

Closing Speech – VIII International Atlantic Symposium ON C4I, 9 May 07

By Dr. José Magalhães

Allow me to thank the organizers of this International Atlantic Symposium for these two days of intense debate on one of the most crucial issues of our time. For the best and the worst reasons, debating “Intelligence in the Global Age” became urgent and the practical results of the debate you promoted may help make the difference between success and failure. ´

I did not hesitate to offer this initiative the strongest possible support. I did it for many good reasons, the first of them being my full agreement with the method chosen to organize the discussion. I sincerely share the belief that in our Global age only a very wide participation of leading experts both from military and internal security and intelligence communities can provide the good answers. Combined skills will certainly be more effective than a brilliant but isolated action that will run the risk of missing a relevant link or fact. Those who share with politicians the enormous responsibility of assessing threats and risks, setting strategies, mobilizing resources to provide security at the national, regional and global level should work together and get used to developing multiple ways of networking. I am also aware of the fact that the Armed Forces Communications and Electronics Association is a forum for the interaction between those who manufacture and commercialize technologies for defense or security purposes and those who have to use them professionally. That interaction is in itself positive and should lead to an accurate information on the best answers to problems that can be solved using a vast array of services and solutions. The new era in which the East-West dialogue against terrorism became possible is also an excellent opportunity to widen the choices we have to make and intensify competition in the global markets.

Those who had the chance to hear or read the contributions presented here by the highly qualified speakers will certainly be impressed and I am sure many decision-makers will benefit from your warnings, assessments and suggestions in the near future.

What has been learned from ongoing efforts in several points of our world confirms that the most dramatic challenges can not be met without excellent systems and methods of coordination and a very efficient functional operability between military units, police forces and intelligence structures .

Centuries ago a well known author wrote in his famous *The Art of War: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.* In all times technology has offered good help to establish subtle differences such as the ones Sun TZU established creating decisive tools for defense and security purposes. What is new in our time is the fact that the massification of certain tools and the global nature of some of them is offering criminals opportunities which are at the same time very affordable, easy to use, global, tremendously effective and difficult to control unless radical methods were to be used, in that case in clear breach of democratic rules. The good news is that Governments and law enforcing agencies can and use technology to protect our security, in a more sophisticated way, leaving the criminals behind and facing the new emerging threats to meet the security concerns of our fellow citizens.

That is the reason why the EU is now developing several initiatives, for instance, to detect dangerous materials, such as explosives, before terrorists use them. Our authorities will also increasingly share information to catch criminals and bring them to justice.

World experts also agree that traditional frontiers between “hard technologies”, mainly used for external security, and “soft technologies” used for internal security are vanishing.

Another obvious fact is that in order to fight against international terrorism and cross-border crime we need strong partnerships with third countries (namely USA and Russia). It is not just about high-tech: we need to build trust, compete and cooperate – all at the same time.

There are excellent reasons to do so.

Technology has brought us already many benefits, some of them less visible than others. One of the main achievements of our half a century of common history in Europe is the free flow of people in the Schengen area, open borders viable thanks to the now old 1st generation Schengen Information System soon to be replaced by a brand new SIS II, that unfortunately had to be rescheduled. Once again, here is Technology helping us against terrorists, smugglers of human beings, drugs traffickers and other criminals.

But even here times are changing: innovation is not subject to any monopoly, good projects can be led by any State with appropriate creativity and even modest resources. The Portuguese Republic offered an example of seizing the opportunities created by this new open environment. In order to allow the new Member States to join that space, we promoted a high-tech initiative we called "SisOne4all" that will hopefully allow States that joined the Union in 2004 to have their borders lifted. The Commission, the Council and all other key partners are doing the best to make this happen in December this year. It will be a very concrete achievement, very practical and extremely visible, allowing our citizens to understand and value their European citizenship.

Building an European Freedom, Security and Justice policy, a vast space more effective, more efficient, more coherent is the challenge we have to cope with. Certainly, the rhythm is slower than it should be, the levels of coordination are insufficient, we keep being separated by different economic interests or disagreements caused by mere political internal considerations. Cultural differences also continue to be too relevant in important areas. We know not what the future will bring in what comes to the European Constitution, but we do know what went wrong in the past and many of the reasons why negative events occurred. The risk of keeping things as they still are is too high. So, we need decisions. Now public authorities try to take the best decisions concerning security, while considering global competitiveness of European companies with respect to the Lisbon objectives. It is not an easy task in a globalized world where no protectionism should prevail. A balance has to be achieved.

Let me offer an example: in 2005, when we had to make choices to guarantee that the new Portuguese Electronic Passport could be issued in due time (and time was running out fast!) we fought to achieve that kind of balance. Turn-key solutions were politely refused. We decided to combine some of the best technologies we bought without hesitation in the world market, some of them produced by Portuguese companies. That is the way forward.

It has justly been said that “only with common security solutions will Europe be able to play its expected international role, as producer of security and not only as consumer at the expenses of our Atlantic allies”. And do agree and I see lots of new opportunities that should be seized by governments and commercial partners. I’ll mention a few of them: - we are drafting a common European legal framework for the use of biometrics in visas, passports, residence permits and identity documents - We are promoting increased and coordinated cooperation between Member States and neighbouring countries on border control to develop more integrated border management, including maritime surveillance systems - The Border agency FRONTEX will be significantly reinforced - Joint teams of border policing specialists will be deployed to face special situations of attempted illegal entry and at all larger border checkpoints (the so called “RABIT”). They will need equipment. Rapid intervention tasks need advanced technologies and innovative systems also compliant with full respect for human rights.

People will ask: where is the money for such an ambition?

Vice-President Frattini has recently offered a good reply:

“We have new finances available in the “Security and safeguarding liberties” Programme to sustain our policy objectives” (including the ones related to the Directive Proposal concerning the protection of European Critical Infrastructures). “We now have a larger budget for research, policy and applications at European level”.

“[The EU has] money available through the European Border Fund to help Member States invest in new applications and systems in this area: 1.8 billion euros for the period 2007-2013. Seven new Member States have

made use of the resources of the Schengen Facility: 1 billion euros for the period 2004-2006 but the use of this money is still ongoing. Bulgaria and Romania have, in the period 2007-2009, funds from the Transition Facility, an important part of which has to be spent on border management. The effort of solidarity between Member States that the EU is showing in this area in very concrete terms is impressive and needs to be recognized”

That solidarity is also a great challenge for the industry.

Another challenge will be the result of the ongoing change of the rules of the “information game”. In order to make law enforcement and security agencies share their information with each other, the EU is working on implementing the ‘principle of availability’ as set out in The Hague Programme. More recently we are working – together with the German EU Presidency – to have the provisions of the Prüm Treaty transferred into the EU legal framework. That should draw our attention to the fundamental need to guarantee wide use of secure transmission of information and the urgent need to protect our networks against attacks and vulnerabilities which presently exist. Organizations based on the circulation of paper or traditional communications are now using the Internet in a dangerous unprotected way, without using cryptographic tools and secure procedures. We have to adjust our agenda to the European agenda. In DG JLS several task forces are already working, with contribution from public and private stakeholders, on fraud in non-cash payments, explosives, detection technologies, critical infrastructures. Combining efforts of all departments involved, we have to help link all these activities, set a global vision and common political strategy and then apply those options at our national level. And we need to be active members of the future European Security Research and Innovation Forum.

That is the way forward. Thank you for your help in such a relevant effort and once again congratulations for this initiative.