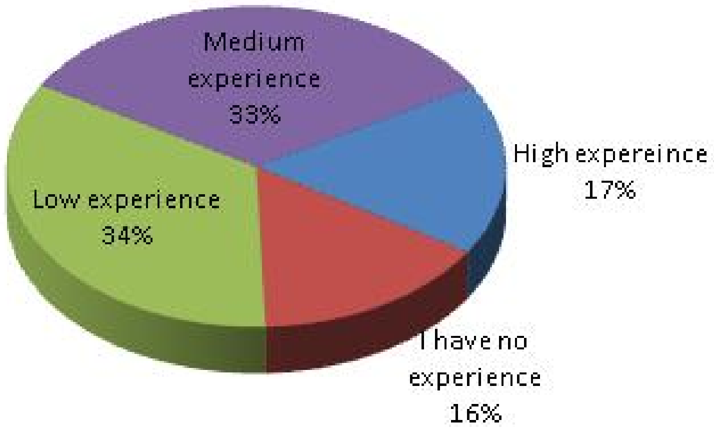


250 respondents

Countries



Security experience



Nanotechnology

1. Molecular Manufacturing

Assembling products "bottom up", molecule by molecule

2. Self-replicating nanoassemblers

Uncontrolled "runaway replication" has been described in fictional/speculative scenarios of futuristic nanotechnology.

3. Medical Nanorobots

Could be one of the next steps in medical diagnostics and treatment

4. Tailored nanoparticles

Designed for use in commercial products, can be hazardous to health.

5. Energetic nanomaterials

Enable powerful propellants and explosives

6. Molecular sensors (sensors with molecular precision)

Will be able to detect where a person has been by sampling environmental clues. Advanced nano-diagnostics could make people "molecularly naked".

Biotechnology

1. Synthetic Biology

"programming living organisms like programming a computer".

2. DNA-protein interaction

One of possible ways to control DNA expression

3. New gene transfer technologies

New devices/ methods for transferring genes from one living organism to another

4. Induced Pluripotent Stem Cells (iPS cells)

Turning ordinary cells into iPS cells, functionally equivalent to embryonic stem cells.

5. Bio-mimicking for fluids mixing at extremely small scales

Speeding up biomedical reactions by filling reservoirs with tiny beating rods that mimic cilia. Perhaps useful for preparation of toxic substances that need very small scale mixing and are harmful in micro quantities

6. Multiplex Automated Genome Engineering (MAGE)

Quick creation of billions of unique gene strains for large-scale programming and rapid evolution of cells. Might be more useful than building genomes from scratch.

New Materials

1. Metamaterials with negative light refraction index

Could enable invisibility "cloaking", and creation of 'super-lenses‘

2. Water catalysing explosive reactions

In hot and dense environments water plays an unexpected role in catalysing complex explosive reactions.

3. Programmable matter

Materials programmed to self-assemble, alter their shape and properties to perform a desired function, and then disassemble

4. Personal rapid prototyping and 3-D printing machines

Inexpensive printers able to self-copy and to use a variety of materials.

5. Future fuels, processes and structural materials for nuclear technologies

Enable to determine the mechanisms of irradiation-induced swelling, predict the behaviour of fuel elements in reactor cores, etc

6. Crystalline polymers, polymer blends, multilayer assemblies

e.g. for gas separation, atmosphere control, reduction of gas permeability...

Converging Technologies: NBIC

1. Nanotechnology-enabled brain implants

"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".

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

Enabled by direct conversion of neural signals into radio signals and vice versa.

3. Cyborg Insects

Insects controlled through implanted electrical stimulators.

4. Brain-Computer Interface – "Mind Reading" commercial gadgets

Toy manufacturers plan to sell a game which involves players levitating a ball "using thought alone." Toyota has developed a wheelchair steered by brain waves.

5. Human enhancement/augmentation based on NBIC convergence

Unprecedented enhancement of human performance: alteration and augmentation of physical and mental abilities. Some envision that human and machine intelligence will converge over the coming century (the Cyborg vision).

Robotics

1. AI-based Robot-Human Interaction and Co-existence
“Social robots" with AI, with which people have emotional and even intimate interactions.

2. Autonomous & semi-autonomous mini robots: Toys and amateur objects

3. Robotic artificial limbs

4. Ethical Control of Robots
Ethical control becomes a new field in computer science. The application of autonomous systems in civilian environments will lead to the use of such ethical control systems.

5. Swarm Robotics
Coordination of large numbers of robots, inspired mainly by natural swarms. Based on the EU project I-SWARM, tiny (about 4 millimeters size) robots could be mass-produced in swarms and programmed for a variety of applications.

Information & Communication Technologies

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

A network of everyday objects (food items, home appliances, clothing, etc), as well as various sensors, addressable and controllable via the Internet.

2. Radio-frequency identification (RFID) and "RFID-dust”

3. Smart mobile telephone technologies mash-ups

New cellphones are equipped with video cameras, GPS, Internet connectivity, and more. As these capabilities are “mashed up” including "Augmented Reality“ (AR) features, they turn the cellphone into an extremely versatile communications and surveillance device.

4. Cloud Computing

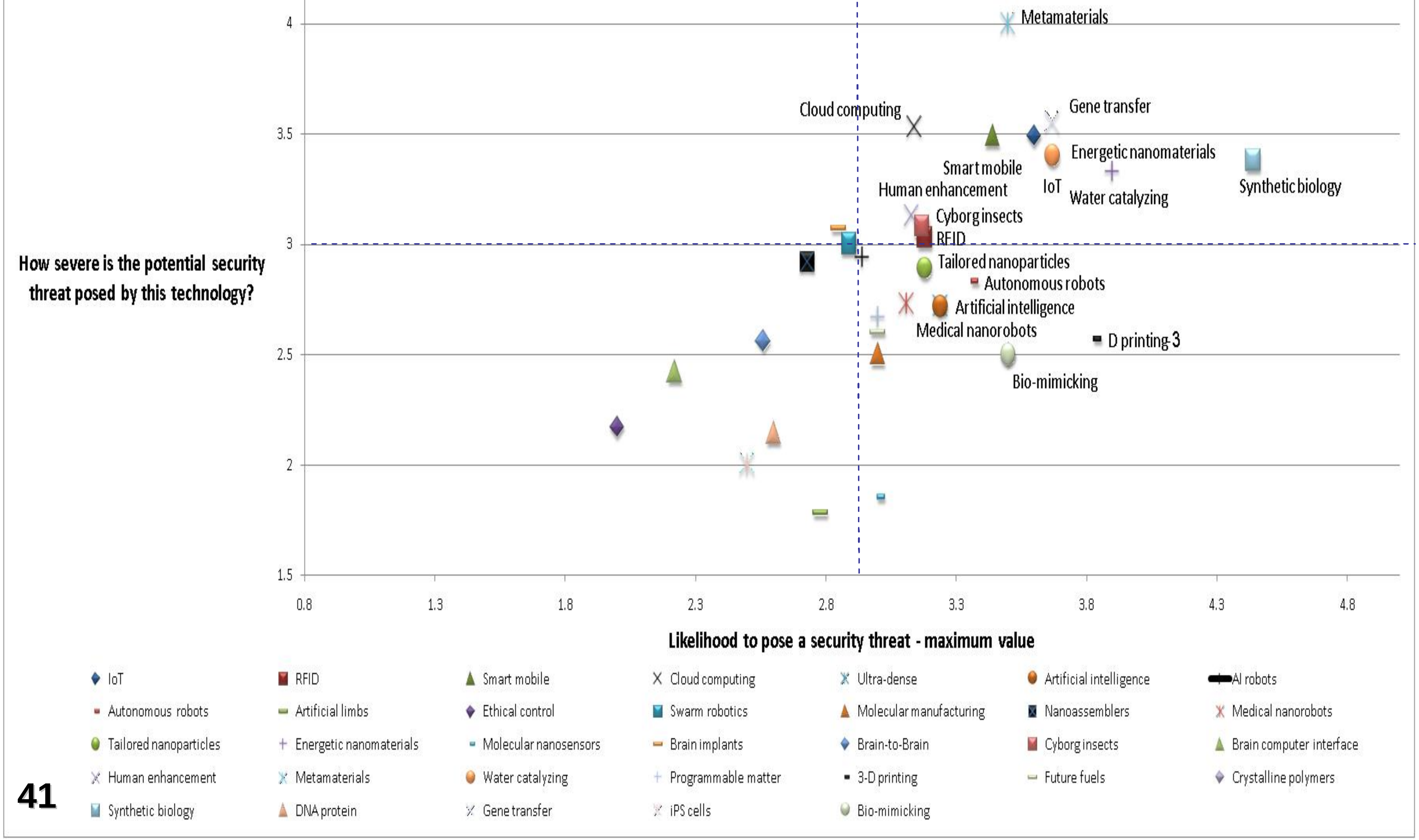
The provision of dynamically scalable and often virtualized resources as a service over the Internet**.**

5. Ultra-dense Data Storage

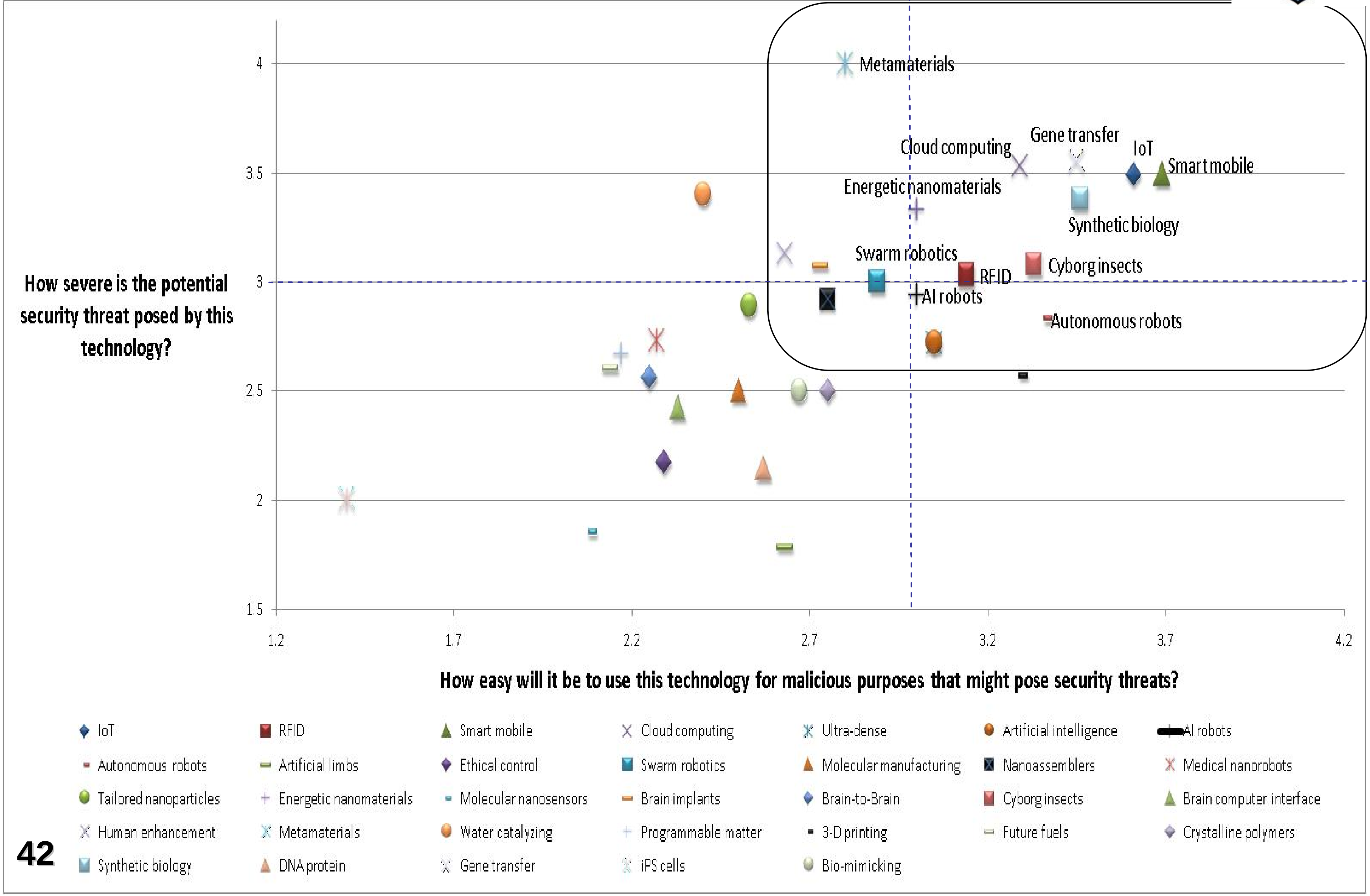
6. Advanced Artificial Intelligence

Severity vs. Likelihood to pose a security threat – max value

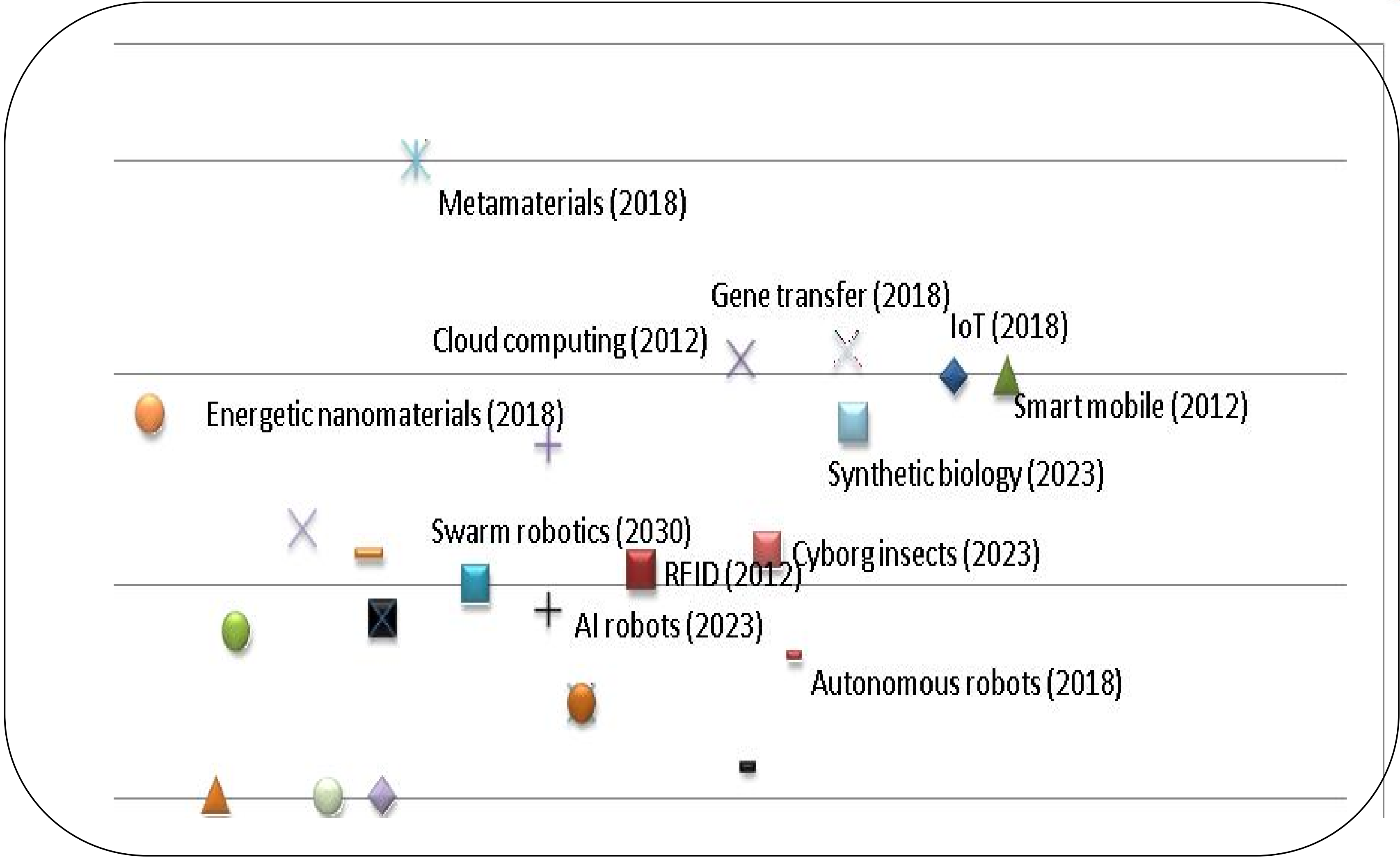
(1=very unlikely 5= very likely)



Severity vs. easiness of malicious use

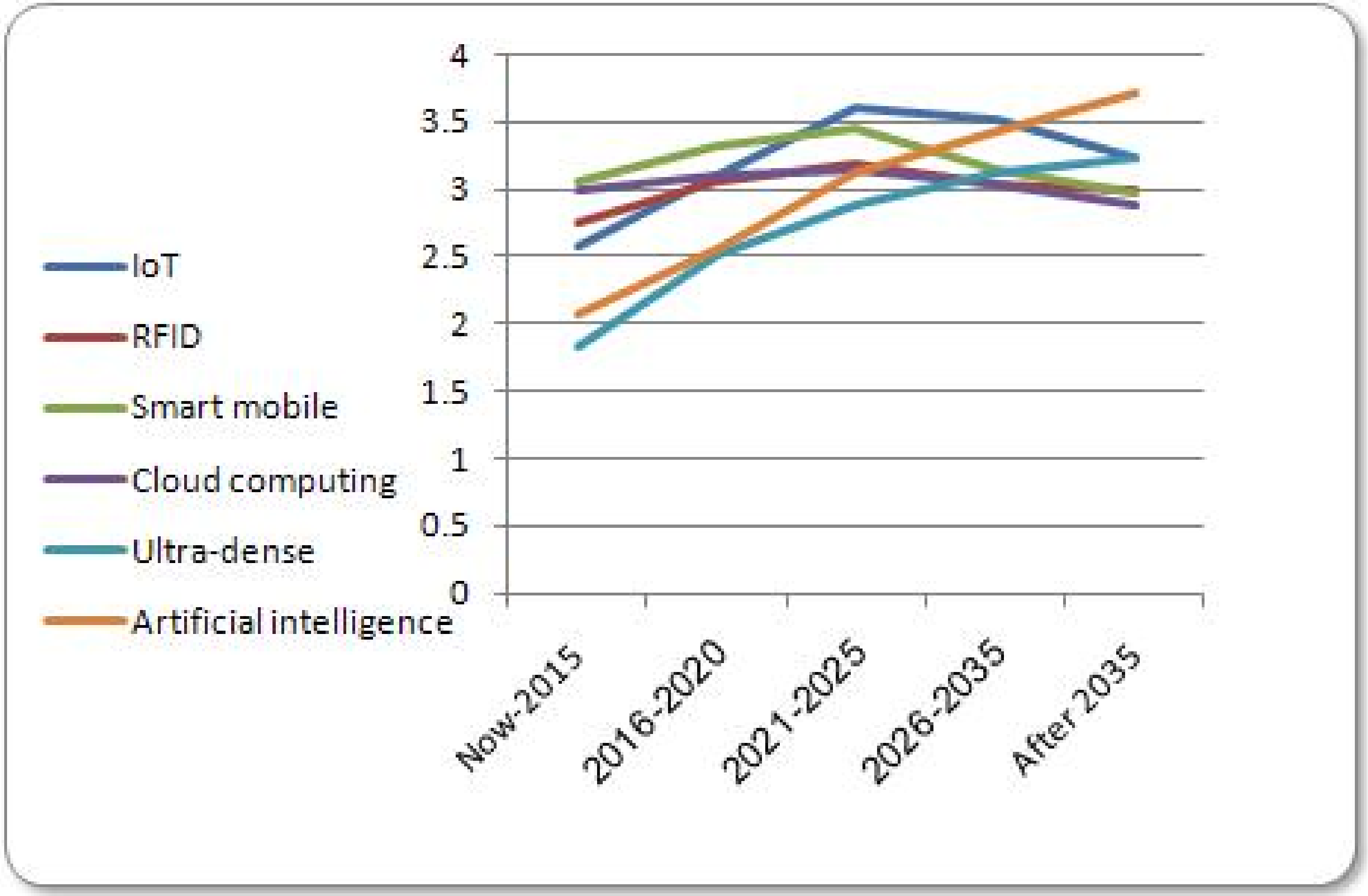


Severity vs. easiness of use for malicious purposes



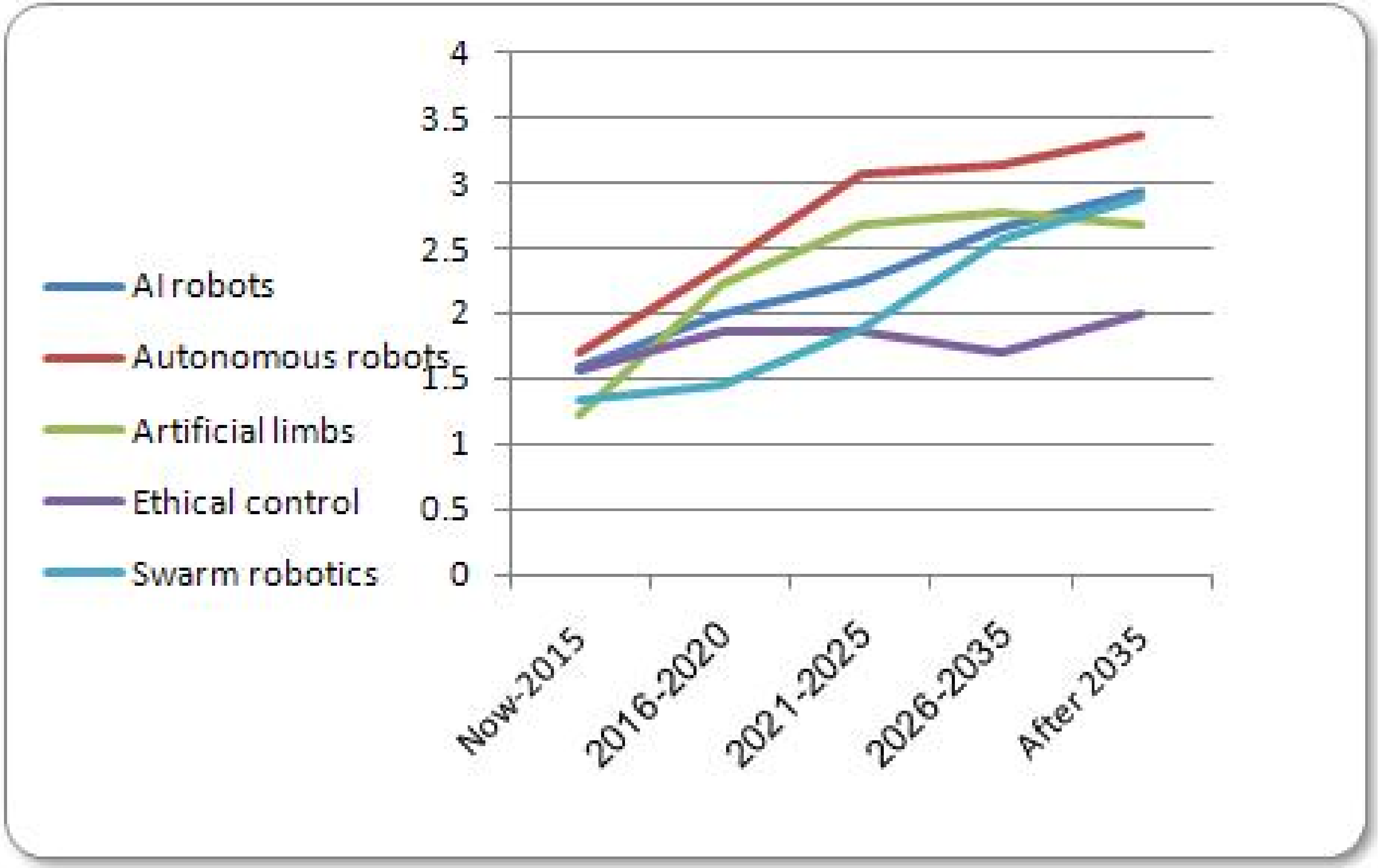
Likelihood to pose a security threat - ICT

(1=very unlikely 5= very likely)



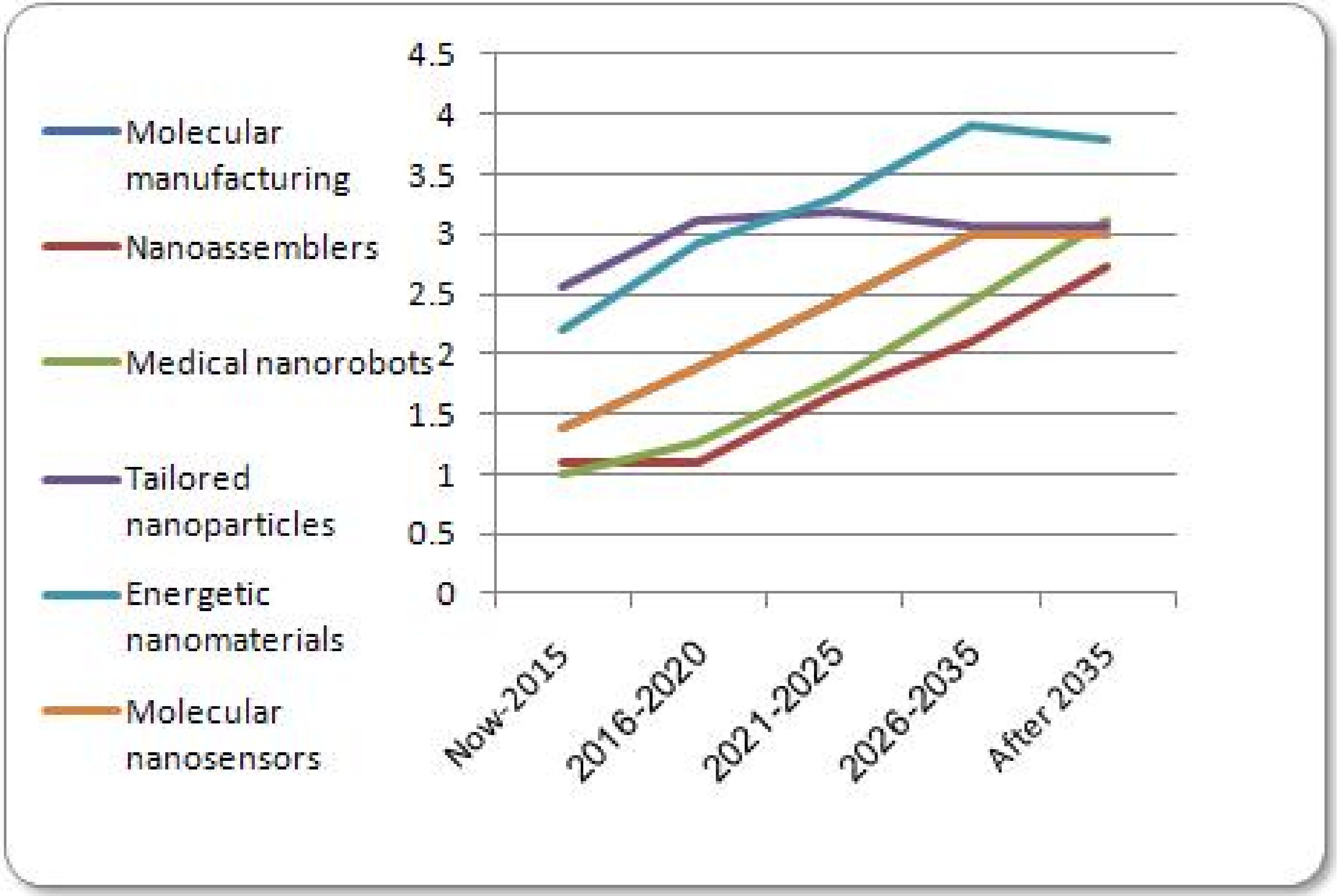
Likelihood to pose a security threat - Robotics

(1=very unlikely 5= very likely)

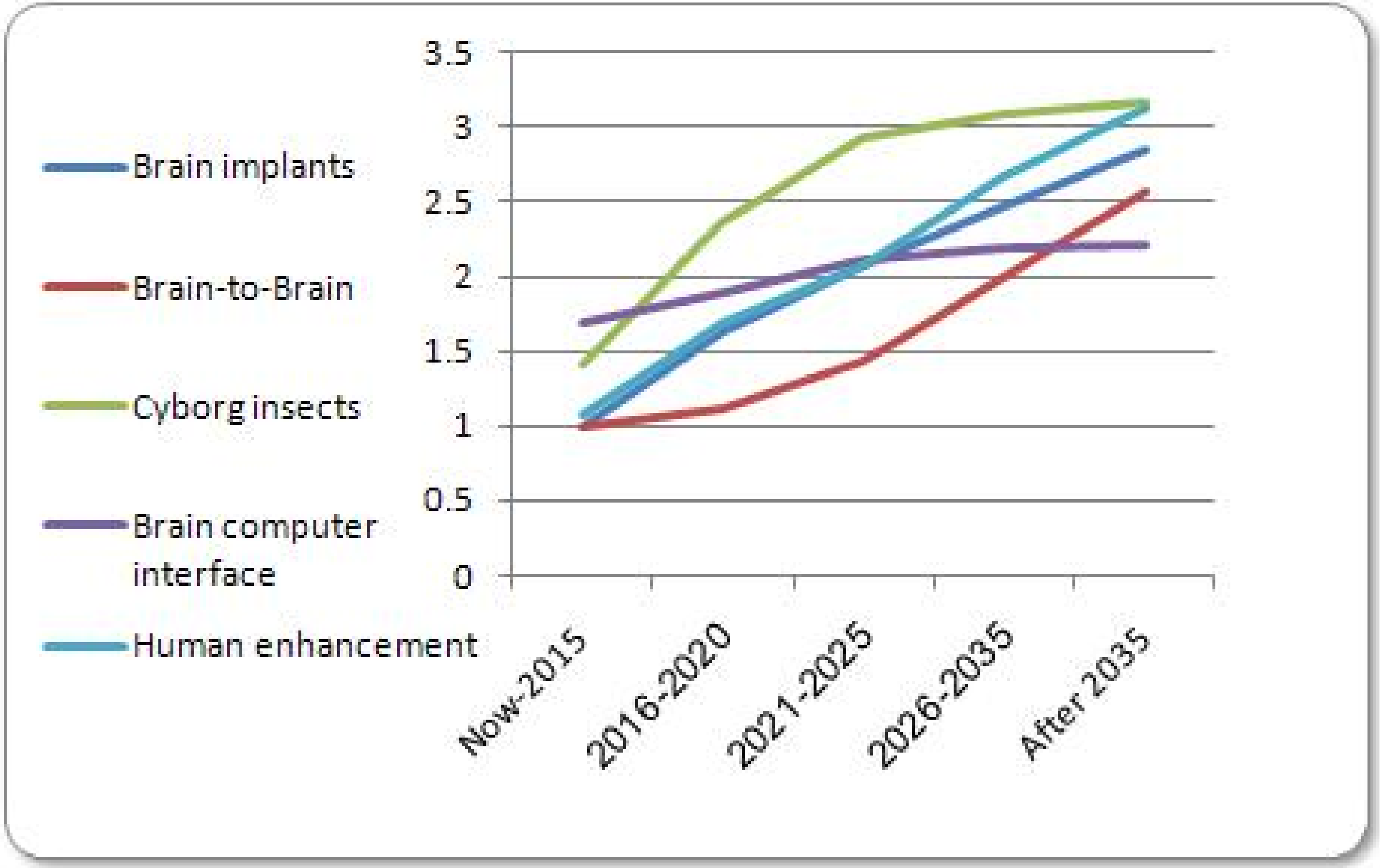


Likelihood to pose a security threat - Nanotechnology

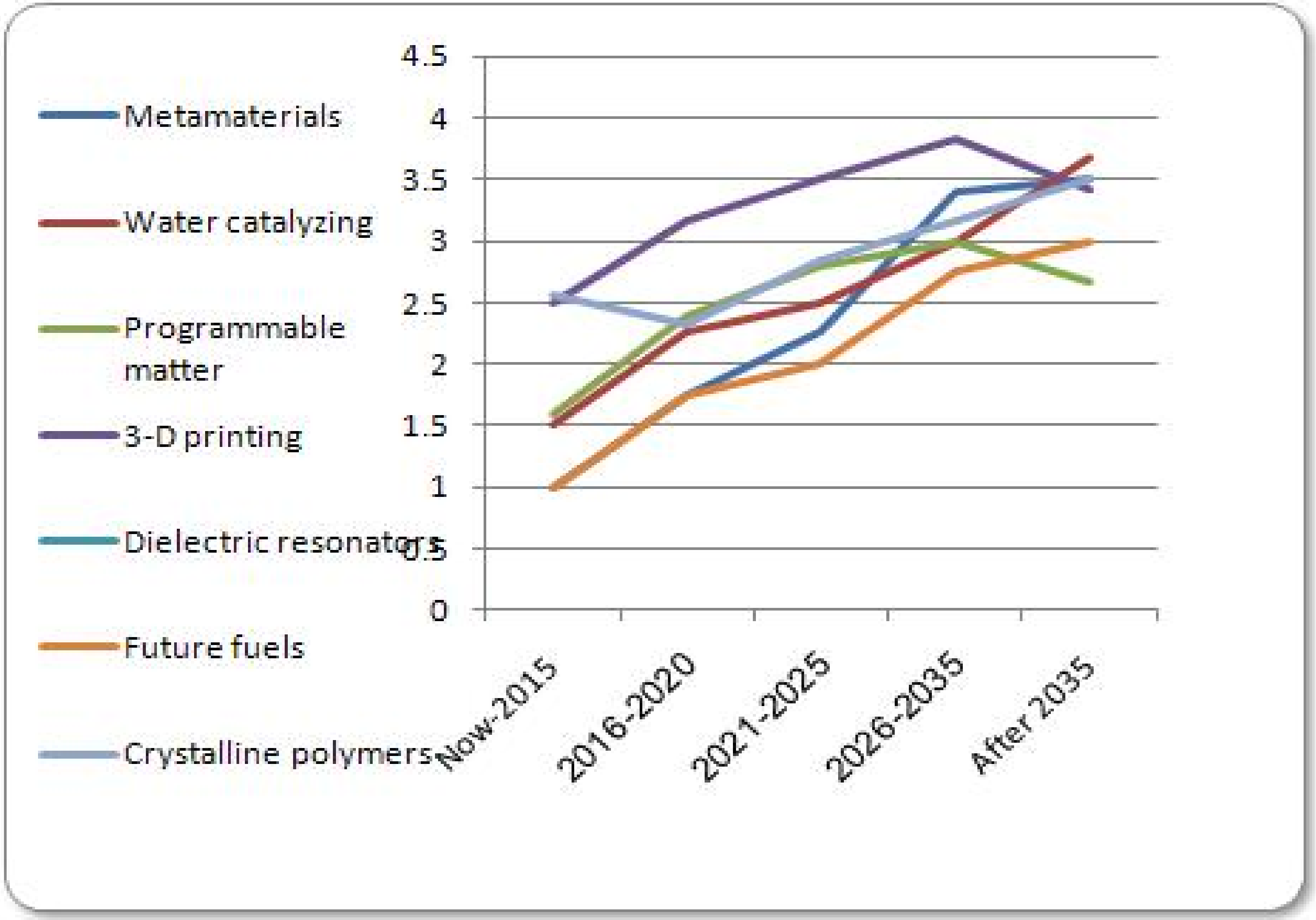
(1=very unlikely 5= very likely)



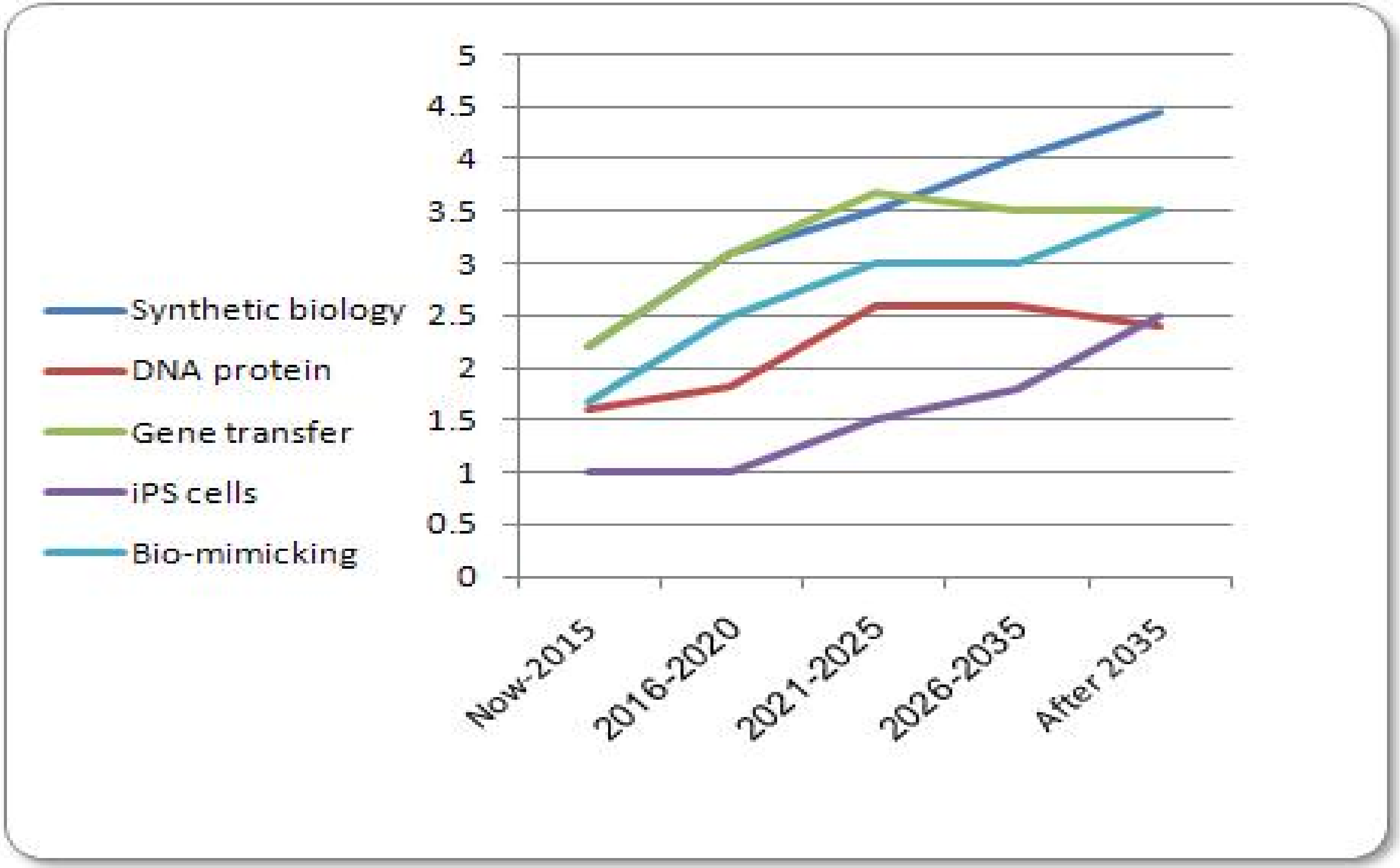
Likelihood to pose a security threat - NBIC



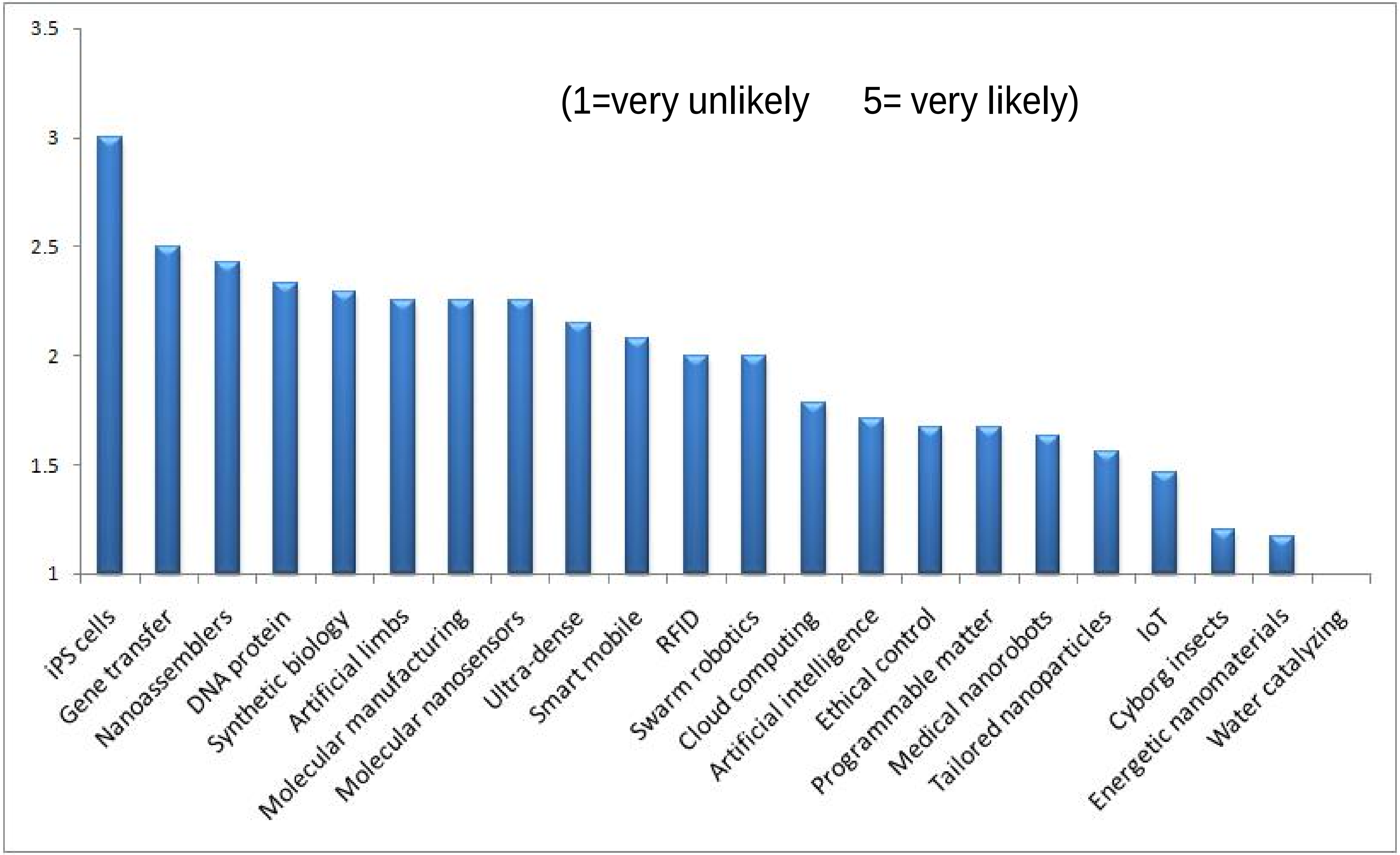
Likelihood to pose a security threat – New Materials



Likelihood to pose a security threat - Biotechnology

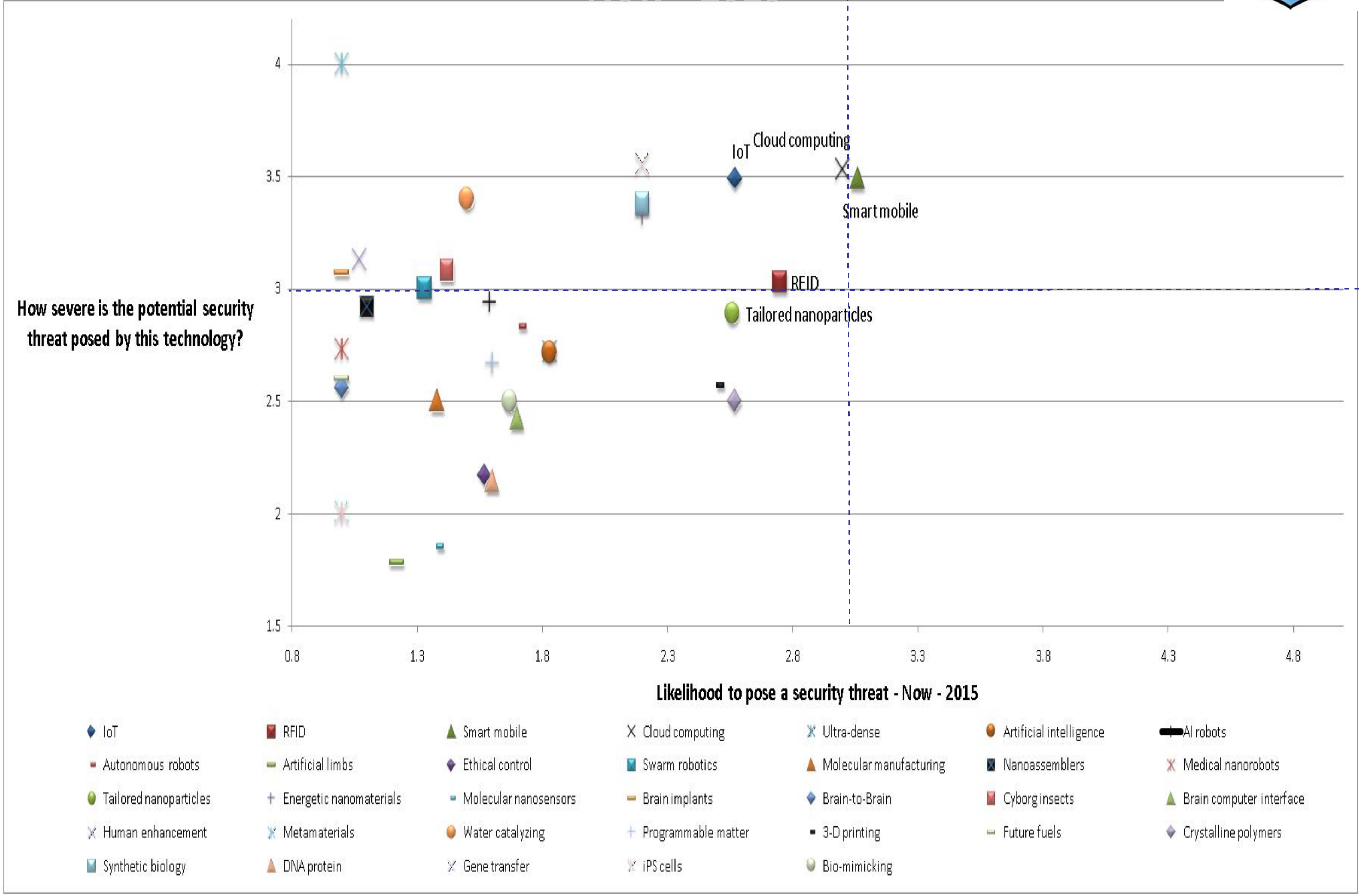


Likelihood that a technology will never pose a security threat

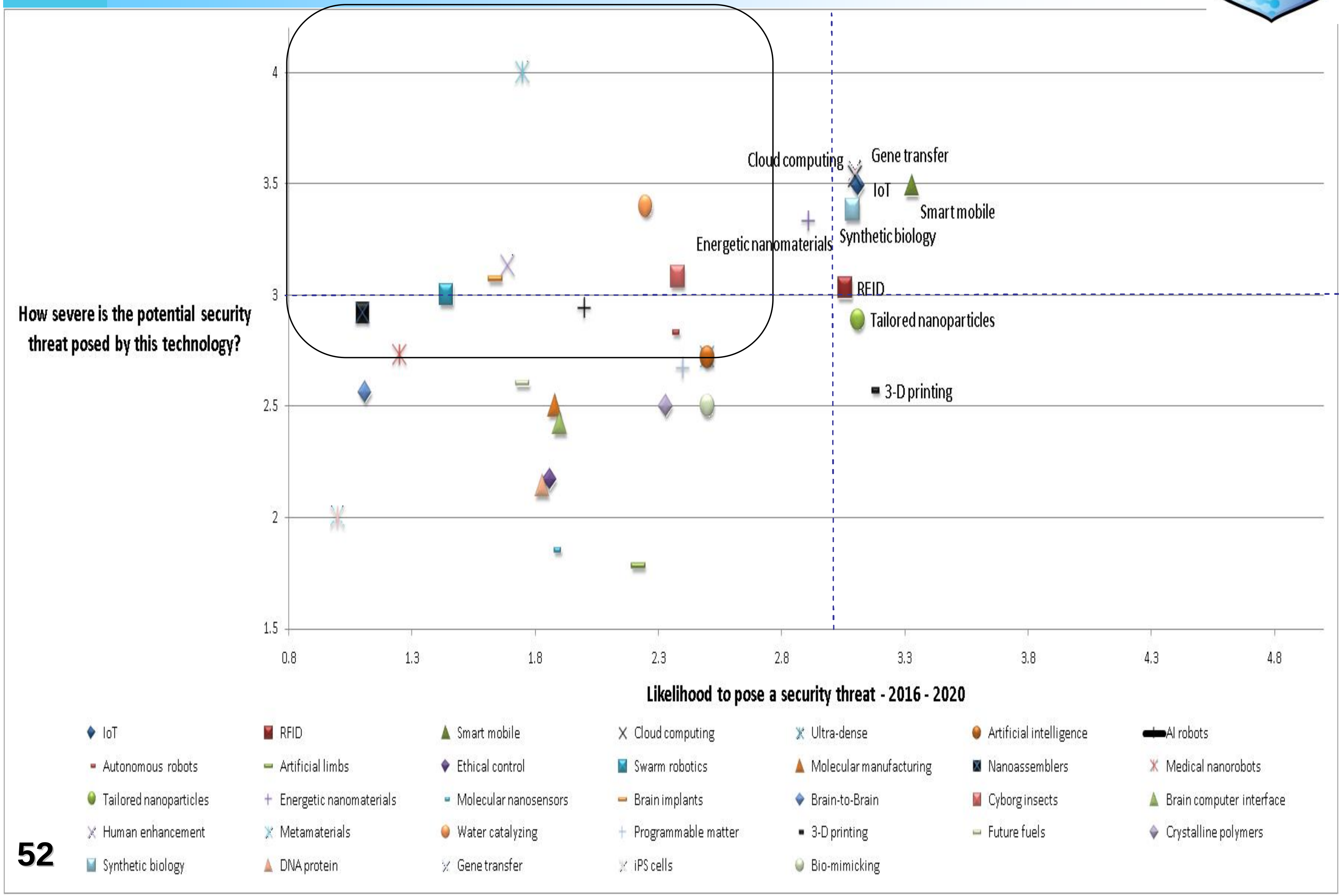


Severity vs Likelihood to pose a security threat

Now - 2015



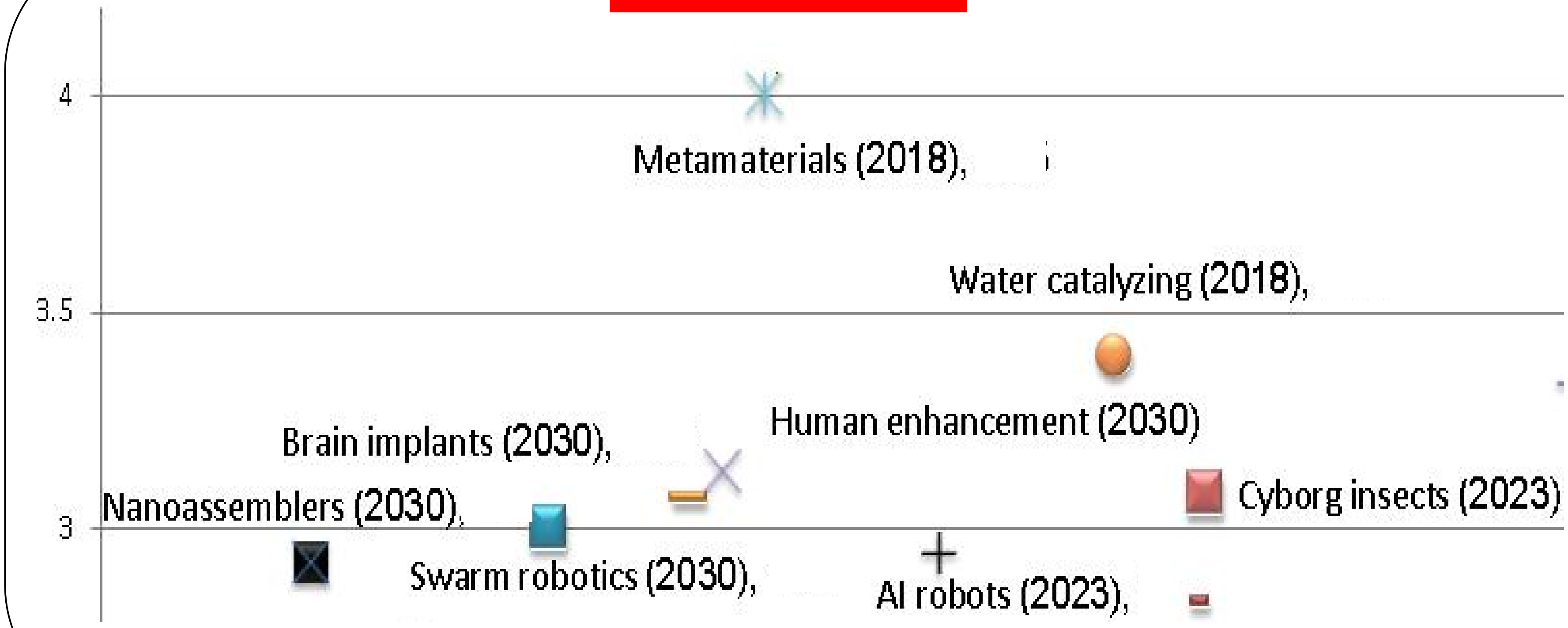
Severity VS Likelihood to pose a security threat
2016 - 2020



Severity VS Likelihood to pose a security threat

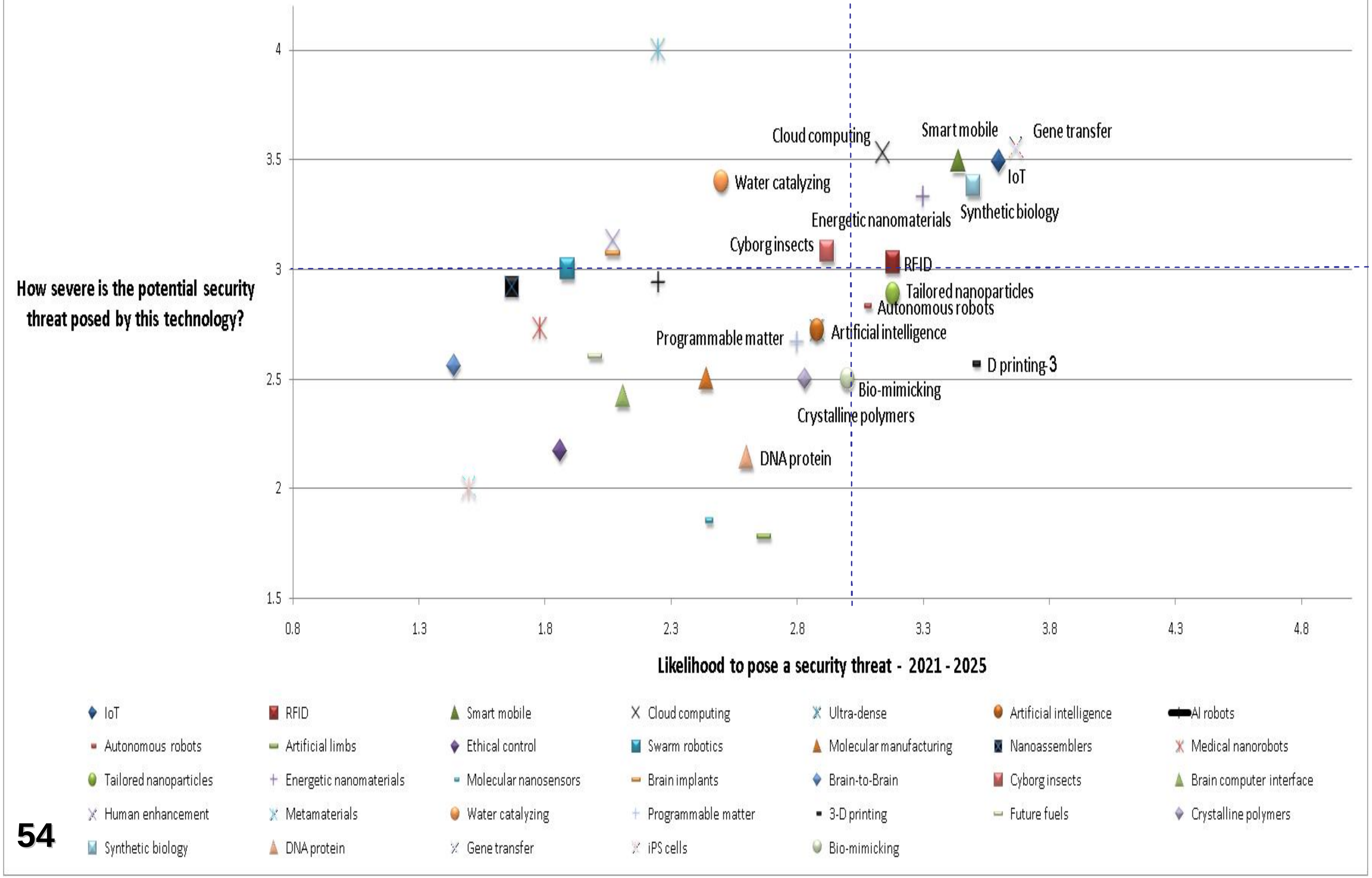
2016 - 2020

Wild Cards

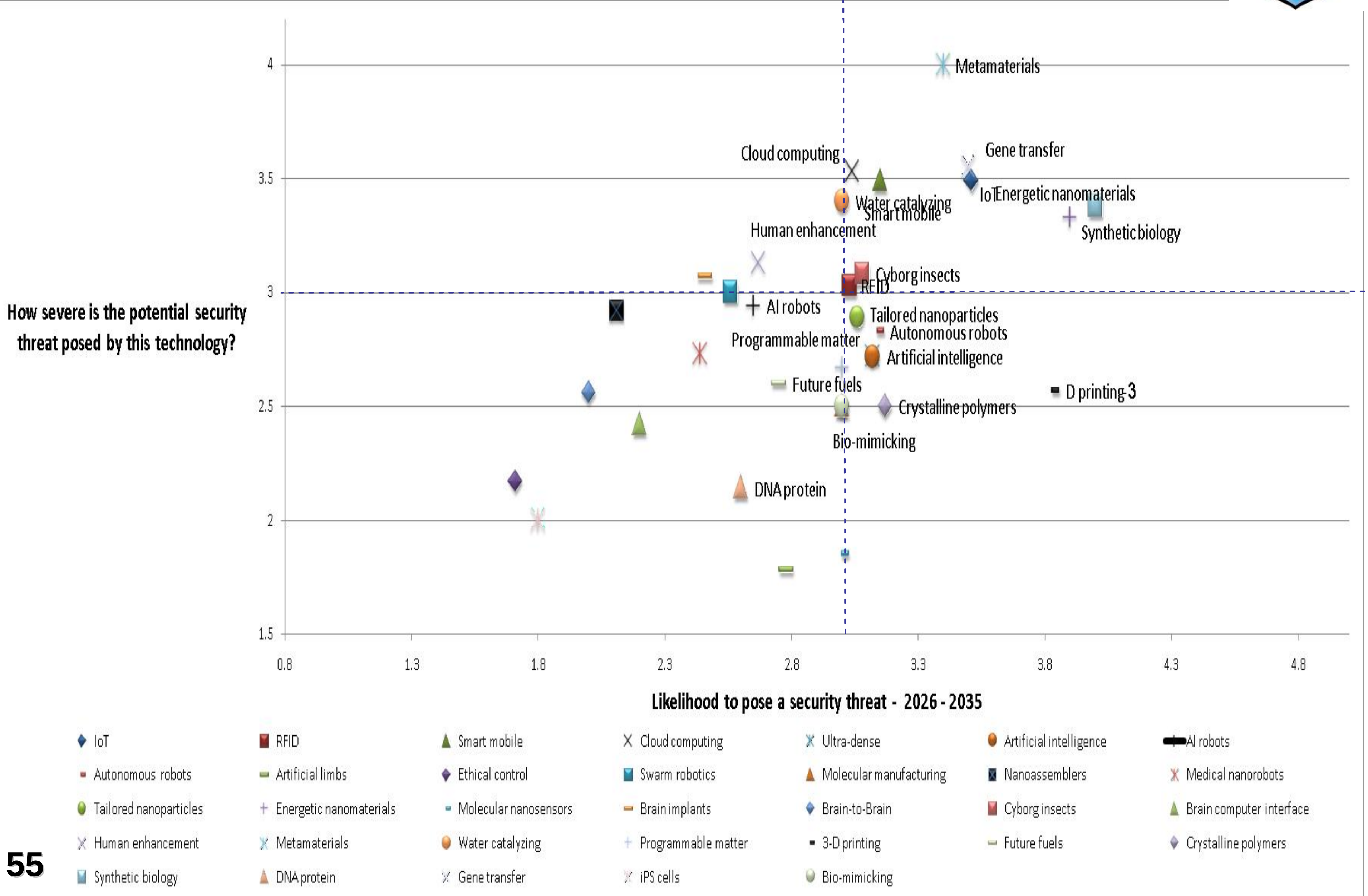


Severity VS Likelihood to pose a security threat

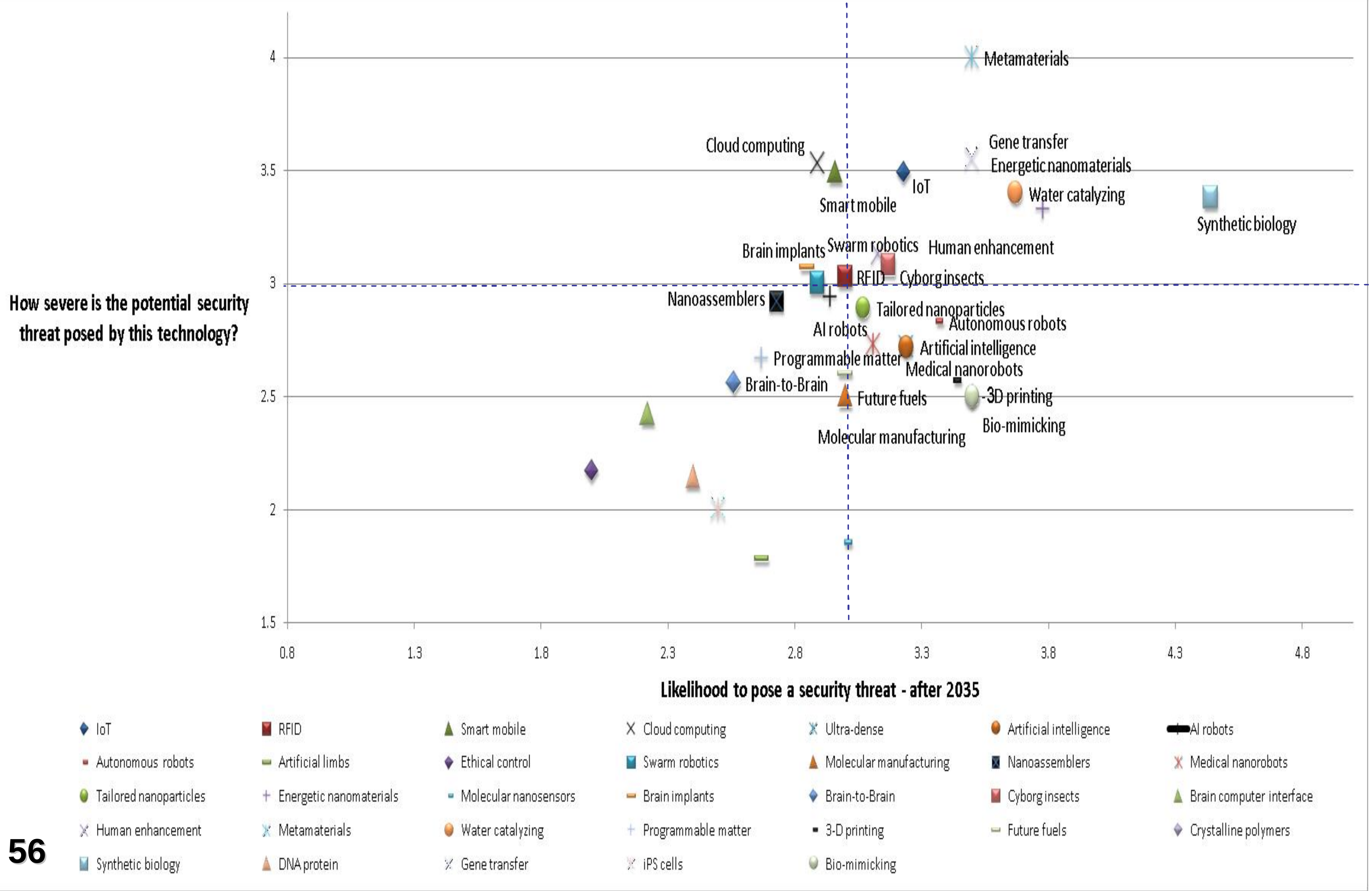
2021- 2025



Severity VS Likelihood to pose a security threat 2026 - 2035



Severity VS Likelihood to pose a security threat – after 2035



Assessment of potential threats

No.	Subject	Application	Potential Threat	Time
1.	New explosives & propellants	Better mixing of fuel and oxidizer; improved energy density, order of magnitude more effective.	+ + +	<5
2.	Metal-less Weapons	Nanocomposites in weapons and munitions overcome detection systems	+	5-10
3.	Mini/Micro/Nano Robots	Explosive carriers, remotely operated “toys”	+ + +	<5

Assessment of potential threats

No.	Subject	Application	Potential Threat	Time
5.	Small missiles	Size below 1m against aircraft, few mm against persons	+ + +	5-10
6.	Bio-electromechanical hybrids	Small animals with sensors, nerve/brain contact for movement control, small explosions, Chem-Bio dispersion	+ +	> 10
7.	Remote control of humans	Better control on suicide terrorists (“Manchurian Candidate”)	+	>10
8.	Chemical and Biological weapons, toxic materials	Capsules, vectors for entering the body, new unknown materials overcome immune reactions, overcome present detectors.	+++	5-10

Conclusions

- Nanotechnology, robotics, new materials, biotechnology, ICT and converging technologies are leading us to a new era

- Society should be more aware of the dark side of technology

- Terrorism and crime ***can*** and ***might*** abuse new technologies

- It is our ***difficult*** task to safeguard the new technologies and control their proliferation – without increasing public distrust in science, and without hurting the freedom of research

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

Karlheinz Steinmüller

Don’t slumber in face of emerging technologies – they might catch you by surprise!

How to enhance preparedness to threats without alarmism and without increasing public distrust in S&T?