PORTUGAL 2007

Future Group
new ideas for
a free and safe Europe

PT

PUBLIC SECURITY, PRIVACY AND TECHNOLOGY IN EUROPE:

MOVING FORWARD

Concept paper on the European strategy to transform Public security organizations in a Connected World

The classical discussion on the balance between individual liberties and security, including today the prevention and repression of global terrorism remains actual. In this context, it is very opportune the proposal by the European Commission to discuss these issues in the framework of the Future Group.

This balance implies decisions on common policies, security strategies and legal rules at the European level, taking into account the future Lisbon Treaty, as we already discussed in the meeting of the Future Group held in Funchal, Madeira. However, there is an important factor that should not be underestimated, which is the role of technology. Technology is not neutral; it must be put at the service of security with respect by the way of life of the citizens in the democratic countries and can have a decisive contribution towards making a global world more secure. This concept paper aims at stimulating that reflexion.

I. The subject

1. The work of the Group of the Future will offer a significant contribution for the elaboration of the planning of an EU home affairs policy towards 2014.

In preparing the meetings of the Future Group during spring 2007, a series of challenges for the future were identified. The debates that followed, in Eltville, Brussels and Madeira, confirmed that enhancing the use of information technologies by law enforcement and judiciary authorities is one of the main challenges we face and deserves a very high priority.

This paper is a contribution to the discussions on this challenge from the perspective of crime fighting and crime prevention co-operation in the EU. The aim is in particular to put some questions for discussion with a view to highlight some possible avenues or actions for achieving a co-ordinated and coherent implementation of measures of technological modernization in the area of public security organizations.

2. The modernization of law enforcement structures is occurring at fast pace in all Member-States. The intensive use of Information and Communication Technologies (ICT's) became a crucial part of that process, allowing police forces to improve efficiency and spare human resources, namely to deliver more effective frontline service to communities and face new threats.

A key factor in that drive has been the adoption of changes to previous information technology policies in order to achieve better value and greater efficiency through measures such as the use of off-the-shelf programs (thus reducing the need for customized applications), greater compatibility with partner organizations' ICT systems, simplification of user interfaces (allowing increased staff satisfaction and easier training) and quick adoption of products delivered by security research. New tools (vg. Schengen Information System, Eurodac) made available by European institutions currently allow the sharing of information under new conditions and the modernization of police forces has been stimulated (namely as a requisite to the Schengen enlargement on December 21).

The overall level of technological development already reached and the fast growth of mobile communications and electronic networks will allow a more efficient adoption of advanced collaboration tools to be used by police forces in different countries. The present and future technological environment favours a truly efficient access of public security organizations to scores of information sources, not only the ones that are made available by Interpol and Europol but an immensely growing number of virtual libraries, "document vaults" and news aggregators.

3. Although home affairs are and will be, under the Lisbon Treaty, at the core of each Member State, the built-in limitations - for instance, as to how far the exchange of information by means of information technology can be developed at EU-level – should not be an obstacle to new forms of working together that will require digital platforms of collaboration, under strict rules that guarantee security and data protection.

There is a consensus on the crucial role that the European Union has to play in the definition of plans that may strengthen the coordination of efforts to fight against terrorism, organised crime and other threats to the EU and its citizens. The Union should therefore be particularly dynamic in demonstrating its capacity to drive forward policies at EU-level and by working together with law enforcement and judicial services in the daily efforts to meet the present challenges and the ones ahead.

Crisis management of terrorist incidents is only one of many areas of security which requires a very significant investment in new technological solutions. It stands to make tremendous progress through the development and integration of satellite and airborne monitoring capabilities, the use of GMES technologies, including multilayer mapping with modelling tools and the development of shared, interactive and secure information, communication and analysis tools.

The Presidency considers however that similar challenges are to be found across the whole spectrum of security. In the area of the fight against terrorism it decided to focus, besides the pursuit of the Check the Web initiative, on furthering work on the constraints and possibilities of Close Circuit Television (CCTV) technology in particular and detection technology, more in general, for the deterrence, detection and disruption of terrorist attacks, the rapid response thereto and the successful investigation thereof.

Biometric identification and the detection of false documents are also key areas to monitor, apprehend and successfully convict terrorist suspects moving through international transport systems and border posts as are land and maritime border monitoring technologies to address other movements of persons, and trafficking in weapons, explosives or other terrorist weapons.

We try to promote, notably in the working of the “future group”, prospective thinking about tomorrow’s technological security requirements.

It will be in our view very important to provide strategic guidance to the Union’s very substantial security research programs so that the basic and applied research is directed towards meeting the real needs of our intelligence and law enforcement officers.

That said, there are in the Presidency's view very substantial and simple gains to make by simply knowing and sharing what relevant technology we already have. It is very probably the case that the Union institutions already have at their disposal tools developed for different purposes which could be of significant use for the fight against terrorism in particular and security more in general.

We also believe likely that results of Union financed security research projects may have not been thoroughly scrutinised by security experts of the member states in terms of potential practical use.

Finally, we believe that many Member States have developed or acquired over the years security tools required to meet their individual needs many of which they could be prepared to share with partners, especially if the costs entailed could be met, at least partially by the EU budget.

The Presidency considers it would be worth reflecting on establishing a European pool of security tools. Such "tool pool" would not be a place, a body, or a data-basis but rather an innovative concept allowing member state and EU institutions to make available and secure condition tools of proven or potential use in the security field for appraisal and or testing by authorities of other member states and, where useful, support its mutual deployment e.g. by meeting related license costs, translation and training.

Portugal believes technology can make a very significant contribution to help to prevent and meet tomorrow's challenges. That can often be done at low financial costs, in relatively short time and with very significant productivity gains for our services, allowing our officers to focus on those tasks only they can accomplish. We believe the Union can and should assist."

If on the short run, a toolbox of resources already existent should be made available to Member-States and gradually widened, on the long run, measures should be taken to allow European public security organisations to be on the frontline at a global scale and cooperate with transatlantic partners in the missions necessary to tackle threats already identified and the ones the future will bring.

4. The process of change has already begun, as the current "Preparatory Action for Security Research" programme includes projects on relevant issues such as imaging for security, crisis early warning situation awareness architecture concepts, testing and

certification of biometric components and systems, people realtime observation in Buildings or standards for border security enhancement.

On the other hand, positive results of European policy making should be further expanded and applied. Special attention should be granted to the 2007 communications "on Public-Private Dialogue in Security Research and Innovation" and "on Promoting Data Protection by Privacy Enhancing Technologies". These initiatives were preceded by the 2006 important communications on "A Strategy for a Secure Information Society" and "on Fighting spam, spyware and malicious software". These initiatives taken by the Commission paved the way to relevant measures to be implemented, both by the Commission and the Member States, to tackle security challenges in relation to information systems and networks in the EU, outlined a comprehensive and dynamic policy framework founded on a holistic and multi-stakeholder approach and correctly underlined the need to foster international co-operation to secure networks in our globalized world. As a reaction to these two Communications, a Council Resolution was approved on a Strategy for a Secure Information Society in Europe (2007/C 68/01).

Similarly, further action will be taken in order to allow the Council to endorse far-reaching policy objectives and priorities discussed on the Brussels Conference on Public Security, Privacy and Technology (20/11/07).

It should also be taken in consideration that, as a follow-up of the Conference of the Chief Information Officers of the police forces of EU Member States and of relevant European and international police (23-25/05/07) dealing with "Interoperability and data exchange between the European Police Forces", the European Police Chiefs Task Force (EPCTF) drafted a document that outlines briefly and on a high level a vision of the common requirements of the European police on IT support (Common Requirements Vision). At the expanded Troika meeting of the EPCTF on 10 July 2007, Germany was tasked to prepare the first draft of the Common Requirements Vision –document which is still under discussion and highlights that

> "similar to single enterprises or institutions, the police forces in Europe require a common basis for their co-operation. This co-operation is largely dependent on the exchange of information, requiring all participating countries and institutions to make their national IT systems interoperable with other national, trans-national or central IT systems such as SIS, VIS, Europol IS, Interpol, Eurodac, Prüm etc"".

The purpose of the present paper is wider, but, not surprisingly, it converges with the Common Requirements Vision–document in exploring key drivers that influence organizational and operational needs of European public security organizations.

.

II. The Digital tsunami and its consequences for public security organizations

5. Put in more detail, the present discussion paper seeks to address the identified challenge with a view on how public security organisations should change to grasp the opportunities offered by as increasingly connected world.

The fact that the world is and will become more and more connected and is going digital as more people, machines, and environments are connected has to be duly acknowledged. This change vastly increases the amount of potential information for use in the day-to-day operations of public security organisations.

One obvious illustration is the ability to track the location of any active mobile phone (and to know where it was last switched off and last switched on). This is just the beginning. In the next few years billions of items in the physical world will be connected, using technologies such as radio-frequency identification (RFID), broadband wireless (WiFi, WiMAX), satellite and small area wireless (Bluetooth, wireless USB, ZigBee). This means it will be possible to trace more and more objects in real-time and to analyse their movement and activity retrospectively. We will soon see this with respect to major consumer items such as cars, but this trend is likely to spread quickly to most items of any significant value. In the near future most objects will generate streams of digital data about their location and use – revealing patterns and social behaviours which public security professionals can use to prevent or investigate incidents.

The recent Conference on "RFID - The next step to The Internet of Things", (15-16 November 2007) identified several social contributions of RFID and THE INTERNET OF THINGS, namely the “potential to benefit people in many ways: safety (e.g., food traceability, healthcare, anti-counterfeiting of drugs); convenience (e.g., shorter queues in supermarkets, more accurate and reliable handling of luggage at airports, automated payment in highway tolls, parking lots, etc.); and accessibility (e.g., disabled people)”. The Conference concluded that in the future, the Commission should “stimulate research on security of RFID systems, including light-weight security protocols and advanced key distribution mechanisms, with a view to preventing direct attacks on the tag, the reader and the tag-reader communication” and

"support further development of privacy enhancing technologies as one means to mitigate privacy risks".

The conclusions of the Presidency on the Outcome of the Conference (www.rfid-outlook.pt) also mentioned that

> "accelerating the process for Europe to take full benefit of the opportunities opened by RFID based applications and THE INTERNET OF THINGS requires effectively addressing at an early stage privacy, data protection, and security concerns in order to assure the confidence of consumers and the industry, and, therefore, it would be desirable to bring as soon as possible these issues to the considerations of the Justice and Internal Affairs Council".

Another expanding source of data is digital transactions. All credit or debit-related purchases already generate monitorable and searchable real-time information; but more and more transactions will be of this kind as we move towards a cashless society where mobile phones or other devices (such as London's Oyster card, Paris's Velib card, the Belgian Proton card etc) are used to make minor purchases.

These trends will be reinforced as biometric measurements are used to enhance security at more and more locations – whether public places such as town halls or train stations; private locations such as amusement venues; or places of work. Most large cities have already seen a significant increase in the use of closed circuit television (CCTV), and usage (by public and private sector organisations) is likely to increase further and to shift from the current analogue technologies to more easily storable and searchable digital technologies.

Further accelerating the tsunami of data is online behaviour. Social networks such as MySpace, FaceBook and SecondLife - and indeed all forms of online activity - generate huge amounts of information that can be of use to public security organisations.

These trends have huge implications for public security. Citizens already leave many digital traces as they move around. What is clear, however, is that the number of those traces (and the detailed information they contain) is likely to increase by several orders of magnitude in the next ten years.

Every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations, and create huge opportunities for more effective and productive public security efforts. There will also be significant risks of criticism where failures occur, since critics will point to the hundreds of ways the authorities could (or should) have noticed what was happening.

Clearly, these developments raise fundamental issues in relation to privacy and how much information about the behaviour of citizens should be shared with States and in what circumstances.

Balancing citizen expectations of privacy against their expectations of proactive protection is not a new dilemma for public security organisations, but it is taking on an ever more acute form.

In the "digital tsunami" environment – which is here to stay and grow– the traditional measures to protect privacy will become less and less effective unless appropriate technological measures are used as an essential complement to legal means.

In order to achieve a sufficient level of protection "privacy enhancing technologies" are – presently and in the foreseeable future- absolutely essential to guarantee civil and political rights in the age of cyberspace.

Paradoxically, those same tools can also be used by terrorists and other criminals. Thus, if data are automatically anonymised, after a certain lapse of time, that procedure may erase evidence of crimes; encryption tools prevent hacking when information is transmitted over the Internet and protect personal data against unlawful processing but may also help conceal criminal plans; cookie-cutters enhance compliance with the principle that data must be processed fairly and that the data subject must be informed about the processing going on, but may also make ineffective police efforts to gather information on illegal activities.

The complex challenge we face is to keep high levels of protection for common citizens and allow the fair use of effective tools against criminals, thus protecting public security.

6. Many signs show that three principles will define the emerging model for policy and public services:

- Use the networks as a platform for collaboration, communication and creativity;
- Empower the edge, that is, give those closest to a problem the power to make more decisions;
- Harness the “power of us” by linking together all relevant stakeholders so that they jointly resolve the problems they face.

How should public security organisations be transformed in order to tackle the challenges and opportunities of the digital tsunami? What are the challenges to enhance the security tools that may defend the EU and the Member-States and millions of citizens?

Challenge 1 – Automate and master data analysis

7. One implication of the digital tsunami is that data monitoring and analysis will become much more automated.

This trend is starting to be seen in public security , but in areas such as financial services automated data analysis and pattern recognition are already well entrenched. By 2010, in many countries a high percentage of all equities trading is likely to be done using algorithmic trading.

Algorithmic trading uses mathematical models as a means of trading large blocks of shares quickly. The rules built into the model determine the optimal time for an order to be placed that will cause the least amount of impact on a security’s price. In addition to trading, large-scale brokers use algorithms internally to support statistical arbitrage trading, event arbitrage, and hedging against risk. Similarly, credit card companies rely on sophisticated programmes that use the purchasing patterns of individual customers to detect and flag up any purchases that are unusual and therefore potentially fraudulent.

Increasingly machines are able not just to analyse records of transactions, but also to analyse visual information as well. Current systems can already identify individuals by their gait or flag up particular types of image, e.g. unattended luggage or a person lying on the ground, apparently injured. Next generation systems are likely to be able to watch for, find and follow even more tightly defined objects, behaviour patterns or events.

These developments mean routine data monitoring and analysis will increasingly be handled by machines; the system will then flag up exceptions (unusual behaviour and anomalies) for human investigation. Some law enforcement agencies are already familiar with this approach in their suspicious transaction monitoring activities carried out by specialised agencies tasked with anti-money laundering activity. But this approach will need to be much more widely understood.

Emerging technologies are likely to push this trend forward in three main areas.

- First, rather than just monitoring a given data stream, these networked systems will start to respond to it intelligently. For example, if a suspicious object is detected on one video feed, the system will examine the object by zooming in on it with other nearby cameras or it might search for images of that object captured earlier on other cameras.
- Second, these systems will work across multiple data streams and multiple types of data stream. For example, if someone in an airport starts making a series of unusual mobile phone calls, the system might monitor the video streams of the areas where that person is more sensitively than it would normally. Or it might check passenger travel information to see if that person or someone related to them is due to arrive or depart in the next couple of hours.
- Finally, the interaction between these systems and humans will become more sophisticated. The system will know the current physical location of the staff it could alert and whether they are available. It will also have automated escalation procedures if alerts are not acted on or if their volume or type is likely to exceed the capacity of the staff to whom they would normally be directed.

Challenge 2 – Making Decision-making more distributed

8. Automation will help turn data into potentially useful information, but the most dramatic improvements in effectiveness will occur as public security organisations get better at using data.

Faced with the need for real-time decision-making in increasingly complicated situations, public sector organisations will look to empower frontline decision-makers.

In order to achieve this emerging technologies have to be used to ensure that the frontline has the same access to information as the centre and that ,as far as possible, co-ordination is achieved automatically and in real-time.

This will be made possible by the creation of communication and collaboration platforms that make the right information visible to the right person at the right time and the right place.

These new platforms will be enabled by

- Maximising the extent and quality of connectivity;
- Unifying communications;
- Automating communications.

9. Public security officers are likely to continue to use a wide range of different devices (radios, mobile phones, landlines, pagers, PCs, laptops, PDAs etc) but, unlike today, all these devices will interoperate seamlessly with each other.

The underlying network (or networks) that enable this will be secure, robust and able to handle large amounts of data with more and more of that data being video- and sensor-related. In the near future all key assets will be connected to the network so their location and operational status can be determined in real-time.

Similarly, CCTV cameras may be connected to the network so their output can be viewed from any other device on the network. For example, in an emergency situation a head of police, who may be at home or on the road, will be able to see a live video feed of the situation after a terrorist attack. The content will then follow him from device to device; so he will be able to monitor the same video stream on a screen in his car as he travels and on a mobile device when he leaves the car.

The rich array of communication possibilities that public security officials will be using in the near future will be presence-enabled. When an officer in the field needs to communicate urgently with a particular type of expert, the communications device he is using will show him all the potential channels he could use to contact an expert of this type and whether those particular experts are available at that moment and on which channel.

This “presence” information speeds decision-making and means that the best available people can be brought together quickly to analyse a problem or make a decision. The lengthy process of checking multiple channels in an often fruitless attempt to involve a

particular individual will be replaced by instant awareness of who is available and which channel is the most appropriate to contact them on.

This critical and little understood benefit of the trend towards unified communications is already having significant productivity effects for its advanced users in the private sector.

10. Collaboration itself is also likely to become automated with one-click collaboration opportunities built into work flows and event management. For example, if information about a new type of terrorist threat is entered into a database, this entry will automatically generate communications to a pre-defined list of stakeholders. Those stakeholders will then have one-click options to further distribute the notification or to link up on the most convenient channel with the person who made the original entry. Similarly, they will have access to click-to-collaborate options, which will enable them to set up instant audio or video conferences for group discussion of the notification if necessary.

These technologies are currently all available – all that remains is the more difficult set of tasks involved in deciding how to use them and manage them effectively and safely.

Challenge 3 – Transform Decision-support

11. Automation will increase the effectiveness of public security organisations by releasing people from mundane data-related tasks; but emerging technologies will also play a key role in transforming information into improved decision-making.

Emerging technologies are transforming our ability to pull together disparate sources of data and analysis and integrate them in a virtual, logical and meaningful way for users and systems. For example, open-standard data formats such as XML enable data and maps to be merged, so that information can be visually represented on a map and made available via multi-modal platforms to the desktop or to the mobile handheld devices.

Such services are becoming increasingly commonplace within distributed infrastructures and result in lower administrative cost, higher usability, and greater situational awareness.

These technologies allow all data streams (whether proprietary or open standards-based) to be transformed into one ubiquitous and common representation. This means that a mass of information can be pulled together and presented in whatever format is most useful to the decision-maker who needs that information.

Furthermore, the systems providing decision-support are also likely to become more intelligent, e.g. if an audio feed or an email mentions a particular type of explosive, the system might automatically offer information on the ten last times that explosive was used or on the location of the ten individuals who have a record of using such an explosive.

12.The increasing power of technology to pull together information in the era of Web 2.0 is already visible today in what are called “Mashups” - hybrid Web applications that combine data from two or more sources into a single tool.

Several websites “mash” publicly available online crime data with cartographic data from digital Maps. The interactive sites allows users to construct maps that display crimes by location, date, and type of crime.

These first-generation mash-ups are relatively simple, but in the near future public security organisations will be building portals that aggregate a huge range of data sources into personalized cockpits for different decision-makers.

The translation and transformation services that enable these mash-ups will increasingly be performed by the network itself rather than on a traditional client-server basis or as part of a specific application or application process.

This will mean that more of the processing will be done in the hardware at machine speed processing levels rather than by a software application. It will also be done in a distributed manner rather than at one central (potential choke) point within a data center. This network services approach increase the speed at which such operations can be performed and allows for the services to occur in a more distributed and efficient manner than centralized approaches.

The sophistication of these services will continue to evolve and additional services will be performed simultaneously with other processes. For example, in the financial services industry brokerage companies are analysing different types of transactions as they are occurring and re-prioritizing the transactions to ensure the highest priority and most important customers receive immediate attention. For example, in the past if an important customer called their broker out of hours and left a voicemail after other

voicemails had been left by less important customers, then when the broker looked at his voicemails either the more important customer would not be dealt with first or the broker would have to waste time going through all voicemails to find the most important one. Today, however, the best systems will assess incoming voicemails and emails and reprioritize the broker's inbox (crossing systems and translating as appropriate) so that the more important customer is at the front of the queue when the broker starts his workday. It is this mid-stream analytics and distributed network mining that allows for new services that traditional, more heavily siloed client-server approaches cannot offer.

13.These developments mean that IT systems will increasingly have automated policies that perform actions on decisions and/or destinations.

This will dramatically speed up decision-making and improve its quality. Compliance rule engines will aggregate many disparate policies into a virtual analysis capability that will allow the public security community to increase productivity and effectiveness. For example, if a police request for information after an incident triggers a massive response from the public, the response will be analysed and automatically prioritised or sorted by key word, type, or origin etc. The systems will also be able to highlight interesting patterns, e.g. repeated mentions of the same name or a large number of calls from a particular geographical area etc.

These application network services combined with mash-ups will be all the more important because the amount of potentially useful information generated by non-public security sources will accelerate dramatically in coming years. The implication is that safety and security professionals will have numerous sources of data, information, and analytics that they will need to integrate with their own internal data sources to increase their ability to monitor trends, prevent incidents, conduct investigations, organize responses, solicit assistance, and take action. Recent conflicts have shown that the media (and emerging unofficial information sources such as blogs) can sometimes post information faster than official organizations. It is, therefore, critical for public security organisations also to be able to tap into these sources of information.

14. In the near future second-generation mash-ups that integrate disparate and decentralized sources of data and analysis will form an integral part of day-to-day operations within public security organisations.

They will also seamlessly integrate communications and collaboration. Effectively mash-ups will create user-centric command centers, accessible via multiple modes of connectivity and devices. These user-centric command centers will provide services that reflect the operational needs and preferences of the user, replacing services that are constrained by the siloed nature of most existing application solutions.

One way of getting a glimpse of the potential of these multi-service and multi-use environments is to look at what MySpace, FaceBook, and other social network sites are offering consumers today. This type of personalised, real-time information cockpit is what public security officials can expect to see in the not too distant future if the appropriate measures are adopted.

III – Implications for the European Union and its Member-States

15. Information is the key to protecting the public and in an increasingly connected world, public security organisations will have access to almost limitless amounts of potentially useful information.

This is a challenge as well as an opportunity – public security organisations will need to transform the way they work if they are to master this data tsunami and turn it into intelligence that delivers safe, open and resilient communities.

Transformation will focus on a number of key dimensions. Public security organisations will need to automate more of their data monitoring and analysis; and they will need to build vastly more effective communication and collaboration platforms. Grasping the opportunities of a connected world will involve empowering local units and frontline staff to make more decisions. It will also involve automating the interaction between the increasing number of stakeholders (public and private) that have a role to play in protecting citizens from the many threats to public security we now face.

Within these new organisational models, the power of information will be unleashed in dramatic new ways. Decision-makers at the frontline and at the centre will be supported by tools that pull together the most relevant real-time information from a huge range of sources and present the results in the most appropriate, user-friendly

way. The key to effectiveness will be using technology to connect the capabilities of a multitude of stakeholders and ensure the right information gets to the right person in the form they are best able to use.

16. The vision set out in this paper has many implications for European Union countries individually and for the Union as a group.

Firstly, it highlights a number of areas that should be seen as priority areas for investment and experimentation. Member States should prioritize investment in innovative technologies that enable automated data analysis and improve real-time collaboration.

Research in these areas should be encouraged, ensuring that ideas can move quickly from a research context to practical implementation.

Secondly, the European Union should ensure that these activities are co-ordinated as efficiently as possible. Member States should be aware of any significant research activities or pilot programmes being undertaken in other Member States and the teams involved in these activities should be given opportunities to share information and collaborate.

Thirdly, Member States individually and collectively should take a “platform” approach to delivering public security. This involves moving beyond interoperability and focussing on a services-oriented approach, so that the outputs from different parts of the system can be shared (within and across organisations) and elements of the system can be easily and quickly reused.

Fourthly, Members States need to focus on building converged platforms – they need to move towards converged networks (or, where necessary, solutions that ensure all their networks can “talk” to each other) and they need to ensure all data streams are digital and capable of being mashed together.

More generally, a focus on building a platform means recognising that public security (particularly in Europe) will always involve a multiplicity of players and therefore the key issues are building systems that enable flexible, real-time collaboration between different organisations. Within this context, it also makes sense to encourage specialisation and sharing rather than an “I-must-have-my-own” mentality.

17. One way that European countries can ensure they grasp the opportunities described in this white paper is by embracing the Web 2.0 tools that support collaboration and innovation.

The aim should be to encourage virtual communities that enable innovators to network with each other and determine on a peer-to-peer basis the most promising options to explore. That was the methodology that allowed the European network of experts from the countries that took part in the «SISone4ALL» Project to achieve, on a very tight schedule, successful results that made the enlargement of the Schengen space possible.

They widely used the new digital environment to set a virtual help desk 24/7, early warning systems and a team of first-responders to critical situations.

Using Web 2.0 tools to create closed online communities is easy and will become easier and more effective. Another way collaborative innovation could be encouraged would be to use the new collaborative tools in the workings of the European Security Research and Innovation Forum to have a wide and deep discussion amongst experts of the projects that should win support and funding. New approaches of this kind are necessary (in this area as in others) if Europe is to lead the way. Fundamentally, Web 2.0 is about bringing together individuals across organisational and geographical boundaries, making the diversity of Europe an asset rather than a handicap.

18. Efforts should be made to launch an “European Security Tool-Pool” Initiative. In fact, some security capabilities require decades to be established and they will have a life cycle of twenty of thirty years. Maybe that is why when one discusses security capabilities there is a general tendency to consider big budgets.

Of course, expensive solutions will always be available in the market. But, a new environment is developing, in which we can act with technology and even tools we already have and at extremely low marginal costs. The whole cost of making the SISone4ALL clone available to the nine new Schengen members is not in the order of hundreds of millions of Euros – rather that of hundreds of thousands. It is up to us public authorities to ensure that we don’t spend more than we absolutely have too in acquiring the tools we need or even that we don’t spend money buying what we already have.

On the other hand, many European Countries are spending tax payer’s money developing security tools which already were developed elsewhere in the EU and could be adapted at a fraction of the price of building new ones. It is very likely that there are tools already developed for and by European Union institutions – e.g. for

monitoring the media or fighting fraud – which could be of great assistance for our security needs if only we knew we already have them. There are definitely huge budgetary gains to be made if public sector players pool together to negotiate the acquisition of software and content licences for our services.

It is time Europe considers the creation of a “pool of security tools”, so that we may use resources wisely – both human and financial ones; that our security professionals are equipped as soon as possible with the best possible means at the best possible price – preferably zero.

Under this vision, any Member State or Institution could place tools of potential value for others in this “European Security Tool-Pool”. We would jointly audit them and, if their broader usefulness was confirmed, then we should seek the fastest, cheapest way to ensure their dissemination – e.g. through linguistic adaptation or block licence acquisition. This kind of solutions would offer the additional advantage of easier interoperability of our security systems.