Interview with Neelie Kroes about Trust and Security in the Digital Agenda

This article is the transcription of the interview of the PvIB board members with mrs. Kroes. You can send your comments to board member Thom Schiltmans, by email to thom.schiltmans@gmail.com

The next boardmembers of PvIB were involved in this interview with Mrs. Kroes: Thom Schiltmans, Philips Healthcare, Sector IT Security Manager; board member PvIB Education

Fred van Noord, Verdonck, Klooster & Associates, Management consultant information security & risk management; chairman PvIB

Tom Bakker, Delta Lloyd Group, Group Security Officer / Business Continuity Coordinator; board member PvIB, editor PvIB-magazine "Informatiebeveiliging"

Erno Duinhoven, Capgemini, Managing consultant information security & risk management; board member PvIB Professionalizing.

Implementing the ambitious Digital Agenda for Europe would contribute significantly to the EU's economic growth and spread the benefits of the digital era to all sections of society. The Agenda outlines seven priority areas for action: creating a digital Single Market, greater interoperability, boosting internet trust and security, much faster internet access, more investment in research and development, enhancing digital literacy skills and inclusion, and applying information and communications technologies to address challenges facing society like climate change and the ageing population.

Trust & Security, one of the priorities in the Digital Agenda, is of special interest for information security. In this interview you find the answers on the questions we asked Vice President Neelie Kroes, Commission Vice-President for the Digital Agenda on several key-actions. We related our questions (*italics*) to key actions (**bold**) in the Digital Agenda.

Key-action 1: Simplify copyright clearance, management and cross-border licensing.

What is the vision of Mrs. Kroes on 'net neutrality'?

- *What is the definition of 'net neutrality' by Mrs. Kroes?*
- What are the limitations on 'net neutrality' in the vision of Mrs. Kroes?

NB. Recently Chili was the first country in the world to approve a law which guarantees 'net neutrality'.

Answer Mrs. Kroes: The European Commission is committed to preserving the open and neutral character of the Internet in Europe. But traffic management and net neutrality are highly complex issues and the terms mean different things to different stakeholder groups. In any event, it is clear that full and effective transparency is essential to enable consumers' choices. Consumers should be able to access the content they want while content providers and operators should have the right incentives to keep innovating and investing.

The revised EU telecoms framework adopted in 2009, which comes into force in May 2011, already contains strict transparency requirements and grants national regulators the power to set minimum quality levels for network transmission services in cooperation with the Commission.

Member States are still implementing the EU telecoms rules into their national legislation and the Commission is closely monitoring the situation concerning potential net neutrality issues. Moreover, we are stimulating debate and examining the contributions to a public consultation (which we ran from end June to end September 2010), and we will report to the European Parliament and public about the results.

Key action 5: As part of the review of EU standardization policy, propose legal measures on ICT interoperability by 2010 to reform the rules on implementation of ICT standards in Europe to allow use of certain ICT fora and consortia standards.

NIST, the National Institute of Standards and Technology, defines standards on information security. The NIST standards are available for free. The Dutch government uses NIST standards for several purposes and also the industry uses NIST standards.

Are there any possibilities for using NIST standards by the EU in the opinion of Mrs. Kroes?

Answer Mrs. Kroes: Yes, but the answer is more complicated than that. The European Commission supports use of both European and international standards. We think this is key to competition and competitive industries - and the priority is good and widely-used standards. But our main role is to promote the use of standards rather than to endorse particular standards. NIST supporters should work within CEN, CENELEC and ETSI at European Level and ISO, IEC and ITU at international level to promote NIST. If a NIST standard is accepted by the ISO, for example, the standard would then become European through the Vienna Agreement.

Key action 6 and 7: Present in 2010 measures aiming at a reinforced and high level Network and Information Security Policy, including legislative initiatives such as a modernized European network and Information Security Agency (ENISA), and measures allowing faster reactions in the event of cyber attacks, including CERT for the EU institutions.

Present measures, including legislative initiatives, to combat cyber attacks against information systems by 2010, and related rules on jurisdiction in cyberspace and international level at 2013.

Trust and security is related to the proven knowledge and skills of people who are

active using the internet. In the digital agenda we did not find any actions on creating user security awareness.

Does the EU have any plans or action on the introduction of a internet driver license (or internet data license)?

Answer Mrs. Kroes: No. The key objective of the Digital Agenda is to promote access to the Internet, not to restrict it. We do not want the entire Internet to become a walled garden. But it is true that we must work towards increasing user awareness of safety issues. Banks for example are well-placed to work with citizens to give them both services they want online and training they need to feel confident in using them. For example, the UK Cabinet Office has worked with industry in partnerships for a number of years to achieve such outcomes, and now these have developed into industry-driven projects like Bank Safe Online (see http://www.banksafeonline.org.uk/). The Commission is keen to promote such partnerships and best practice.

The UK government supports the qualification of information security professionals on a wide area (www.instisp.org). Also within the Netherlands are initiatives for qualification and certifications of information security professionals in a wide area of their profession.

Does the EU have any plans on having to meet any international recognized qualification for information security professionals?

- *What are the advantages in meeting international recognized qualification for information security professionals in the opinion of Mrs. Kroes?*
- *Does the EU want a publicly available registry for information security professionals which public consultation is possible, similar to healthcare workers in the Netherlands (BIG-registry, a registry for professionals working in healthcare), and if what are the main reasons in the opinion of Mrs. Kroes for (not) wanting such a registry?*
- *Does EUROPASS provide in qualifications for information security professionals on a wider area then a pure technical area?*

Answer Mrs. Kroes: In order to attract good people to working with ICTs, in both the private and public sectors, it is very important to have skills frameworks and well-known career ladders. Through such tools ICT professionals can plan better and make smart choices.

The European Commission is committed to developing tools to identify and recognise the competences of ICT practitioners and users by 2012. These should be developed in connection with the European Qualifications Framework (EQF) and EUROPASS, so as to make national qualifications more mutually recognised across Europe and to promote the mobility of information security professionals.

As to a publicly available registry, I wonder whether this would not be better organised at the level of PvIB and your sister organisations?

In the opinion of Mrs. Kroes, does the EU on itself have the power to face cybercrime or are there any thoughts on working together with other large economies / countries?

- *Which relation does Mrs. Kroes see in the current lobby of the US government in counterfighting cybercrime?*

Answer Mrs. Kroes: The importance of the different elements making up the Internet is sometimes perceived in very different ways. This partly explains the diversity of governmental positions expressed in international fora and the sometimes contradictory appreciations of the urgency of this matter. Cyber security is vital for the European economy, to protect the businesses and operations of ordinary citizens. Users must be safe and secure when they connect online. Besides, some of the most innovative and advanced online services - such as eBanking or eHealth - would simply not exist if new technologies were not fully reliable.

This is why the Digital Agenda for Europe contains key actions to allow faster reactions and combat cyber attacks against information systems. An integrated EU approach is required because of the international dimension of the problem. We have to achieve a common consensus on the priorities in terms of public policy and of operational deployment. In this way, we will add value to national programmes and be able to engage third countries and international organisations to develop a set of principles reflecting European core values.

This is where ENISA (European network and Information Security Agency) comes in. ENISA's job is not to maintain security on behalf of Member States, but to help them work together to both strengthen the weakest links in the chain, and to lift security in general. In practice that means EU-wide training exercises and working more closely with Europol and Interpol, for example. ENISA can only be as strong as the working relationships it and Member States can develop with each other.

What does Mrs. Kroes see as the most dangerous developments and threats in cybercrime which have to be dealt with at EU level?

- *Which low effort countermeasures will have the largest effect on the safety of the ICT infrastructure and the internet (low-hanging fruit)?*

Answer Mrs. Kroes: There are widely varying opinions on the extent of the threat from so-called "cyber-war", or cyber-threats in general. The Internet is generally remarkably robust - but there are no guarantees it will stay that way if we grow complacent. IT networks and end users' terminals remain vulnerable to a wide range of evolving hazards: from identity theft to spam spreading a wide range of viruses and malicious software. Attacks are becoming increasingly sophisticated (trojans, botnets, etc.) and often motivated by financial gain, but they can also be politically motivated as shown by recent cyber-attacks that targeted Estonia and Lithuania.

Clearly more effort is needed to prevent the next Estonia-type situation. Cross-border threats demand cross-border coordination, it's as simple as that. The first EU-wide cyber security preparedness exercise is taking place in November 2010: that should provide a better understanding of the extent of threats and remaining weak points in networks and information systems. The next steps are effective and rapid implementation of the EU action plan for the protection of critical information infrastructure and of the Stockholm Programme (which is under the responsibility of my colleague Cecilia Malmström).

With the EU institutions a Computer Emergency Response Team or "CERT" is clearly needed.

The internet infrastructure is mainly in the hands of private companies. What is the opinion of Mrs. Kroes on the cooperation between the large amount of private held companies, the national governments ant the EU in fighting cybercrime?

- *What is the role of market parties in the fight against cybercrime?*
- *What is the vision of Mrs. Kroes for pubic/private partnership in fighting cybercrime?*

Answer Mrs. Kroes: Cybercrime is everyone's responsibility. The EU is supporting ICT-based public private partnerships (PPPs) with €1 billion to leverage around €2 billion of private spending by 2013.

PPPs are designed to establish European leadership in future strategic technologies that will help to stay ahead of challenges like tomorrow's information infrastructure.

Moreover, national PPPs are now being enriched by the European Public-Private Partnership for Resilience (EP3R) launched by the European Commission under the CIIP (Critical Information Infrastructures Protection) action plan of 2009. In addition to the existing national initiatives and the operational activities of ENISA, the EP3R will support the exchange of information and knowledge on specific topics with an EU and international dimension. It should foster the involvement of the private sector in the definition of strategic public policy objectives as well as operational priorities and measures in order to bridge the gap between national policy-making and operational reality on the ground.

An efficient network of CERTs should be established in Europe. That is why ENISA is already mobilising and supporting Member States in completing the establishment of their own national CERTs.

The EP3R should also address the needs and procedures to ensure information exchange to prevent and prosecute cybercrime. Finally, it is important that internationally coordinated actions which target information security are pursued and joint action is taken to fight computer crime.

Key action 9: Leverage more private investments through the strategic use of precommercial procurement and public-private partnerships, by using structural funds for research and innovation and by maintaining a pace of 20% yearly increase of the ICT R&D budget.

How can the security and privacy within solutions like national Electronic Medical Record Systems profit from this increase of ICT R&D budget so that convincingly can be proven for everyone that this kind of solutions can be implemented securely and still provide the benefits for EU and national healthcare?

- *What are the advantages and disadvantages of self-control by the civilians in the opinion of Mrs. Kroes in the possibility in managing authorizations on his/her own files and be given access on the log files to see which medical professionals have had access to the medical files?*

Answer Mrs. Kroes: eHealth systems use the power of ICTs to enable patient empowerment and better care. In particular they can provide better information both to patients and to healthcare professionals as well as give personalised guidance, which can improve illness prevention and chronic disease management. At the same time, fast and secure access to personal health data can help greatly in cases of urgent need for medical intervention anywhere in the EU.

A good example of this is the epSOS large scale pilot. epSOS aims to develop, test and validate patient summaries and ePrescription solutions across borders. The project has identified the pilot sites which will run the services and in November 2010, we will launch a testing event open to all companies willing to implement the specifications defined by the project. In practice, this could mean that an EU citizen on holiday could be treated abroad by a doctor who has access to potentially life-saving information.

However, citizens will only use new technologies and e-services if they trust that their personal data, especially sensitive data related to health, is safe. Current technologies could ensure the appropriate level of security and privacy from a technical point of view, but the main issue is at the legal and organisational levels of implementation. Legislation needs to offer cross border services with a harmonised level of security and privacy. In addition, the processes and responsibilities at all levels of organisations (public and private, governments and health care providers) need to enforce and ensure the targeted level of security and privacy. For this reason, the ongoing review of the data protection regulatory framework aims to modernise all relevant legal instruments to meet the challenges of enhancing trust and confidence by strengthening citizens' rights. In parallel, under the Digital Agenda we will launch a set of actions to strengthen further the network and information security policies.

What is the optimal rate between investments in information security and other parts of ICT in the ICT R&D budget?

Answer Mrs. Kroes: This is not a figure that can be written in black and white terms. Every year, the ICT programme committee, the ICT advisory group and other preparatory stakeholder consultations define priorities which determine the ICT R&D calls for proposals. We are then bound by the quality of the proposals we receive. Better proposals obviously mean more chance of funding. So while trust and security improvements matter, they are competing with other priorities. For example, there is no point in securing a network or service that doesn't exist, so these aspects of ICT also need funding.

Key action 12: Access by 2012 whether the ICT sector has complied with the timeline to adopt common measurement methodologies for the sector's own energy performance and greenhouse gas emission and propose legal measures if appropriate.

A large number of information security professionals are worried about smart energy meters.

- *What are the guarantees of the EU to security and privacy for smart energy meters?*

Answer Mrs. Kroes: The right to privacy and to the protection of personal data are fundamental rights in the EU which we take very seriously. We recognise that there are potential privacy and security concerns when introducing smart meters and we surely want to avoid them. But we must also make sure that people get informed about their energy use and empower them manage their consumption. , Moreover, smart metering will support the roll out of smart grids. The banking and payment card industries may offer valuable lessons how to approach this, by developing a list of high level principles to be implemented at EU level, by which smart grid operators could design their systems and processes. We support the view that there is a need to distinguish between individual consumers and aggregated technical data (used for grid management) to minimise the vulnerability of private data. As transmission is so vulnerable from a privacy point of view more work will also need to be done to clearly assess the most appropriate encryption measures to be used.

This interview with Neelie Kroes, Commission Vice-President for the Digital Agenda was based on the English version from 19.05.2010. Since 26.08.2010 the translated Dutch version is available on http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245(01):EN:NOT.

See also: http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=5826 for the Digital Agenda and related documents. On http://ec.europa.eu/information_society/newsroom/cf/pillar.cfm?pillar_id=45 you can find the list of specific actions to enhance trust and security within the European Union.