

## **1ST PUBLIC-PRIVATE SECURITY CONFERENCE**

**BERLIN – 27. MAI 2008 – ILA**

**SPEECH BY DR. MARKUS HELLENTHAL**

**CHIEF EXECUTIVE OFFICER THALES DEUTSCHLAND**

**"ENHANCING RESILIENCE THROUGH TECHNOLOGY AND INNOVATION BASED ON  
A BETTER COLLABORATION BETWEEN STATE AND INDUSTRY."**

Ladies and Gentlemen,

Let me first express how honoured I am to have the opportunity to speak to you at the occasion of this distinguished PUBLIC-PRIVATE SECURITY CONFERENCE.

Providing security by a state or any given private organization in charge of risk-relevant processes and installations are first of all dependent on a comprehensive and in-depth understanding of both: the specific vulnerabilities and the specific threats. Based on such an adequate and always current insight of vulnerabilities and threat exposures, it should be evident to implement necessary, comprehensive and appropriate mitigation and response measures. This will lead to the desired enhanced resilience of our societies.

Based on applied risk management, the areas of vulnerability rightly drive the core missions of our diverse public and private security organizations. These organizations are equally challenged when it comes to providing security to our societies on a day-to-day basis. In view of their core missions, technology and innovation have to meet the essential requirements of security missions and, by doing so, improve significantly the relevant capabilities of the respective security organisations. Only then they will have an impact on the level of security in our societies at large.

Without such significant improvements it seems evident to me that our societies will continue to increasingly suffer from terrorism and organised crime, but not to forget the many other criminal activities as well as natural and man made disasters, which more and more seem to burden our modern societies.

Therefore security research and innovation have rightfully achieved paramount importance today. This aims in particular at an improved insight into the comprehensive spectrum of vulnerabilities, threats and adequate mitigation and response capabilities. The required mitigation and response capabilities go far beyond pure technologies. This is one of the two main messages

- Of the European Security Research Advisory Board (ESRAB), where I was chairman,
- Of the current European Security Research and Innovation Forum (ESRIF), where I was member and rapporteur of the Critical Infrastructure Working Group until very recently, and
- Of the European Organisation of Security (EOS), where I was one of the founders and the first chairman until very recently, as well.

The other important message of these security research and innovation activities on European as well as German national level is: It will not work without a sincere and constructive day-to-day collaboration between state and industry. This is also one of the main reasons, why in security research and innovation in Europe and elsewhere the linkage between "demand" and "supply" is rightly stressed as an essential factor in achieving success in security affairs.

But it is not just a relationship between "suppliers" and "buyers" or "requesters". We need to go much further and understand provisioning of security for our societies as a common endeavour of all those who are in charge or responsible for critical or risk-relevant processes and installations. Taking into account that over 80 % of all critical infrastructures belong to private operators, one cannot oversee the fact that provisioning of security has to be tackled as a common challenge.

Therefore the theme of my intervention is: **Enhancing resilience through technology and innovation based on a better collaboration between state and industry.**

Such an approach will help us to strengthen our superior interest in safeguarding freedom, liberty, and human rights for those who live their lives as they wish within the law.

---

## Ladies and Gentlemen,

Today, the world is displaying a single, global reality, which is – regarding security issues – manifesting itself in disguise of internationally operating ruthless, murderous terrorists and criminals. In particular terrorist are a serious threat to all of us. Their persistent attacks, although still limited to specific geographical areas, individual countries or political and economic institutions and enterprises, affect the entire international community and cause previously unknown damages and casualties.

In addition to the predominant fight against terrorism, we are facing other severe security threats, in particular organized crime, often conducted across state borders in what can be called common and unified criminal geographic areas.

These threats are no longer singular, stand-alone ones, which can be tackled separately and consecutively. Countries and enterprises are on the contrary challenged with tremendous damage and loss potentials, which grow out of patterns of interdependence, which neither stop at the borders of nations nor of traditional organizational charts of security organizations. This is particularly true in countries with highly fragmented security organizations as opposed to the typical national military organisation.

Consequently, these threats have globally changed the perception and the understanding of security and the importance of resilience of modern societies as well as of enterprises and even individuals. We must ensure our resources, effectuate our capabilities, and improve our legislation in order to support our common endeavour to defend the shared values of our countries from terror and other significant crimes. Terrorists are criminals, whose victims come from all walks of life, communities and religious backgrounds. Terrorists therefore attack the values that are shared by all law-abiding citizens. Together, let us ensure that their evil ambitions are never turned into reality. Only through our unity will terrorists ultimately be defeated.

In addition, and as a strong support to all people who live their lives as they wish, within the law, efficient and effective security measures have to be applied. These measures need to

tackle terrorist and other criminal threats appropriately as well as day-to-day capital and minor criminality or disorder caused by natural or man made disasters. This development requires societies and enterprises to improve their resilience against such diverse threats.

At the same time, security providers need to continuously advance their capabilities, designed seamless and comprehensive enough to allow for taking the necessary and appropriate actions. Security providers in this respect are either governmental organizations like law-enforcement authorities, but also fire brigades, civil defence organizations, search & rescue forces, or – in the frame of civil-military collaboration - military resources if need be, in particular with regard to logistical support, heavy vehicles or construction, engineering, decontamination and similar capabilities, which are otherwise attached and attributed to the military, or otherwise private security companies or operators of critical infrastructures like airports or industry sites.

There is another dimension, which is also of utmost importance, and which cannot be tackled by a traditional silo approach. This is the interdependencies, or rather integrative aspects of several terrorist and criminal activities. An example for this growing phenomenon is the prominent involvement of terrorist and organized crime organizations in the production and distribution of drugs and their correlation with all kinds of enabling criminal activities and shadow facilitators, like money-launderers, weapon and alien smugglers, counterfeiters, etc. This also means that terror and organized crime organizations get more and more independent from state support or subsidies and become businesses of their own, following their own agendas, which makes them even more dangerous for the community of free and democratic societies.

In essence, whether we are confronted with symmetric or asymmetric criminal or terrorist threats, our capability to respond depends essentially upon our ability to take the necessary actions, such as:

- To protect people and territories from terrorist and other criminal attacks as well as from man made or natural disasters as much as possible
- To detect, deter, and pursue terrorists and other criminals and their supporters
- To prepare for the consequences of an attack
- To take the necessary decisions in case of alarms and emergencies
- To respond adequately in case of attacks or other disruptive events

It is essential that such actions have to rely upon adequate risk management procedures and techniques to anticipate, detect, identify, analyze, and mitigate relevant threats appropriately, decisively and effectively.

The basis of this has to be a thorough analysis of national or enterprise threat and risk scenarios, which need to be documented and continuously updated. In particular the vulnerability of nations and enterprises towards 'unplanned disruptive challenges' necessitates improved risk assessment capabilities and response planning.

Security, in particular counter-terrorism science and innovation draw on a wide spectrum of research areas, for example: detecting, mitigating, and understanding the properties of chemical, biological, radiological and nuclear (CBRN) material and explosives. Another very important dimension is social and behavioural science. This will potentially bring a new dimension of profiling, which is basically one of the core policing tools already today, although not technically enabled as it could be.

---

## Ladies and Gentlemen,

In my experience as former law enforcement officer working within several security organisations and today as a provider of latest security technologies, solutions and services, but also as an advisor on security affairs, I believe it is essential to think in terms of vulnerabilities and missions. Security organisations typically reflect the variety of vulnerabilities and are typically structured around respective missions. So, if we do not structure our thinking along these lines, we might have lesser chances to reach the mindsets of the security organisations and their personnel. It should be our goal to effectively support them in their desire to improve their operational capabilities, which is ultimately to improve the effect of their operations on countering terrorism, other organised crime, or any other relevant security burden of our modern societies.

The effective counter-management of threat potential and crisis is a highly complex task. The complexity stems from the need to simultaneously and collaboratively manage major 'areas of vulnerability' for the security of our societies and enterprises.

One of the currently most pressing areas of security concern in many countries and regions around the globe is the necessity of protecting Critical Infrastructures. This requires adequate protection of

- **Critical industry and other sensitive sites, facilities and infrastructures, in particular water, oil and gas plants - with their off-shore platforms -, chemical industries, IT data centres and hubs plus utility distribution networks for oil, gas, water, and power, voice- and data-transmission.** A very important part of the security of critical infrastructure is the security of the Information and Communication Technology (ICT), which is at the heart of modern societies and economies. Without properly functioning and secure ICT, societies and economies cannot function.
- After the attacks of suitcase bombers in Koblenz and Dresden and explosions in ground transportation installations in London and Madrid it has become evident that also managing the security of **mass aggregation of people, typically in metropolitan areas and cities, and mass transportation and their hubs (in particular airports and train stations) as well as whole supply chains**, are another incredibly important area of security concern.

Over 80% of these critical infrastructures are in private possession or operation. Therefore applying necessary prevention and protection measures is often not an easy undertaking. In fact private businesses are much more driven by short-sighted needs, and security measures are often not envisaged as qualified enough in this respect.

Consequently, success will be based upon an integrated and utmost cost efficient management of infrastructure protection, most of the time including access control for people and goods. Here, the objective is to ensure an adequate level of security while at the same time maintaining operational feasibility and economic operability. In particular in the transportation and supply chain areas, the processes of embarkation and disembarkation are typically conducted under very high time pressure. Therefore facilitation of transportation flows is of highest importance to the users as well as to the operators, while the private as well as public security authorities seek the needle in the hay stack and are typically perceived as the number one obstacle within a transportation process, if they involve themselves.

On the other hand, the criticality stems from the fact that such an environment is not only interesting business wise in the normal sense because of the many potential customers or network effects such mass aggregation of people can provide. As terrorists and other criminals

follow the same laws of physics, sociology, and economics, people are significantly endangered particularly where many people live and work in one and the same place.

In case the unexpected happens, which we can be sure that it will, the deterrence of threats as well as the mitigation of damages depends on the ability to respond swiftly and with the most appropriate and sufficient means. Therefore comprehensive and adequate Civil Protection, Emergency Response and Crisis Management in particular in case of natural and man made disasters and catastrophes are essential. Public, but also private security organisations have to be prepared to react efficiently and effectively in any given emergency event or crisis and to provide the necessary protection and relief support for the citizens.

---

## Ladies and Gentlemen,

I believe it has become evident that in the case of Critical Infrastructure Protection in particular, not only can one state alone not be successful in mitigating threats. States and enterprises have to work together to have at least a chance to mitigate risks and counteract threats and attacks in an appropriate and meaningful fashion.

Therefore, security work is all about a high level of situational awareness and warning systems, of preparedness to execute emergency action plans and to implement rapid crisis-response measures, and of seamless, cross-border collaboration of all involved public and private security forces.

This leads us to the question, which capabilities are required, to enable security organisations to adequately respond to these challenges and to take the necessary steps to fight terrorism and other forms of organised crime as well as natural and man made disasters.

Throughout the military sphere, countries have been able – at least to a significant extend - to respond to new challenges in the defence world. These adjustments have been made rather swiftly by adequately transforming national armies as well as military alliances. By this a new dimension of cooperation, applicability and effectiveness on the one hand and a capability-related approach regarding technological as well as operational means on the other hand have been ensured, to come up with, in the end, truly effect based operations.

Slowly but steadily countries are currently transferring this approach to the new civil security requirements, knowing that this is a more difficult undertaking since sensitive sovereignty

rights, which lie at the foundation of the state-citizen relationship, are affected. In addition, in most if not all countries, the number of public and private security organizations, including often military organisations, involved in civil security is diverse and fragmented.

Therefore, a capability-related approach, similar to the one the defence sector has been entertaining for decades, has to be implemented in accordance with the described persistent, manifold vulnerabilities, to also enhance the efficiency and effectiveness of security organisations. In this regard, relevant state-of-the-art, innovative, and inter-operable supporting technologies are of major significance as an enabler for improved capabilities or resilience. This will lead to a better prevention, deterrence, preparedness, as well as adequate responses to terrorist and other criminal threats.

It goes without elaborating here too much that, as we have learnt from the military side, such a comprehensive transformation program needs a significant, broad and pro-active change management approach, not only for the people inside the security organisations, being involved in the transformation process, but also within the societies at large. This will be tremendously important if we want to successfully introduce new and more effective capabilities and overcome existing hurdles of acceptance and understanding, while continuing safeguarding freedom and liberty.

---

## Ladies and Gentlemen,

As threats as well as possible solutions become more and more complex, those who are responsible for providing necessary security precautions will tend to ask more and more for new or enhanced security capabilities and no longer for specific individual or isolated technology components. More and more pieces of technology will therefore become part of systems, or "System of Systems" also in the civil security domain. In order to bring the full value of a chosen set of technologies to the end users in a way that the latter are able to leverage such new capabilities as desired and expected, sophisticated skills are required on the side of the "Security Capability Enabler".

In particular, a capable "Security Capability Enabler" needs to master the relevant technologies (i.e. to understand their functionalities and specifications) as well as their respective interdependencies among each other as with the skills required on the end user side (i.e. processes and human skills) to tackle them. In addition, the "Security Capability Enabler"

needs to have strong skills in the domains of system architecture, system integration, program and project management, sourcing and vendor management, financial controlling, and, last but not least, quality assurance.

But most importantly, he needs to be fully aware ("live, breath, feel and think end user") of the end users security operational requirements and to be able to translate between these and systems requirements in order to match both to the satisfaction of the end users. Only then the "Security Capability Enabler" will truly stimulate science, technology research, and innovation for the benefit of the end users and will ultimately become his long-term partner. Concept design and experimentation as well as demonstration and simulation capabilities will therefore play a mayor role in the process of implementing new and more sophisticated capabilities. This is in particular true in view of the many diverse actors who need to be involved in modern threat prevention and counter-measures.

By this we might be able to enhance resilience of our societies through technology and innovation, but only in a very collaborative manor between state and industry.

---

**Ladies and Gentlemen!**

Thank you very much for your kind attention.