Science, Technology and Society in Europe

volta 02

June 2012

YOU HAVE BEEN HACKED!

Critical infrastructures
Cyber security can no longer be an afterthought

Editorial

Dear Volta reader,

We all know the internet is a great place for those who seek information, hope to meet people or want to buy stuff. But the internet can also be a dangerous place. Like the real world, the virtual world has its thieves and criminals. That's why government campaigns warn us to be very careful when using passwords, or social security and credit card numbers in internet transactions.

But governments should be a lot more careful themselves.

The special report in this second issue of Volta is on cyber security and the vulnerability of critical infrastructures like electricity grids and water supply systems. Because many control systems for these critical infrastructures are accessible directly from the internet, they can be hacked.

And, as experts say: what can be hacked, will be hacked.

Thankfully the awareness within government organizations is high and rising. Across the world reports are being written, tough words are spoken, action lists formulated. But it's not enough. We need new laws and treaties. In our global world, we need a new organization to battle cross-border crime in cyberspace.

Security and safety also feature in another critical topic covered in this edition of Volta – genetically modified organisms. GM crops are grown on a significant scale in other continents, but not in Europe. Why? Is it possible for Europe to maintain this isolated position? What will be the tipping point for the (currently opposed) public in terms of accepting GM products?

I hope this second issue of Volta offers you inspiring insights and opinions. Please don't hesitate to contact us if you have any questions or suggestions.

Antoinette Thijssen
a.thijssen@rathenau.nl

Volta - Volume 2012 – no 2

Volta is an initiative of fifteen technology assessment organisations that work together in the European Pacita project - a four-year EU financed project aimed at increasing the capacity and enhancing the institutional foundation for knowledge-based policy-making on issues involving science, technology and innovation.
www.pacitaproject.eu

Danish Board of Technology (Denmark); Karlsruhe Institute of Technology (Germany); The Rathenau Institute (Netherlands); Norwegian Board of Technology (Norway); The Institute of Technology Assessment (Austria); Applied Research and Communications Fund (Bulgaria); Institute of Technology of Biology and Chemistry (Portugal); Institute Society and Technology (Flanders, Belgium); Catalan Institution Foundation for Research Support (Catalonia, Spain); Swiss Centre for Technology Assessment (Switzerland); Knowledge Economy Forum (Lithuania); Technology Centre ASCR (Czech Republic); University of Liège, SPIRAL Research Centre (Wallonia, Belgium); University College Cork (Ireland); Hungarian Academy of Sciences (Hungary).

Photo:
Jeroen Cant

DBT to become a foundation

The Danish Board of Technology – in Danish, Teknologirådet – is undergoing a process of transformation. Since 1985, the DBT has been a public self-governing institution, established by law and with a mandate of parliamentary technology assessment. In November 2011, a newly elected parliament agreed a state budget which included the abolishment of the DBT as part of the financial solution to expand the budget for research and innovation. However, a public hearing process revealed very strong national and international backup to the work of the DBT. Since then the government has set a new course towards establishing a foundation, which is to take over the work, staff and financial running of the DBT. At the time of writing, the change of the DBT into becoming a foundation was expected to be finalized by mid-May 2012.The new foundation will be commercial with a public goods aim, including the aim of executing parliamentary technology assessment. Whether the foundation has a formal mandate with the Danish Parliament is still under consideration and expected to be clarified before summer 2012.

Call for Papers: Technology Assessment and Policy Areas of Great Transitions

The first PACITA conference will take place in Prague from March 13-15, 2013. Organized by the Technology Centre of the Academy of Sciences of the Czech Republic (TC ASCR) and the Institute for TA and System Analysis (ITAS, Germany), it covers societal areas witnessing great transitions in health care and medicine, energy supply, climate change, mobility and the use of computer technology in all areas of society.

Please submit a one-page proposal by **July 16, 2012** via e-mail to **vancurova@tc.cz.** Full details on the Pacita website **www.pacitaproject.eu**

Parliamentary debate on knowledge-based policy-making

European policy-makers involved in TA related issues are meeting in Copenhagen on 18th June 2012 to discuss knowledge-based policy-making. How do politicians cope with science and technology issues and what kind of knowledge do they need? How can a stream of high-quality knowledge be ensured in the political decision-making processes on innovation? What is the role of 'knowledge brokers', such as the Technology Assessment institutions? How is national policy-making embedded in global issues? The meeting will be introduced by keynotes from Prof. Wiebe Bijker (University of Maastricht) and Prof. Ortwin Renn (University of Stuttgart). A synthesis of the discussions will be published next autumn.

www.pacitaproject.eu

Parliament TA Debate,
Copenhagen, 18 June 2012

Coming up

ESOF 2012
The program for Europe's largest general science meeting has been announced and will feature 400 high profile speakers including five Nobel Laureates, the Director Generals of CERN and The European Space Agency, NASA's Charles Bolden, James Watson, and Craig Venter. The event is expected to attract 5,000 delegates from 50 countries to discuss the hottest topics in science in 2012.
www.esof2012.org

Euroscience Open Forum (ESOF)
Dublin, 11-15 July 2012

PICNIC 2012
The rise of new ownership: the shift from top down to bottom up is the theme of this year's PICNIC Festival to be held in the new EYE Film Institute in Amsterdam. PICNIC is one of Europe's leading creativity and innovation platforms putting participants in touch with experts and thought leaders through keynote presentations, co-creation workshops, interactive demos, hackathons and devcamps, and active matchmaking.
www.picnicnetwork.org

PICNIC Festival
Amsterdam, 17-18 September 2012

EASST / 4S 2012
The theme for the biennial conference of the European Association for the Study of Science and Technology is Design and Displacement. In science and technology, 'design' implies the rearrangement of materials and ideas for innovative purposes but when newly designed scientific and technical objects enter the world, their initial purposes are often displaced. Pre-conference activities include study of 'Copenhagenisation'. The conference is held jointly with the Society for Social Studies of Science (4S).
www.easst.net

EASST / 4S 2012
Copenhagen, 17-20 October 2012

ICT, always a good idea?

Flemish authorities — like those in the rest of Europe — are in favour of using ICT in situations where senior citizens need healthcare. The project, *ICT, always a good idea?*, from the Institute Science and Technology (IST) in Brussels explores whether ICT applications could respond to a wider range of needs and preferences and contribute to the optimization of life quality in general. Via desk research, interviews, a stakeholder workshop and three citizen panels, insights were gained on further work to be done to develop socially robust and non-stigmatizing ICT applications for a variety of citizens and life situations. A fundamental conclusion is that ICT policy should be considered from a social—rather than a solely technological—innovation perspective. ICT products and services largely set the rules for how institutions, organizations, and individuals should adapt to their uses. However, a comprehensive policy vision is needed on the service systems that can respond to a variety of needs and preferences and which ICT applications are useful to develop. Senior citizens do not constitute a homogeneous group and may have very diverging opinions on appropriate ways to fulfill their needs.

www.samenlevingentechnologie.be/ists/en/projects/allprojects/ictandelderlypeople.html

German network conference

Every two years, the Network Technology Assessment (NTA), organization of the German speaking institutions active in the field of Technology Assessment (www.netzwerk-ta.net), holds a conference in order to share information, identify research topics, initiate co-operations and reflect upon the role and significance of TA in science and society. This year's conference (the fifth) coincides with the jubilee of TA-SWISS so there will be additional reflections to celebrate 20 years of TA experience in Switzerland. The program will include scientific talks, plenary sessions with international experts, panel discussions and a poster presentation by young scientists.

Conference program: **www.ta-swiss.ch**
NTA5/ 20-year-jubilee of TA-SWISS, Bern, Switzerland, October 29 - 31, 2012

TA Summer School

The European project PACITA (*Parliaments and Civil Society in Technology Assessment*, FP7, Science in Society) has announced the first European summer school on Technology Assessment (TA), hosted by the Université de Liège, to be held from 25th-28th June 2012 at the Château de Colonster, Belgium.
The three and half days of lectures, workshops, and information exchange will focus on the theme of renewable energy systems from a variety of approaches. The summer school is particularly directed at policymakers, academia, industry, civil society organisations and the media.

Program:
www.pacitaproject.eu

First European Summer School on Technology Assessment (TA), Liège, Belgium, 25-28 June, 2012

06

What can be hacked, will be hacked

Text:
Philip Dröge
and Pascal Messer

Across the world, the number of cyber attacks on public and private critical infrastructure - assets that are essential to the functioning of our society - is growing. Little seems safe. Electricity grids, oil and gas plants, water supply systems, financial infrastructure, traffic management – they are all vulnerable. Hollywood fantasy is becoming reality.

Cyberspace is contested every day, every hour, every minute, every second

The year is 1995. In the movie *The Net* Sandra Bullock plays a reclusive software engineer who stumbles across plans by a secret organisation to dominate the world by breaking into critical computer systems. As she skirmishes with these mysterious *Praetorians*, she and her pursuers use computers as weapons, hacking into just about anything: power grids, Wall Street computers and airplanes. 'Impossible', many technology pundits pointed out at the time. Pure Hollywood fantasy.

These days *The Net* seems strangely prescient. More and more technology experts are convinced, just about anything can, and therefore will, be hacked including vital infrastructure systems. And those pesky Preatorians? Well, some argue they became reality too. Only they call themselves Anonymous. This group of anarchistic hackers is known for their successful attacks on civic, commercial and government sites to gain notoriety and inflict damage. In February this year, *Operation Unmask* was launched: an international initiative supported by Interpol which led to the

Photo: Istockphoto

arrests of 25 hackers from countries in Europe and Latin America. The group, aged from 17 to 40, are believed to have links with Anonymous. According to Interpol, the international arrests followed a series of coordinated cyber attacks against the Colombian Ministry of Defence and presidential websites, as well as Chile's Endesa electricity company and national library. On internet forums and Twittter, Anonymous has vehemently denied it would attack critical infrastructures, calling suggestions like these 'ridiculous'and 'fear mongering'.

Global risk

But the western world is vulnerable to online attacks, that much is clear. Earlier this year, the World Economic Forum listed cyber security as one of the five global risks to watch. In their *Global Risks Report 2012*, experts considered risks that have 'severe, unexpected or underappreciated consequences'. The risk to critical systems failure that respondents cited most frequently was cyber attack. In the report, the WEF states: "National critical infrastructures are increasingly connected to the internet, often using bandwidth leased from private companies outside of government protection and oversight."

How can terrorists and hackers harm or destroy critical infrastructure from the comfort and safety of their own sofas? Well, for one thing, the information is out there. There are many control systems that are accessible directly from the internet or that can be easily located through internet search engine tools and applications. "It is indeed possible to hack into critical infrastructure", confirms Eric Luiijf, Principal Consultant at TNO, the Netherlands Organization for Applied Scientific Research. He's been warning about this since 2002: "ICT is everywhere these days; my car has 120 processors on board. And if it can be hacked, it will be hacked, sooner or later. Even if you pay a lot of attention to security."

Malfunction? Technical glitch?

Media reports abound. In March this year, the US Government Accountability Office (GAO) testified that at least four energy facilities have been hacked in the United States, two of them nuclear plants. As early as 2001 the Californian electricity grid was hacked, causing an outage in parts of the state. Closer to home, there are reports of multiple hackings into the Norwegian electricity grid. NASA admitted last March that hackers had broken into critical systems, including those that control parts of the International Space Station. To top it all, former US 'cyber security csar' Richard Clarke testified that the blueprints for the F35 Joint Strike Fighter Jet were copied by Chinese hackers breaking into Lockheed's intranet, resulting in a serious breach of US national security. But this is just the tip of the iceberg, according to Luiijf. "Many cyber security incidents involving critical infrastructure are not properly identified as such to higher management. Moreover, organisations want to keep quiet about it to the outside. It is simply called a malfunction or a technical glitch."

The Dutchman thinks that security is still not a primary concern in many organisations. Because of 'ease of use' considerations, protection of infrastructure against hackers is often minimal. Take a municipal water supply service that needs to install a new pumping system. "To manage it, they will probably get a remote access industrial control system. You can buy complete systems off-the-shelf at an industrial hardware wholesaler. And if that system has password protection, chances are the people installing it will not use it – to make it easier to access the system in the future." The result is a weak link in the water supply chain, waiting to be tested by somebody. And it was. Recently hackers in the Netherlands took control of the pumps of a tropical swimming pool."They were just playing with it, but it could have been a lot worse if they had malicious intentions", notes Luiijf.

Too easy

After denials from manufacturers that their systems could be remotely controlled, Dutch TV-journalists broke into a pump station in Veere, a small community in Zeeland, warning the local authorities they could turn off the pumps and flood the countryside. In a separate incident they turned off the central heating of the national headquarters of the Salvation Army. The entry to both remote control systems was made possible through the internet and because of a very easy to guess password ('Veere'). An IT-specialist hired by the journalists said on-camera that within 'half an hour' he could teach his mother how to hack into systems like these. "That's how simple it is."

Stuxnet

Flashback to Hollywood and John Travolta in *Swordfish* (2001). In this movie he forces a retired hacker to steal 10 million dollars (an accumulated government slush fund) from a bank. The money is destined for a secret government organisation called *Black Cell* which kills terrorists who have targeted Americans. Rebels and spies using cyberspace as a battle ground? It seemed farfetched in the year terrorists used real airplanes to launch an attack on the US.

Duqu – the next Stuxnet?

In November 2011 security firm Symantec warned of the emergence of new malware called Duqu which contains code identical to that used in Stuxnet. It also targets Scada Systems used in power, water and sewage plants, oil and gas refining and telecommunications, but its purpose seems to be to gather intelligence for mounting future attacks. Symantec stated that Duqu infections have been confirmed in at least six organizations in eight countries (France, the Netherlands, Switzerland, the Ukraine, India, Iran, Sudan and Vietnam).

And then nearly a decade later, in 2010, Stuxnet was discovered in a nuclear plant in Iran.

Stuxnet is powerful and complex malware – malicious software - that sabotages or spies on the type of computers used in industrial control systems.The worm, which is designed to attack Siemens systems, was discovered in several important SCADA-programs - those that control the operation of valves, pipelines and other industrial equipment - at the Iranian uranium enrichment facility at Natanz. According to the draft report *Information and National Security* by UK NATO rapporteur Lord Jopling, Stuxnet deploys two extremely complicated programming payloads to bomb the target's operating system, causing damage to the centrifuges while blinding its systems to the reality of what is happening. Such is the sophistication of the Stuxnet code, analysts believe it was designed by the US and/or Israel or Russia to slow down the development of weapons technology in Iran. Whoever tried to thwart the Iranians, it worked. The centrifuge operational capacity at Natanz dropped by 30 percent after the incident.

Meltdown

Most experts agree that only nation states currently have the resources to sabotage a critical system of that nature but the emergence of Stuxnet suggests what is possible. From the World Economic Forum report: "A virus like Stuxnet could conceivably trigger a meltdown in a functioning nuclear power plant, turn off oil and gas pipelines or change the chemical composition of tap water."

Stuxnet also showed the potential scale of fights in cyber space, and the gloves, it seems, are off. In the

What is… Critical infrastructure

Countries differ when describing what exactly constitutes a critical infrastructure, also called vital infrastructure. The most important element is that they are essential to the functioning of society. The EU definition is: The physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments.
Think electricity systems, gas and oil plants, water supply (drinking water, sewage), transportation and financial/ governmental (IT) services.

SCADA

Supervisory control and data acquisition (SCADA) programs are also called industrial control systems (ICS). These are computer systems that monitor and control processes in industry, infrastructure, or facilities. More and more of them are becoming connected to the internet.

decade since *Swordfish*, hacking has become part of geo-political armoury, seen as being on par with conventional weapons. The American government has a doctrine that says as much:

'When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defence, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.'
International Strategy for Cyberspace, The White House, May 2011

The Obama administration is also pushing for a three-year mandatory imprisonment sentence for attacks against critical infrastructure systems.

NATO's new policy

On the military side, NATO – whose own networks are constantly under attack by hacktivists – was early to spot cyber security as a serious issue when it implemented a Cyber Defence Programme in 2002. Last year, NATO defence ministers adopted a new cyber defence policy, focusing on prevention and building resilience. In November 2011, in an opinion piece for *The New York Times*, NATO's Supreme Allied Commander Transformation, French General Stéphane Abrial, wrote that cyber attacks are "among the most pressing and potentially dangerous threats to our collective peace and security."

Abrial: "In discussing a hypothetical major attack, NATO leaders are often asked what circumstances would trigger a response under Article V of the Washington treaty — in other words, when would an attack against one be considered an attack on all? It would not be prudent to try to define exact tripwires in advance, or to tie our hands as to how we would react. But assuredly, the alliance would respond deliberately to any significant attack, adapting its reaction to the extent of the damage, the degree of certainty in attribution, the identity of the attackers and their perceived intentions."

In the article, the NATO Commander states that civilian authorities in all 28 NATO member nations have the lead responsibility on cyber security. Abrial: "NATO is therefore working in support of whole-of-government approaches to cyber defence — led by civilian agencies in each nation — and with actors outside government. Key among those are commercial suppliers and the wider industrial base, since NATO-wide, 85 percent of critical infrastructure is in private hands."

Who hacks?

Professor Solange Ghernaouti–Hélie of the Faculty of Business and Economics at Lausanne University (Switzerland) is an international expert in cyber security and cybercrime. She has seen hacking become a weapon but acknowledges there's no clear profile of those wielding cyber weapons. "There are all kinds of people who hack into critical systems', says Ghernaouti–Hélie. 'Think of 16-year-old boys who want to prove that they can. But also criminals who want to blackmail the owners of a system. And lately we see government agencies trying to generate chaos in another country. The internet is very busy with people trying to do harm."

As said previously, Stuxnet was an unusual development both in the complexity of its code and the nature of its intended target. Sources in *The Economist* claimed that its designers must not only have had access to the target plant's blueprints and a detailed knowledge of Siemens's industrial-production processes and control systems, but also pointed to their use of four previously unknown Windows security-holes – known as zero-day-vulnerabilities - that are so valuable to hackers that they would not generally use so many in a single attack.

Photo: Istockphoto

Thomas Rid and Peter McBurney of the War Studies Department at Kings College London believe that the more destructive a cyber weapon is, the more expensive and difficult it will be to produce, especially in terms of the intelligence needed about the target. As a consequence, such cyber weapons will be very specific, not easily repurposed, and unlikely to cause collateral damage. In a report on cyber weapons produced earlier this year, they concluded that: "The cost-benefit payoff of weaponised instruments of cyber-conflict may be far more questionable than generally assumed: target configurations are likely to be so specific that a powerful cyber weapon may only be capable of hitting and acting on one single target, or very few targets at best." While Ghernaouti–Hélie agrees that hackers or terrorists are not yet knowledgeable enough to produce something as destructive as Stuxnet, there is danger in other collaborations: "We see more and more

links between radicals and tech-savvy criminals, who do know how to penetrate a critical system. If your goal is to disturb and disrupt, hacking is an excellent way to reach your goal."

And she believes hacking is developing into a powerful weapon that might force us to rethink current political conflicts. "Take the Israelis and the Palestinians. They hack each other on a daily basis. No amount of security is going to stop some of these hacks to be successful, because both sides are incredibly motivated. If you don't solve the root of the problem – the conflict between the two states – you are not going to stop the relentless hacking." Since that might not be on the cards – Israel and the Palestinians have been at each other for decades, for example – governments and companies have no other choice than to invest heavily in cyber security to keep their, and our, critical infrastructure safe.

'One of the biggest problems is that security is often just an afterthought'

As a result, security is now the single biggest software market. But even the best security is not a cure-all, according to Professor Bernhard Hämmerli, cyber security expert at the Lucerne University of Applied Sciences (Switzerland). Since so much of our society is now online, protecting each and every nook and cranny of our networked lives has become impossible. Hämmerli compares it to guarding an extremely long fence. Unless you have guards at ten meter intervals, somebody can (and therefore will) climb across. "The defender has to defend everything, the hacker can be specific. He can stake out a system for a long time and look for that one weak spot he needs to get in. To make it even more difficult, IT infrastructure is constantly evolving. You have constant updates, maintenance, new applications; each and every change you make to a system could render it more vulnerable to a breach of security." And then there is the money issue. Hämmerli: "Budgets always have limits; no organisation in the world has the funds to completely seal off a system."

The World Economic Forum suspects that some security suppliers themselves could be in on the hacking game. In their *Global Risks Report*, the Forum stresses one of the key challenges in cyber security, that 'incentives are misaligned': vendors of online security products have a financial interest in talking up the threats of cyber crime, while the victims often have an interest in remaining silent. It believes correcting such 'information asymmetries' should be at the centre of policies to improve global cyber security.

Fire sale

Security professionals turning into hackers brings us to the summer blockbuster of 2007. *Die Hard or Live Free* stars Bruce Willis as an analogue cop in a digital world. While escorting a young hacker to the FBI, Willis finds himself in the middle of a fire sale, a state of utter chaos caused by the simultaneous hacks of several critical systems including utilities, traffic management and communications. This large scale hack is performed by former US government security adviser Thomas Gabriel, who is proving a point: he warned in vain that such a large scale attack was possible and is now causing mayhem.

The world has yet to witness a real fire sale consisting of simultaneous hacks against critical infrastructure but if past movies about hackers are anything to go by, we should see one in about five years. Probably not as spectacular as in the movies – hacking in real life never is.

For critical infrastructure IT professionals from around the world, it is only a matter of time. In a survey by security firm McAfee of 600 IT specialists from 14 countries, more than half the respondents think we will witness large scale attacks within the next few years.

The internet of things

Robbert Kuppens, Chief Information Officer for Cisco Systems in Europe, the Middle East and Africa also thinks it could be on the cards. His company manufactures a large portion of the infrastructure that powers the internet so must remain one step ahead of the hackers. According to Kuppens new threats are constantly lurking in the dark corners of cyberspace; there is no room for complacency with more and more devices, such as smart electricity meters, connecting to the internet. The US Governmental Accountability Office (GAO) recently underlined this in a report on Electricity Grid Modernization, with the realistic headline 'Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed.'

Shockingly slipshod

Kuppens: "We are currently heading for the *internet of things*, in which many devices that were until now offline will connect to the internet, either by cable or wireless. All these new devices are potential leaks for the networks they are connected to, so you should secure them all. Don't think for a moment that a device will not be hacked because it does not look like a computer. Take mobile phones. Until recently a lot of people thought they could not be hacked, but now we know that is not true anymore."

Kuppens says that a lot of companies and governments are very security conscious. But he also regularly encounters critical systems, both public and private, protected by shockingly slipshod security measures. "One of the biggest problems is that security is often just an afterthought. And that the people who make decisions about investments in hardware and software are sometimes ill-informed. Security costs money, while its benefits are often not immediately clear to the layman. And if there are security-conscious IT staff in an organisation, we find they lack strong support from management to invest in the necessary hardware and software."

Photo:
Istockphoto

'No organisation in the world has the funds to completely seal off a system'

Security and security management nowadays ask for a holistic approach. It is no longer a responsibility of IT only, but of the organisation as a whole.

Next target: energy supply

So, where could a large scale attack take place? Kuppens thinks – and Hämmerli, Luijjf and Solange Ghernaouti–Hélie agree – the energy supply is a logical target. In Europe, the management of electricity is often centralised with one organisation controlling the whole electricity supply. Electricity grids are often managed online which increases the risk of a breach of security at the central level. In a worst case scenario, an attack could shut down the electricity in a whole country or even the whole of Europe.

Cyber incidents have already taken place in energy facilities. In 2009, at a hearing for the US Congress, it was stated by US national security officers that cyber spies had compromised the electrical grid of the United States and installed software programs that can disrupt the system when activated by a hacker.

In a testimony for a committee of the US House of Representatives, the US Governmental Accountability Office (GAO) cited four incidents concerning energy plants. Apart from Stuxnet in Iran, the GAO believes that in 2006 the failure of two circulation pumps at Browns Ferry, a US nuclear power plant in Alabama, was caused by cyber security breaches. In 2003 an alarm processor in FirstEnergy, an Ohio-based electric utility, failed, resulting in the cascading failure of 508 generating units at 265 power plants across eight US States and a Canadian province.

Earlier that same year a worm known as Slammer infected a private computer network at the Davis-Besse nuclear power plant in Oak Harbor, Ohio. It disabled a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again.

James Lewis, cyber specialist at the American Center for Strategic & International Studies (CSIS) has been keeping a 'significant cyber incidents' list since 2006. According to this list, Norway's National Security Agency (NSM) reported that in 2011 at least 10 major Norwegian defence and energy companies were hacked: "The attacks were specifically 'tailored' for each company, using an email phishing scheme. NSM said that the attacks came when the companies, mainly in the oil and gas sectors, have been involved in large-scale contract negotiations. The hacking occurred over the course of 2011, with hackers gaining access to confidential documents, industrial data, usernames and passwords."

Holistic approach

So, how do we deal with these threats? The response from governments is a mixed bag, according to security specialist McAfee. Governments continue to play an ambiguous role in cyber security - sometimes helping the private sector, sometimes ignoring it. The US and the UK are taking the lead in developing cyber security strategies and have made cyber security a top priority in their national security programmes. The US has its Cyber Command, the UK its Government Communications Headquarters. GCHQ director Iain Lobban, reported in *The Guardian*, has no illusions about the scale of the threat: "Cyberspace is contested every day, every hour, every minute, every second," he said. "I can vouch for that from the displays in our own operations centre of minute-by-minute cyber-attempts to penetrate systems around the world."

The EU is slowly stitching together a holistic approach. In 2011, the European Commission published the *Communication Achievements and Next Steps: towards Global Cyber-security*. It focuses on the global dimension of the challenges and the importance of boosting cooperation among EU states and the private sector at national, European and international level. The EU is striving for more awareness and preparedness.

European member states are rapidly installing national CERTS (computer emergency response teams) while ENISA, the EU's cyber security agency, issued a thick study on industrial control systems (ICS) security. Derived from a hundred key findings, the report proposes seven 'urgent' but 'challenging' recommendations for improving ICS security. The recommendations call for national and pan-European ICS security strategies, a Good

Practice Guide on ICS security, research activities, spreading awareness, the establishment of a common test bed and ICS-computer emergency response capabilities. ENISA stresses the importance of active collaboration between public organizations and the private sector. Earlier this year ENISA saw its mandate extended after the successful coordination of the first pan-European cyber security exercise. This was, reported German think tank Bertelsmann, despite criticism for its location on Crete, making it hard to attract qualified IT staff.

New laws needed

Across the world, reports are written, tough words are spoken, action lists formulated. But stopping hackers interfering with our critical infrastructure seems not to be so easy. Existing regulation is not enough, the experts say. International laws and international or even global cooperation is the key, as these are often cross-border crimes with major jurisdiction issues. That's if you can even identify where an attack comes from. There must be a new framework. "We need new laws. We should determine internationally what is and what is not punishable when it comes to the internet", according to Cisco's CIO Kuppens. "While politicians tend to look at their own back yard, the virtual world knows no borders. Something that is prosecutable in one country is allowed in the next. We should have treaties about what constitutes a cyber crime and how and by whom it should be punished. Perhaps we could establish a WTO-like organisation to battle cross border online crime."

NATO rapporteur Jopling proposes just that: "On the global level, NATO should support initiatives to negotiate at least some international legal ground rules for the cyber domain. International law should clearly prohibit the use of cyber attacks against civilian infrastructures." Jopling also called for NATO member states to hurry up when ratifying binding international

Read More

For this article, Volta used the sources listed below - and many more.They might be a reference point for your research.

INTERNATIONAL COOPERATION

Achievements and Next Steps: Towards Global *Cyber-Security*
JEuropean Commission Communication on Critical Information Infrastructure Protection (Brussels, 2011)
[http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm]

A List of Significant Cyber Incidents since 2006
James Lewis, CSIS (2006-2012)
[http://csis.org/publication/cyber-events-2006]

Baseline Capabilities of National/ Governmental CERTs -Part 2: Policy Recommendations
EU (2010)
[http://www.enisa.europa.eu/activities/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations/at_download/fullReport]

Defending the Networks – The NATO Policy on Cyber Defense
NATO (2011)
[http://www.nato.int/cps/en/SID-59665BDE-D35979E8/natolive/75747.htm]

Global Risks Report
World Economic Forum (2012)
[http://reports.weforum.org/global-risks-2012/]

Information and National Security - Draft General Report
Lord Jopling (United Kingdom) General Rapporteur, NATO Parliamentary Assembly (2011)
[www.nato-pa.int]

Nato builds its Cyberdefences
Stéphane Abrial, The New York Times (2011)
[http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html]

Protecting Industrial Control Systems – Recommendations for Europe and Member
States ENISA (2011)
[ENISA - Protecting Industrial Control Systems - Recommendations for Europe and Member States.pdf]

Reducing Systemic Cyber-security Risk
OECD -IFP Project on Future Global Shocks- Peter Sommer and Ian Brown (2011)
[http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1743384]

Rethinking Cybersecurity – a Comprehensive Approach
James Lewis, CSIS, 2011
[Rethinking Cybersecurity - A Comprehensive Approach]

ACADEMIC

Cyber norm emergence at the United Nations – An Analysis of the Activities at the UN regarding Cyber-security
Tim Maurer - Belfer Center for Science and International Affairs (2011)
[Full text of "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-security"]

Cyber War Will Not Take Place
Thomas Rid - Journal of Strategic Studies (2012)
[http://www.tandfonline.com/doi/full/10.1080/01402390.2011.608939]

Cyber Weapons
Thomas Rid and Peter McBurney The RUSI Journal (2012)
[Cyber-Weapons (.pdf)]

Security Economics and Critical National Infrastructure
Anderson and Fuloria, Springerlink (2010)

Software Failures, Security, and Cyberattacks
Charles Perrow (2008), Schwerpunkt, Technikfolgenabschätzung (2011)

treaties, like the Council of Europe's Convention on Cyber crime, because banning cyber criminal activities would also help in dealing with cyber terrorists and state-sponsored cyber attacks that often use the same techniques as cyber criminals.

A role for the UN?

Professor Ghernaouti–Hélie sees a role for the UN. According to her, this is the only international organisation with sufficient clout to author an enforceable code of online conduct for states, companies and individuals. "We need to integrate security in every piece of technology that is coming on the market. Only an international organisation like the UN can force the market to do that. We need a UN charter for the internet that establishes what you can and cannot do online."

Chances are slim however, that such a scenario will unfold. Although the UN is working on cyber security, through the UN General Assembly and through the International Telecommunications Union, there is as yet no UN Cyber Security Department. A spokesperson for the UN says there are to date no plans for a charter, new laws or a conference on the subject. International law specialists question the UN's capacity on this subject because since the nineties, the conclusion of international treaties has taken a sharp decline. Most plausible is that bilateral treaties and regional, or if possible, global partnerships, might help generate some agreement on establishing cyber security. In the meantime nations, owners of critical infrastructure, and the rest of us, are left to fend for ourselves.

Where is the Hollywood superhero to keep us safe in cyberspace?

Read More

MISCELLANEOUS

Anonymous says Power Grid Concerns are U.S. Gov't Spin
SC Magazine (2-02-2012)
[http://www.scmagazine.com/anonymous-says-power-grid-concerns-are-us-govt-spin/article/228687/]

Assuring a Trusted and Resilient Informations and Communications Infrastructure
US Cyber Space Policy Review (2010)
[www.whitehouse.gov/.../Cyberspace_Policy_Review_final.pdf]

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to be Consistently Addressed
GAO (2010)
[http://www.gao.gov/new.items/d10628.pdf]

Cyber Security in the UK
Post - Postnote (2011)
[www.parliament.uk/briefing.../POST-PN-389.pdf]

EU Cyber Security Policy
Eurowire – Bertelsmann (2011)
[EuroWire July 2011 | Bertelsmann Foundation]

Hackers reportedly linked to 'Anonymous' group targeted in global operation
Press statement, INTERPOL (2012
[http://www.interpol.int/News-and-media/News-media-releases/2012/PR014]

In the crossfire. Critical infrastructure in the age of cyber war
McAfee/Center for Strategic and International Studies (CSIS) (2009)
[www.mcafee.com]

In the dark. Crucial industries confront cyberattacks
Baker, Filipak and Timlin, McAfee/CSIS (2011)
[www.mcafee.com]

The meaning of Stuxnet - A sophisticated "Cyber-missile" highlights the Potential —and Limitations—of Cyberwar
The Economist (2010)
[http://www.economist.com/node/17147862]

The Stuxnet Outbreak -A Worm in the Centrifuge
The Economist (2010)
[http://www.economist.com/node/17147818]

W32. Duqu – The Precursor to the next Stuxnet
Symantec (2011)
[http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet]

ONLINE READING

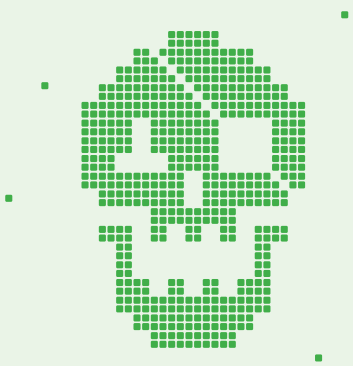
Nato
NATO has an online library which provides a 'few starting points to assist you with your research on issues related to cyberspace security, in particular, in the NATO context.'See www.natolibguides.info/cybersecurity

EU Policy on Network & Information Security
http://ec.europa.eu/information_society/policy/nis/index_en.htm
ENISA: http://www.enisa.europa.eu
EU Digital Agenda website:
http://ec.europa.eu/digital-agenda

GAO - Cyberwar resources Guide
[http://www.projectcyw-d.org/resources/items/browse?collection=17]

Cyber attack timelines
Italian IT specialist Paolo Passeri collects cyber attacks and puts them in daunting monthly and yearly timelines. Have a look at www.hackmageddon.com

Computer security
Fellow TA colleagues at ITAS / KIT are working on Compartmentalised Computer Security (CCompS), trying to isolate operating systems and applications differing sensitivity or risk from one another. See www.open-hypervisor.org

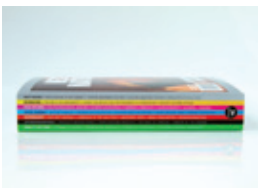


Creative Space

Volta Magazine highlights a trio of big ideas websites: multi-disciplinary connecting from a creative curator; the Truth-O-Meter that takes political accountability to new levels; and the think tank where nature and technology trade places.

'I think we need editorial more than ever right now' Steve Jobs / D8 Conference June 2010.

®Koert van Mensvoort WEB



NextNature: as wild and unpredictable as ever

The Next Nature Foundation is an Amsterdam-based think tank exploring the changing relationship between people, nature and technology. In themes like 'Back to the tribe', 'Office garden' and 'Anthropomorphobia', (the fear of recognizing human characteristics in non-human objects), it suggests we must challenge our existing notions and ask ourselves again 'what is nature?' The foundation has recently published a compendium of its most thought provoking observations and has a lab associated with the Industrial Design Department of the Eindhoven University of Technology, where end-of-term projects included self-camouflaging bikes and blushing dresses. The NANOWorld Map is designed in collaboration with the Rathenau Institute. Speculative products that could hit the shelves in the next decade go on tour in The NANO Supermarket. Think interactive wallpaint, or programmable wine.

www.nextnature.net;
@nextnature (twitter);

The Next Nature Book edited by Koert van Mensvoort and Hendrik-Jan Grievink (Actar, Barcelona);
NANO Supermarket and tour dates **www.nextnature.net/events/nano-supermarket.**

PolitiFact: who's telling the truth?

When US Republican party candidate Herman Cain suggested in 2011 that China is currently trying to develop nuclear capability, he scored badly on the Truth-O-Meter TM of PolitiFact. Hillary Clinton famously got carried away relating her Balkan adventures: "I remember landing under sniper fire". Every day, reporters and researchers of PolitiFact (2007), a project of the *Tampa Bay Times* and winner of the Pulitzer Prize for National Reporting in 2009, examine statements by American political movers and shakers with a special category, the Obameter, for keeping tabs on the President. Public utterances are analysed in detail and then assessed for their veracity as true, mostly true, false, mostly false, and pants on fire (after the saying liar, liar, pants on fire - see Cain and Clinton).

www.politifact.com;
@politifact (twitter)

Brain Pickings: combinational creativity

'Interestingness curator' Maria Popova (27), a Bulgarian-American writer, has spent the past six years developing a highly successful cultural blog and Twitter feed. Brain Pickings covers a wealth of disciplines across art, design, science and technology, empowering readers to 'combine them into original concepts that are stronger, smarter, richer, deeper and more impactful'. Popova produces three articles a day in addition to regular tweeting to over 165,500 followers, with a weekly online newsletter containing her best. A typical day's collection covers sage advice to children from *Narnia* author C.S.Lewis, a report of Frank Warren's PostSecrets project highlighted at TED, and a (gorgeously illustrated) review of *A Glorious Enterprise: the Making of American Science* – a history of the oldest natural history museum in the western hemisphere in Philadelphia. Her latest initiative is The Curator's Code, a standard to honour discovery across the web.

www.brainpickings.org;
www.curatorscode.org,
'@brainpicker (twitter);
@brainpickings (twitter)

Consensus conferencing

How can ordinary citizens contribute to the assessment of complex issues on science and technology? The 'consensus conference model' shows the way.

Text:
Jon Fixdal

Photo: Eivind H. Natvig

Imagine a group of 14-16 ordinary citizens engaging in a dialogue with a panel of experts about a complex technology policy issue. The discussions are focused on questions developed by the citizens themselves and they can formulate advice to policy makers on how that topic should be dealt with. This is what happens in a consensus conference.

The Danish Board of Technology developed the model in the 1980s and it has been used throughout the world to debate issues such as electronic surveillance (Denmark), spatial planning, mobility and sustainable development (Belgium), plant biotechnology (New Zealand), and genetically modified food (Norway). It is an exercise in practical democracy whereby citizens contribute knowledge and perspectives that scientists and experts might miss, because they are not influenced by scientific norms or economic interests.

A typical topic will affect a large part of the population, it will require scientific knowledge for clarification, and include ethical/normative issues. Part of the rationale for consensus conferences is that ordinary citizens can be just as qualified to assess such issues as experts.

'Citizens contribute knowledge and perspectives that scientists and experts might miss'

It takes place in three stages. Two preparatory weekends where the lay panel learns about the topic and formulates questions, the conference itself with questioning of experts who each give a brief presentation, and finally, the writing of the consensus report. This is often an intensive two or three days involving around-the-clock effort at the end. As soon as the final statement is ready, it is presented to policy makers and the media at a press conference.

Two of the most important contributions citizens can give to a decision making process, are valuative understanding and knowledge about the local environment. After an introduction to the topic, citizens without specialist knowledge are able to discuss and form opinions about how a technology might affect their values. They can also contribute with causal information about their home environment; knowledge they have accumulated by being members of their specific community.

Norwegian Citizens participating in World Wide Views on Global Warming in September 2009. World Wide Views was an international project, organizing consensus conferences on global warming in 38 countries around the world

Who are the participants? A lay panel in a consensus conference is a selection of engaged citizens. People who respond to an advertisement for participation, and who are willing to spend three weekends learning about and debating a complex policy issue. They cannot be considered representative of the broader public in any statistical sense, but by using criteria like age, education, occupation and area of residence, it is possible to increase the likelihood that the questions they formulate will cover a similar set of issues as another group fulfilling the same criteria.

Similar participatory models, like the German Planning cell method and the US Citizens panels, share a belief in the ability of ordinary citizens to debate and provide advice about complex issues. Discussions concerning the ethical sides of cell research or biotechology can provide great input for decision-makers and play an important role in lifting complex policy issues out of the often closed realms of experts and policy makers, and into the public sphere.

Danish Board of Technology **www.tekno.dk**

Andrea Bonaccorsi on playing the policy game: Europe must become more innovative

'It is not a waste of academic time to focus more on policy advice', believes Italian scientist Professor Bonaccorsi.

Text:
Marlies Hanifer
Photos:
3ipictures

Assessing the future of European society and the direction of scientific policy making is a hard one. "And sometimes it can be confusing" admits Andrea Bonaccorsi after the workshop *Coordination in the Science System* in Amsterdam. But his firm belief is that the quality of European science is lying behind the US, especially in emerging sciences such as IT, life sciences and material sciences, and a shift in policy is necessary for it to become more competitive and innovative:

"The worst-case scenario that could happen to Europe is that the gap between rich and poor European regions is maintained" he states. This will result in brain drain, disintegration in science systems, a highly polarised Europe resulting in a negative effect on the democratisation process on the continent.

'Europe has to put more effort in attracting top scientists to compete internationally with the US and Asia'

One might say Professor Bonaccorsi's career has been designed to prevent a worst-case scenario for Europe. His eagerness and ambition typify him not only as researcher, but also as a policy advisor and person. Bonaccorsi attributes a large role to science: it is most valuable when researchers are able to share their knowledge with society, he believes. But how adaptable are scientists themselves?

"In the past, the contribution of science to society has been mainly indirect and mediated by specialized expertise, separated in a profession. Today society demands that the interaction is more direct. Scientists often react to this demand with anxiety, because they feel the risk of external influence on the search for knowledge and a threat to their professionalism. But this is not necessarily true. We have to trust democratic societies, after all".

Innovation emergency

Besides his academic work focused on the economics of scientific policy, technological change and innovation, Bonacorssi fulfils an active role in advising the Italian ANVUR (National Agency for the Evaluation of Universities and Research Institutes) and the European Commission. With Europe declaring a state of 'innovation emergency' and R&D budgets lagging behind the US and Japan, what are the innovation obstacles in Europe being considered by the Innovation 4 Growth (i4G) panel of which he is a member?"There is lack of financial support for innovative ideas generated from research, because they are perceived as too risky even by the venture capital market. Or there are legal and administrative obstacles to the implementation of demand-driven innovation policies, using public procurement as a leverage for innovative solutions".

Economic studies of individual member states show that Europe has to put more effort in attracting top scientists to compete internationally with the US and Asia in areas of rapid growth believes Professor Bonaccorsi: "This can only be realised when European science policy focuses on three principles: the architecture of funding, clear selection and evaluation criteria and the mobility of human capital. Only with this competitive framework, can Europe become a strong innovative continent, with respect for diversity and local issues".

Funding

Bonaccorsi stresses the importance of joint programming in the European Research Area (ERA) which will result in a more accountable and transparent environment for research in Europe. He sees implementing multi-level funding as the key to success. This could mean a range of different partners including the government (central, regional or local), research councils, industry, foundations, NGOs and venture capitalists, playing an active role in selecting excellent research programmes. It doesn't necessarily need additional financing: "The fun part is that it is all about the way those resources are organised within the science system". Bonaccorsi stresses that if we manage to realise a more competitive model, the necessary innovative shift within Europe is possible. "Currently only a tiny part of research funding goes through a European *ex ante* evaluation process. If we were able to develop such a system for the bulk of research funding, including the one managed at national level, then we would have a standardised selection process and a much larger pool of resources for good quality research. The forthcoming report on socio-economic benefits of the European Research Area makes a compelling argument for cross-border funding inviting Member States to join funding schemes using a European evaluation procedure."

Equal opportunities

When taking a closer look at how our research system should be organised, Bonaccorsi believes clear selection and evaluation criteria should be standardised and managed at European level to improve mobility. "An excellent Greek researcher in computer sciences should have the same possibilities as the one in Germany" he avers. But as of now, the Greek researcher has fewer instruments than the German to find funding and career development opportunities. Standardisation is needed to avoid this current randomness and

Andrea Bonaccorsi was born in Pisa in 1962. He is professor of Economics and Management at the School of Engineering at the University of Pisa and has published widely on the economics of innovation and research policy. In 2011 he was nominated to be a member of the Innovation for Growth (I4G) expert group and has served as a member of several high level expert groups at the European Commission (DG Research). He has led the EUMIDA project, the project that has built up the statistical feasibility for a European system of microdata on universities. He is currently on leave from the university to serve in the Board of ANVUR, Italy's National Agency for the Evaluation of Universities and Research Institutes.

to resolve a scenario where science is following the dynamics of the rich versus the periphery. It's extremely important, believes Bonaccorsi, "to solve problems in 'weaker' European countries. The brain drain of less central regions should by all means be avoided". Financial support and cross-border funding should be in place to create equal opportunities: "In some cases it is useful to double or triple investments to the so-called cohesion countries".

Mobility

The mobility of human capital within Europe is a key factor in contributing to a competitive and innovative Europe. (Whether the Greek computer researcher wants to move to Germany, or vice versa, is a different matter.) Mobility enables Europe to improve areas of excellence, but moving around Europe is still not straightforward says Bonaccorsi: "The differences in welfare systems, pensions and salary between countries are just too big". Even young scientists are discouraged to move around, and it's obviously much easier for them than a 40-year-old researcher with a spouse or family. It is not usual in the European Research Area (ERA) to offer researchers a package – salary, welfare insurances, and career possibilities – as it is in Korea or Singapore.

Although Bonaccorsi is not really afraid that European researchers move to Asia for better opportunities, European science policy should still promote mobility within Europe as a positive thing for its researchers. We should not forget that Asia is gaining ground as a research region, while their government is investing enormously into science and institutionalizing their science systems. "Asian countries are actively contributing to a recently created benchmarking system, publishing data on research volume, quality and impact, and allowing all universities to examine their positioning across 250 disciplines", points out Bonaccorsi. "The system has been created by the United Nations University at Macau and currently covers all universities in North America and Asia (see www.researchbenchmarking.com). Paradoxically, European universities will be the last to be included in the system, because we still do not have a census of universities and a unified statistical system." And the grinding nature of European policy making systems may be at fault: "Since 2008 we have been discussing a European ranking system: in Asia they managed it in less than one year, also covering European universities!"

Scientists should feel they are contributing to society and have a positive effect on the process of democratisation

Science friendly Europe?

So, Bonaccorsi wants more attention to clear selection and evaluation criteria, mobility of human capital and the architecture of funding through cross-border and European coordination and standardisation. This is what Europe needs to catch up internationally, and become a well-balanced, diverse but equal Europe. But what lies behind this ambition? Although Bonaccorsi favours a competitive model, it is clear he wants to promote a European science system that is friendlier for researchers to work in and they they should feel they are contributing to society and have a positive effect on the process of democratisation: "Europe is historically the home of science. It is still a friendly place for scientists, but the opportunity cost of being a productive scientist in Europe is growing."

And many researchers are often frustrated that policy makers do not make use of their knowledge. "Maybe", starts Bonaccorsi, but continues: "Policymakers might not use academic knowledge directly, but they will be deeply influenced by visions and arguments that they are building upon. It is not a waste of academic time to focus more on policy advice".

Such time enables scientists to investigate a variety of issues, such as regional policies, the future of EU research and new indicators in science. "It might be a difficult attitude, still it is worthwhile" he says, as someone who has sat at innumerable policy making tables. His advice to other scientists is to follow suit: "Go directly into the field and play the game. Speak the language of policymaking. Be flexible but combine this with rigidity to the needs of the decision maker".

About the big picture he is very clear: "I am confident that science and democracy can grow together". In recent years, researchers may have felt threatened by governments pushing a populist rather than rational point of view. And here, according to Bonaccorsi, transparency is key: "There is even a moral obligation - 'can you trust me?' - science has a duty to society to produce knowledge". And that is what will make Europe strong.

Delicate Balance

When Technology Assessment began in the 1970s in the United States, its mandate was straightforward: to provide expertise to Congress. But over time, European organizations have taken on different roles in different countries. Why is that?

Text:
Philip Dröge
Photo:
Istockphoto

'There is much that the founders of technology assessment in the United States might learn from their progeny'

In 1972, the United States was the first country to establish a government agency aimed at assessing the impact of technological developments on society, including citizens' opinions. Until its closure in 1995, the Office of Technology Assessment (OTA) helped Congress make better informed decisions about science and technology.

In the early eighties, a number of European countries also established TA agencies. The idea behind them was initially clear. "Problems such as regulating the telecommunications industry, controlling air pollution, choosing military weapons systems, or constructing a national health care policy demand more expertise that can be asked of even the best educated and most attentive citizenry or most specialized representatives", wrote Bruce Bimber, then an assistant professor of political sciences at the University of California in his 1996 book *The Politics of Expertise in Congress*.

For the French, who founded the first European TA committee in 1983, TA was first and foremost a political tool, designed to inform and enlighten parliament. TA organisations established later, especially those in Denmark and the Netherlands (both from 1986), had an additional task: stimulating debate in society.

Double role

Many scholars theorize that the decision to give those newer TA organisations a double role was a reflection of the predominant political cultures. Denmark and the Netherlands typically have coalition governments, which are accompanied by more public debate and more compromise-seeking. In Denmark, a pragmatic type of egalitarianism permeates society. In these countries, TA would help to establish a public technology debate and create a public bedrock of knowledge and opinions to make political decisions on.

Other TA organisations founded in the late eighties and early nineties, like the British POST (founded in 1989) and German TAB (in 1990) have a mandate more similar to the American and French TA organisations - they have primarily been set up to inform parliamentarians and other politicians. The political culture of those countries is – according to Vig and Paschen – more 'elitist'. There is no one model in Europe; when incorporating scientific and technical expertise, each country has its own policy making style.

Yet the role of European TA is focused. Europe stated in the Lisbon Strategy that it wants to become a global leader in the field of innovation and TA could play an integral part in managing that process. There are now 18 organizations in the European Parliamentary Technology Assessment Network set up in 1990 and members of the European Technology Assessment Group provide TA studies for the European Parliamentary body STOA (Science and Technology Options Assessment).

Their role could become even more prominent as the need for independent assessment grows. In investigating the delicate balance between scientific exploration and safe societal benefits, the work of these TA organizations reaches far beyond European borders.

Read More?

Parliaments and Technology: the development of technology assessment in Europe eds Norman J. Vig and Herbert Paschen, State University of New York, (2000)

Technology assessment: democracy's crucible for the future endorsement of science and technology in the 21st century Robert McCreight, Policy Studies Journal, August 1 (2010)

Ocean Trash

Text:
Pascal Messer

Photos:
Mandy Barker

The millions of tons of plastic suspended in the North Pacific Ocean in an area known as the *Garbage Patch* bring devastation to marine ecosystems and wildlife. Plastic is a killer. UK photographer Mandy Barker has created collages from debris collected from beaches around the world to make a chillingly beautiful series called 'SOUP'. Her aim? "To make people act. Or at least make them think."

Translucent:
Ingredients; translucent plastic debris.

State of mind?
Contemplative, satisfied with the aims for my work, but always keen to progress.

Biggest success?
Being recognised and nominated for this years' Prix Pictet 2012, the world's leading photographic award in sustainability, is a great honour.

How did you get where you are?
By 4 years of studying photography, but more importantly: because I believe, with a passion and determination, that I had to put forward my point of view on this problem, to a wider audience.

Failures?
I would like to think I could see the positive side of everything, - even if things don't go exactly to plan.

Dreams?
To make people aware of problems through visual interpretation. And to prompt them to act. Or at the very least – to make them think.

What will it take?
In some respects I have achieved my dreams, taken by the amount of emails and enquiries I receive from around the world. People ask to use my images for publication or to re-blog on social networking sites, - they are very positive about my work and ask what they can do.

Biggest fear?
That people don't care.

Inspiration?
I get inspiration from people who seemed to have achieved the impossible when everything is against them. But I find inspiration in most things: it is all around us, in nature, art, books, in what people say and do and their experiences.

Plans for the future?
I want to visit the North Pacific Gyre to continue my work on marine plastic debris, by seeing the extent of the problem for myself and by documenting it. I am looking for sponsors or media partners to enable me to take part in such a research expedition. So, if anyone reading this would like to help, please contact me.

What would you change?
I would eradicate poverty and remove power from those who use it to detrimental effect. Closer to home, I would make conservation and environmental issues part of the school curriculum.

Until the 16th of June 2012, Barker's work can be seen in the Renaissance Photography Prize, Mall Galleries, London. She has a solo exhibition April through May 2013 at The Sugar Store Gallery, Brewery Arts Centre, Kendal, UK.

To support, and for more photographs and information:
www.mandy-barker.com

More info on marine plastic debris?
www.unep.org/yearbook/2011/pdfs/plastic_debris_in_the_ocean.pdf

Growing Pains

Europe has proved a hostile environment for GMO crops but is this zero-tolerance position sustainable?

Text:
Huup Dassen

Photos:
istockphoto

'The problems of implementation of the GMO legislation stem from the way these sensitive issues are handled at a political level.' John Dalli, European Commissioner

GMO crops are controversial. But particularly so in Europe. Public opinion is strongly opposed to their introduction and also the inclusion of GM products in processed foods. In other parts of the world, especially in the Americas, the opposite seems to be true. There the acreage of GMO crops is growing and new biotech cultivation applications reviewed with relative speed. In Europe, public perception has translated into public policy with only two GM crops (over a decade apart) approved for cultivation. Experts disagree on the question whether Europe can maintain this 'splendid isolation'.

In fact only a minority of six EU member states (Austria, France, Greece, Hungary, Germany and Luxembourg) ban the cultivation of GMOs completely, although this may not present the whole picture. According to biotech industry group EuropaBio, there are 15 'positive' and 12 'negative' countries in Europe, based on their last 10 GMO-related parliamentary votes. And substantial quantities of GM soy and maize are currently imported into European countries as cattle feed.

On the other hand, commercial crops are being grown on a very limited scale. In addition, the regulatory framework with regard to GMOs is very strict. It is based on the precautionary principle (producers of GMOs have to prove that there are no harmful effects, e.g. to the environment or health) and freedom of choice. This implies strict segregation of non-GM and GM products and mandatory labelling of the latter. The most recent attempt to address a regulatory framework that has been described as 'stifling' and 'dysfunctional' are proposals by EU Commissioner John Dalli to provide individual member states with more flexibility in allowing or blocking the cultivation of EU-approved GM plants on their own territory. They have so far ended up in a stalemate.

The relationship between producers of GM products and various European authorities has at times taken an unfriendly some might say hostile, turn. Biotech companies have not always found safe redress in Europe's legal institutions as illustrated by the case of Monsanto's GM maize and the French government (*see box*).

How can this difference between European countries and the rest of the world be explained? What makes GM so different from other modern technologies, which are more readily adopted?

Cultural traditions

Several experts point out that there is no single answer to this question. Both René Custers, regulatory affairs manager at the Flanders Institute for Biotechnology and Arnold Sauter, deputy director of the TA Bureau of the German *Bundestag*, point to some important cultural aspects. According to Custers the European attitude towards novel technologies in food and agriculture is fed by longstanding cultural food traditions. "These have become more prominent in recent decades, as witnessed by for instance the slow food movement", suggests Sauter. He adds that these differences also apply to attitudes towards possible risks, the role of the state, and individual and corporate freedom.

GM crops are grown on a limited scale in Europe

Helge Torgersen from the Institute of Technology Assessment in Vienna emphasises that particular regional problems and concerns also play a role, like the Austrian preoccupation with small-scale farming. "Similar idiosyncrasies can be detected in many countries, like France, Greece or Italy. What they have in common is that local issues neatly fit into a general debate on safety."

Food safety fears

NGOs have played a prominent role in this debate. According to Custers, "European NGOs have been much more successful than the pro-GMO bodies in influencing the political and policy debate, leading to an over-stringent GMO regulatory framework." To his fellow countryman Bart Staes, member of the The Greens/European Free Alliance in the European Parliament, this is no coincidence. He points out

that the start of the debate on the regulation of GMOs in Europe coincided with public concern about food safety caused by the BSE crisis in Britain and the widespread misuse of hormones in Belgian cattle. Sauter even speculates that the whole debate on GMOs might have had a different outcome, had these events not taken place.

Torgersen takes a similar line: "In my opinion, the current situation is not the result of divergent scientific concepts of risk or uncertainty, or a deeper concern over risk as a result of a rational cost-benefit calculation. It is the result of a series of contingent decisions, made over time by different players like the European Commission, declaring GM an indispensable future technology; Monsanto, shipping GM soy to Europe despite unclear regulations; Greenpeace, taking up GM as a campaign issue; various governments, reacting with stricter control and/or the precautionary principle, etc."

Long haul position

The fact that Europe's unique going-it-alone position is the result of a complex interplay of a wide variety of factors makes the question whether it stay the same in the future even more fascinating. The experts agree that in the short and medium term this shouldn't be a problem. As Arnold Sauter notes, "Europe's position is *de facto* a pragmatic one. All relevant GM crops can be imported and processed; they are just not being cultivated in many countries." So there is no urgent need for change and no need to challenge the generally negative public opinion in his view.

But when it comes down to the sustainability of Europe's *Alleingang* in the long run, opinions diverge. René Custers is most outspoken. He believes that at a certain point not only farmers but also groups of consumers will demand that certain types of GM crops can be cultivated and used in the EU. Livestock farmers are already feeling the consequences of not being allowed to use the same innovations as farmers elsewhere. And, in his opinion, the whole concept of 'the consumer' is misleading. There are many different consumers who all shop with different needs and ideals in mind. Some will certainly be interested in GM products that have clear health advantages, e.g. peanuts with their allergens knocked out.

'At a certain point not only farmers but also groups of consumers will demand that certain types of GM crops can be cultivated and used in the EU'

Bart Staes sits on the other side of the spectrum. Europe's agriculture is self-sustaining and will continue to be so. In his view GMOs are economically and ecologically unsound. They will not help to solve world hunger and farmers will become more and more dependent on a few large corporations for their seeds and herbicides.

Photo: Istockphoto

Legal battles

At times the public debate whether GMOs are acceptable has turned into outright conflict, sometimes with far reaching consequences.

***Non!* France bans GM maize (again)**

MON810 is a genetically modified strain of maize manufactured by US company Monsanto. It contains bacterial DNA that is designed to make plants resistant to pests that can threaten harvests and was initially approved for cultivation in 1998. In March 2012 the French government imposed a temporary ban arguing that this type of maize poses significant risks for the environment. The decision was taken despite the fact that an earlier ban (in 2008) had been overturned by the *Conseil d'Etat*, France's highest administrative court, and also by the European Court of Justice. In May 2012 the European Food Safety Authority stated "there is no specific scientific evidence, in terms of risk to human and animal health or the environment" to support a ban.

Pollination to 'contamination'

In September 2011, the European Court of Justice ruled that pollen was not a constituent of honey but an ingredient. It initially came about when an amateur beekeeper in Bavaria with hives near fields of GM maize, sued the state when GM pollen was discovered in his honey. The ruling has significant consequences. Because pollen has been categorised as an 'ingredient' it is subject to rulings on genetically modified food and feed, and for the beekeeping industry, the financial burden of testing and appropriate labelling (for example, 'produced from GMOs' if GM pollen is above the 0.9% threshold). There is also an impact on honey imports. Supporters of GMOs have always argued that their crops can safely coexist with conventional crops without fear of contamination. As it turns out, if such contamination occurs, it has dramatic consequences for the conventional farmers. Opponents see the ruling as further support for their zero-tolerance argument that these crops should be completely banned.

No market for GM products in Europe?

When *Time* magazine asked "Is Europe finally ready for genetically modified food?" in March 2010, when the green light was given by the European Commission to the cultivation of a second GM crop in Europe, it spoke too soon. In January 2012, the German chemical group BASF announced it had decided to stop promoting its GM Amflora potato designed for industrial use in Europe and was moving most of its plant science group to the United States. Developing products for the European market no longer made business sense, stated BASF spokesman Dr Stefan Marcinowski: "There is still a lack of acceptance for this technology in many parts of Europe – from the majority of consumers, farmers and politicians."

A more sceptical view is Helge Torgersen's. He believes that Europe cannot change its present position as long as public opinion stays the same. To him the question is not: can Europe maintain its position, but rather under which conditions would the need to change European GM policy be so urgent that politics would ignore consumer disapproval?

Future scenarios

With no imminent change to present policy, there is time to consider possible future developments. According to the authors of a recent report by the Netherlands Commission on Genetic Modification (COGEM) together with the Rathenau Institute, scarcity and rising prices will be the most powerful contributors to creating external pressure to accept GMOs. Today's low public acceptance may change when the perceived risk of GMOs equals that of conventional products; or when GMOs have obvious advantages (price, taste, health); or, perhaps ironically, when public debate shifts to another subject like nanotechnology or the consumption of meat.

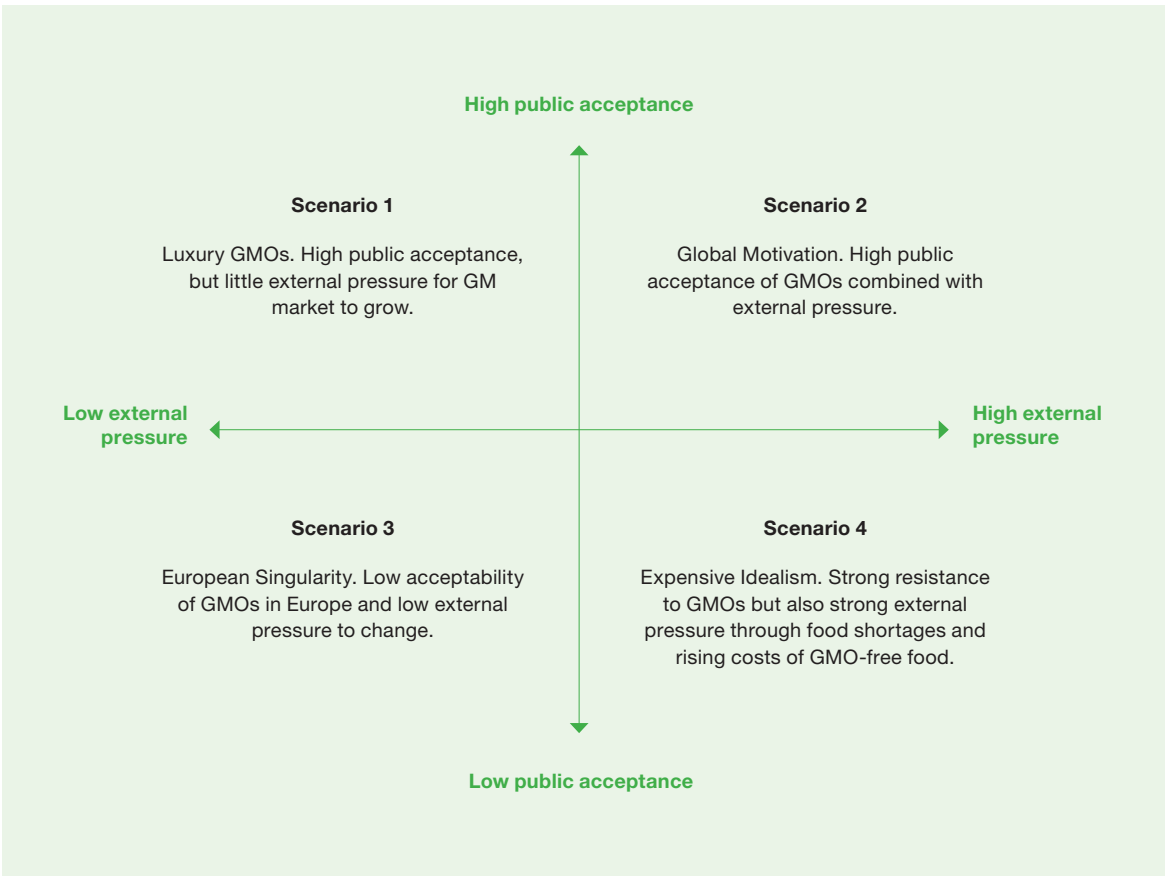
Defined by two so-called drivers (high or low public acceptance of GMOs and high or low external pressure to accept them), the report distinguishes four possible scenarios (*see table*). The assumption in all scenarios is that outside Europe GMOs are cultivated at the present scale. Obviously these scenarios serve as frames of thought and as such are striking illustrations for the fact that there are no simple solutions, whichever turn the future will take.

Photo: Istockphoto

Read More

Stats on worldwide GM crop growth
www.isaaa.org/resources/publications/briefs/43/pptslides/default.asp [includes table of countries and crop sizes]

Future scenarios
COGEM, Rathenau Instituut, Vier scenario's voor ggo's in de Europese landbouw. The Hague, december 2010 (in Dutch. Download from www.cogem.net/index.cfm/nl/publicaties/publicatie/mondiale-motivatie-of-europese-eigenheid-vier-scenario-s-voor-ggo-s-in-de-europese-landbouw. An English translation is in preparation).



Cosmetic labelling
The last free summer for the nano

In July 2013, the new EU directive on Cosmetics will come into play requiring manufacturers to state on the label of creams, lipsticks and sunscreens if nanoparticles are contained. European politicians have their say.

Text:
Emiliano Feresin

Photo:
Istockphoto

Materials defined as 'nano' are sized in billionths of a meter and show different physical and chemical properties from the bulk form. If added to a product they can enhance or change its features. For example, titanium dioxide is a known ultraviolet absorber and sun reflector additive in sunscreens, but manufacturers prefer it in its nano form. That's because it makes the sunscreen transparent on the skin, instead of white. As well as declaring their presence on the label, the EU will require producers to submit a detailed safety report on the nanomaterials used.

Unanswered questions

It's difficult to decide for or against nano-labelling, because many questions need to be answered first. For example which nano definition do we want to use? Which size range do we choose for that and do we include natural particles as well? What should this labelling tell the consumer? Should consumers handle nano-products differently from standard ones? I don't see these questions answered fully yet. Once we have the answers, then labelling more consumer products might be a good idea. Personally I would prefer a sunscreen without nanoparticles, but most sunscreens sold in Germany include them already.

Rene Röspel, German MP, **www.roespel.de**

Consumers should be informed

Nanotechnology is a powerful scientific field. Its advances can offer great opportunities for the EU's growth, competitiveness and sustainable development. At the same time, nanomaterials may bear risks for consumers and workers. If cosmetics include nanomaterials, safety concerns must be paramount. Consumers should be informed of all product ingredients, including nanomaterials, in order to choose their products accordingly. I am therefore in favour of the labelling of nano-content in cosmetics and sunscreens. I personally will continue to use sunscreen containing nano-particles. Cosmetics manufacturers are prepared for the change in legislation and will have the opportunity to provide consumers with an even bigger variety.

Richard Seeber, EU MP from Austria, **www.richard-seeber.at**

Nano-labelling in food should come before cosmetics

I clearly support the labeling of cosmetics and sunscreens containing nanomaterials. According to the Woodrow Wilson inventory on nanotechnology, 143 cosmetics products and 33 sunscreens currently on the market contain nanoparticles, so I suppose manufacturers will have to endeavor to evaluate safety and labelling standards. Similarly with the case of labeling of GM food products, I assume that nano-cosmetics labeling will slow down the business. In my opinion labelling is much important for food products containing nanomaterials, since several studies show that there is lack of safety information on various nanoparticles used in food. Personally I would not buy nano-sunscreens nor eat food containing nanomaterials.

Maya Graf, Swiss MP, **www.mayagraf.ch**

Could labelling cause alarm?

I am not against the nano-labelling of cosmetics and products containing nanomaterials in general. But it's important that any label comes with a key to understand what it says: the possible risks, the appropriate behavior to minimize that risk – we also need more research on these issues. But a label with no explanations could unleash alarmed reactions in the population. Personally I don't have problems using sunscreens with added nanoparticles, since there is no proven risk for the skin. Instead, I would be more careful with products or materials that free nanoparticles in the air, because they could easily get into contact with our lungs thin tissue, altering cellular functions.

Vittorio Prodi, EU MP from Italy, **www.vittorioprodi.it**