**Optimizing Resource Allocation: Lessons Learnt by Industry**

**Speech on behalf of Huawei Technologies at the SDA Conference**
**After Chicago: Re-evaluating NATO's priorities / Section 2: Smart Defence**
**Brussels, 25th May 2012**

Ministers, Excellency's, Ladies and Gentlemen,

I am delighted to be invited this morning and to speak in front of such an impressive audience. Thank you so much for your kind attention.

In the context of NATO's "Smart Defence" or EU's "Pooling & Sharing" initiatives, I have been asked to share with you some insights on lessons learnt by the industry. This is when we strive to optimize the allocation of our always scarce resources in order to optimize the economic output for the advantage of all stake holders, be it customers, employees, shareholders and the society at large.

Before going in medias res, I owe you a brief explanation why I was chosen for doing that.

The first reason is probably my professional background:

- Over the first 14 years in my career I was a German public servant and police enforcement officer. In my last position I was in charge of the German border guards and aviation security, equivalent to a one star general.
- After that I have spent 15 years in the ICT industry focussing mostly on the defence and security sector, first as a Partner with Accenture and then as SVP with EADS and finally Thales.
- In parallel, since 10 years, I am contributing to the European and German security research agendas, having been the chairman of ESRAB and the co-founder of the European Security Organization, just to name two relevant activities.
- Since February of this year I am consulting international companies and the German Ministry of Economy and Technology on business strategy, marketing and security policies.

In all of my functions I was deeply involved in major change and consolidation programs. From three times reorganizing the German border guards as a consequence of the German unification and the European enlargement processes, till integrating the fragmented structure

Office: Udostrasse 49 | 56154 Boppard | Germany | Tel +49 6742 899 146 | Fax +49 6742 921 342
Mobile + 49 172 82 83 522 | E-Mail email@markus-hellenthal.de | Web www.markus-hellenthal.de www.resultsconsulting.de

of Thales in Germany with previously 12 independent business entities into one company. Some of the experiences I am happy to share with you.

The second motivation is the astounding development of Huawei in the ICT market and the relevance of advanced, All-IP capabilities for the advantage of private and governmental organizations, making them more successful with significant productivity gains in their own business activities.

Established only 25 years ago, Huawei is a leading global solution provider of information and communication technologies and electronic communication devices. Still, Huawei is not so much known to many of us. It is one of the few private Chinese companies, owned entirely by its employees as almost 70.000 of them have bought a stake in the company. The company employs over 140.000 people in 150 countries worldwide. Also in the European Union Huawei is an important employer with over 7,000 employees, mostly European nationals. Huawei foresees this steadily growing number to be doubled in the period ahead.

Huawei's success strategy relies on investing significantly in research, technology and development and has established global R&D centres in several EU cities, including Paris, Milan, Munich and Stockholm. Huawei plans to underpin its commitment to Europe by further investments in, and contributions to, the EU and its future ICT capabilities.

Huawei has established end-to-end advantages in the ICT infrastructure, application & software, devices and professional services. Huawei has gained a leading position in the All-IP convergence age. Huawei products and solutions have been deployed in over 100 countries and serve 45 of the world's top 50 telecom operators and as of the end of 2011, Huawei's wireless networks products and solutions had been deployed by more than 500 carriers worldwide. The flow of electronic communication of one third of the world's population is supported by Huawei technologies.

Based on its success, Huawei's vision is very ambitious: Huawei strives to help bridging the digital divide and giving people the opportunity to join the information age, regardless of where they are situated or from which geographic origin they might be.

In order to tackle increasing environmental challenges, Huawei has developed and deployed a wide range of green solutions that enable customers to reduce power consumption and carbon emission, contributing to the sustainable development of the social economy and the environment at large.

Yet on another page I know of course that there are questions related to IT security. IT and IT security are essential prerequisites for optimizing the allocation of resources of all kinds. This is because a lot of ways how to do that efficiently is dependent on IT enabled capabilities and processes, which boost efficiency and collaboration across organizational and physical boundaries. I will come back on this specific topic in a minute.

Before that I would like to briefly describe my understanding of the issues related to NATO's "Smart Defence" or EU's "Pooling & Sharing" initiatives.

We all know that the budgets of EU and NATO member states are heavily constrained by financial and economic stress. As a consequence, the defence budgets have come under pressure. Although this is not a fundamentally new observation, the size of it has reached such a level that no one can shy away anymore from the consequences, as the German defence state secretary Stéphane Beemelmans has put it. In addition, international challenges for piece enforcing and piece keeping missions are certainly not going to diminish in the foreseeable future, while at the same time the level of expectations towards European engagements will increase. As a consequence, the UK defence minister Hammond stated in Berlin a few weeks ago in April that the economic crisis turns out to be one of the biggest security threats, if states do not find a new balance between possible economic input and realistically required military output. In an article published last weekend, the chairman of the NATO Parliamentary Council and member of the German Bundestag, Karl Lamers, has seconded this.

Only a week ago I attended the annual conference of one of the most important dialogue platforms in Germany between the defence organization and the respective industry. It is the German defence technology association DWT. The key note speaker was the Chief Executive of EDA, Mrs Claude-France Arnould. She referred to the history of her agency and how over the last two decades she and her colleagues are pushing for what we call today "Smart Defence" or "Pooling & Sharing". And, as a matter of fact, many small projects have been undertaken, but still, a major breakthrough has not yet occurred. The big flagship programs in this context, like air-to-air-fuelling or the like, are still to be seen.

Therefore the intention seems to be to make "Smart Defence" a strategy of the future by trying to define new capabilities which in the time to come could be jointly leveraged and or shared. Although this is understandable, one could also argue to start immediately by introducing existing capabilities as central and shared military functions or capabilities based on

SLA and cost sharing mechanism at least for those EU and NATO member states that are willing to do that. We know that there are some initiatives in that direction already going on.

Also in the industry we observe from time to time divergences between economic framework conditions and capabilities at hands or required. This situation is typically associated with activities phrased “consolidation” or by such tools like outsourcing. The effects are sometimes shrinking organizations and diminishing power in the market. This sometimes leads into a vicious circle. The longer these cycles turn, the more painful recovery can get.

I don’t believe this being the best strategy. To some extend it is a normal necessity that every 5 to 10 years organizations have to revisit their strategy. They need to redefine where they come from, where they strive to, which capabilities they need for that and can afford and, finally, how best to orchestrate all human as well as material and nonmaterial resources. As there are many interdependencies among these resources and with the market outside, this journey is always an iterative process. Another important element are available or new technical means which provide or enable new capabilities and can change the way how the organization operates. ICT is one of the most relevant technical means of this kind which has a huge impact on all aspects of design, development, production, delivery and service of products and solutions, including the delivery of military and public security powers.

Of course, prerequisite for such an approach are always transparent, standard-compliant, interoperable and interchangeable ICT products and solutions, including respective applications and management procedures. It is in my opinion just not acceptable as it has been done when introducing Tetra by the Schengen Treaty and afterwards it came out that the companies delivering Tetra into the various Schengen or EU member states did not provide the requested real interoperability. I know from Huawei that they are focussing a lot on such transparent, standard-compliant, interoperable and interchangeable equipment. Necessary resilience in our countries is calling for such precautions anyhow.

Therefore my experience suggests that it is better to look for productivity gains which provide advantages to as many players as possible as opposed to keeping inefficient structures and production methods only for the sake of short-term comfort. Many of these productivity gains come from shared services or central functions which are made available for all players in the respective organization. Such shared services and central functions are not confined by the conventional functions like Finance, HR, Procurement, IT, Marketing or Legal. Today, many organizations also include previously separated operational units like sales, research and technology, engineering and development, project purchasing, operational IT and finally

logistics and services. In my view there is no principal boundary or obstacles. It all boils down to the question, how best from an economical perspective, the organization is able to deliver its value add to the customer.

How to do that can of course be a severe question. Is it best to leverage in-house capabilities or go for outsourcing? And if in-house, which one doing it today should be chosen?

At the end of the day it is an equation of how best to leverage economy of scale while entertaining the core differentiating value in view of the markets or customers. For that we in the industry define the core values we can effectively deliver to our customer. In military terms you can call this the desired military effect. Based on that we have to define the capabilities we need to achieve the desired effects. Then we segregate between those capabilities which are necessary to be owned and managed by the company and such which only need to be secured. The main decision criteria to be applied are: What helps the company to differentiate from competition in front of the customer? What ensures reliability of expected delivery? What provides the best cost effectiveness? What supports best the mid and long term sustainability of the business model? And not all answers are the same at any time and under any circumstances.

Based on these decisions efficient production and delivery processes for capabilities sourced from the inside and procurement and delivery processes for capabilities sourced from the outside have to be created and supported by stringent SLA. And, finally, a secure supply chain, comprised of inside and outside supplies, has to be established.

If one does all this, the notion of central and shared services as well as integrated production and delivery capabilities will be very normal and will demonstrate quickly significant returns on investment.

If in NATO and EU the question is, how the EU Common Security and Defence Policy be further integrated while making available more effective capabilities in and by the EU, the respective question in the industry is, how - by leveraging shared services and central functions - the economic equation between input and return can be improved. Or, as the former U.S. Secretary of Defense Robert Gates has nicely put it: “Get more bang for the buck.”

In view of the existing threats and significant budget retrains, efficient and intelligent utilization of resources is called for, and should not be sacrificed on the altar of allegedly sacred

cows. If we continue to do so, it will be harder in the future to explain to taxpayers on the one side and to peoples in need of robust help on the other side, why.

It all boils down to trust; also in this respect in my experience there is no fundamental difference between a widely deployed industrial organization and states. Without trust in the reliable delivery of central and shared functions or capabilities as well as trust that joint actions do not have negative implications on the other levels or entities but are seen as jointly justifiable, no alliance or conglomerate will work.

A final remark on IT security: We all know that cyber security is a global challenge. It requires all governments, operators, suppliers and industry experts to work together. It is basically the same as with land, sea and air transport. Being open, transparent and cooperative and applying open standards and interoperability is the most effective way to resolve security problems. This is true for IT as with other transportation means. Huawei is committed to these requirements.

Huawei has established a Global Cyber Security Committee (GCSC) as the company's highest cyber security management organization. This organization is run by John Suffolk, previously the CIO & CISO of the UK government and before that the CEO of the UK Criminal Justice Transformation Agency. John reports directly to the CEO of Huawei and is responsible for developing overall security strategies as well as the planning, management, and supervision of all departments involved, such as R&D, supply chain, marketing, sales, engineering delivery, and technical service with regards to IT security. This end-to-end approach underpins Huawei's commitment to IT security; the company treats it as a built-in process, not as a bolt-on feature.

Huawei has conducted security tests and audits in many countries, and it has established Cyber Security Offices in several of them, including the US, the UK, India, and France. At present, the centre in the UK has passed the inspection of the British government and is operating properly with well-structured resources. It is open, readily accessible and transparent to the UK government and has won high acclaim from governmental security organizations, operators, partners and the media.

Thank you very much for your kind attention.