CESTUDEC-CENTRO STUDI STRATEGICI CARLO DE STOFORIS

Making Security Smart

RALPH THIELE

2012

CESTUDEC

Making Security Smart

1. A Turning Point

NATO Secretary General Anders Fogh Rasmussen introduced Smart Defence as a concept at the 2011 Munich Security Conference. The idea is simple. Smart Defence is about nations building greater security with more collaboration and more coherence. In a couple of weeks President Obama will welcome Allied Heads of State and Government at the NATO Summit in Chicago. A key deliverable for Chicago relates to Smart Defence.

The dynamically changing global security environment has been a key parameter for the reorientation of security forces and security business in the past years. The financial crisis has put public budgets under severe pressure. Public spending has been cut. Defence budgets have been cut. Few countries spend enough on defence capabilities. At the same time the crisis has led to the withdrawal of those resources that have enabled Ministries to conceal inefficiencies in the security sector. This situation will continue and escalate rather than the reverse.. The financial crisis poses a serious risk to national and transatlantic security and to the security business. It also offers opportunities as shrinking budgets increase the pressure on key actors to cooperate and seek innovative ways to improve the security situation.

Senior NATO officials have recently looked to multinational cooperation as a way of maintaining and even enhancing military capabilities in times of austerity. Role specialization, pooling and sharing of capabilities and multinational procurement programs have been tried before with some success, but with many more have proved disappointing, often with more costly results.

One prevalent feature of the majority of multinational collaborative defence programs has been the focus on large, expensive and platform-based systems, such as the Eurofighter. Many decision makers have been paralyzed by managing huge platform programmes that governments and private actors no longer need - in terms of quantity and quality - nor are able to afford. Such programs, conceived during the Cold War, have arguably outlived their operational purpose. Their continuation is to a large extent fuelled by considerations of sunk costs and the desire to preserve jobs and international cooperation as well as contractual obligations. In many cases, cancelling a programme will incur such high penalty-fees for the government that it makes more sense to continue it. The potential of developing synergetic systems has been ignored. This has led to institutionally and conceptually fragmented capabilities that do not meet existing security challenges. In fact, institutional and conceptual coherence is at the core of required systemic capabilities – nationally, internationally, as well as in private and governmental business.

2. The Challenge

Recent operations have driven the shift towards more expeditionary forces. The transformational dimensions of *network-enabled capabilities*, the *effects-based approach to operations* and the *comprehensive approach to security* will drive developments over the next decade. Addressing new challenges such as cyber, ballistic missile defence, and space will require allocation of additional defence resources. All these initiatives will have to be found within the given financial framework and will gradually consume a greater proportion of ever more scarce resources. While long-term savings might follow ongoing reforms, first of all it will cost money in order to save the same.

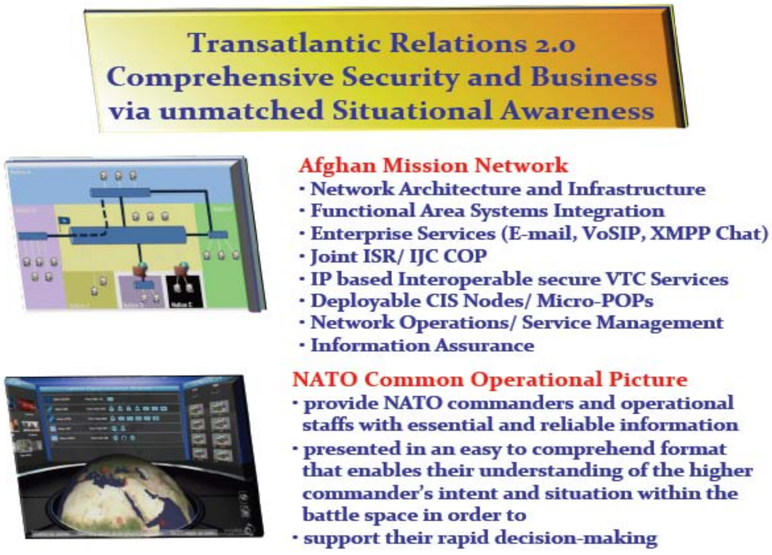
Working together in NATO will become increasingly difficult when the capability gap across the Atlantic keeps on growing while the ability to operate together remains underdeveloped. These deficiencies impact directly on transatlantic political cohesion. Consequently, future collaborative programs are the key to success. These will be evaluated rigorously on their ability to deliver real cost savings and produce significant operational capabilities that are developed independently. Civilian and military security forces as well as the security business need to come up with meaningful contributions to a comprehensive national and transnational security system while taking far-sighted, cross-government and international action in cooperation with all relevant stakeholders including government institutions and private business.

3. The Vision

Transferring these challenges into a viable, multinational security capability that also pays off on national and global markets is the core of meeting complex security requirements and succeeding on the national and international markets. Nations should focus their security contributions on plug-to-operate capabilities that have the capacity to generate an easy to comprehend, efficient and effective Situational Awareness Environment (SAE). Via architecture, processes, and tools it could provide for informed, responsive decisions in an interagency and international security environment that includes the services of government actors and private business.

Politically this approach requires serious leadership. Industrially it builds on the concept of *Lead System Integration* as an important and viable operating model with rapidly increasing success on global markets. This vision is reinforced by two recent important developments in NATO:

- With the **Afghan Mission Network** for the first time in Alliance history a common C4ISR network has been established for all ISAF forces and operations consisting of the ISAF-Secret network as the core with national extensions. In times of austerity cuts these national extensions have an enormous shaping impact on national C4ISR structures.
- The Afghan Mission Network supports a **NATO Common Operational Picture.** Soon it will provide NATO commanders and operational staffs with essential and reliable information presented that enables their understanding of comprehensive security environments in order to improving situational awareness and supporting rapid decision-making.



Transatlantic Relations 2.0
Comprehensive Security and Business
via unmatched Situational Awareness

Afghan Mission Network
- Network Architecture and Infrastructure
- Functional Area Systems Integration
- Enterprise Services (E-mail, VoSIP, XMPP Chat)
- Joint ISR/ IJC COP
- IP based Interoperable secure VTC Services
- Deployable CIS Nodes/ Micro-POPs
- Network Operations/ Service Management
- Information Assurance

NATO Common Operational Picture
- provide NATO commanders and operational staffs with essential and reliable information
- presented in an easy to comprehend format that enables their understanding of the higher commander's intent and situation within the battle space in order to
- support their rapid decision-making

Both developments will serve in a global scale as **best-practice-examples** for security forces and security business. Consequently they will shape both requirements and markets.

4. The Benefits

Instead of huge platform programmes a **Situational Awareness Environment Program** would allow for a plenitude of national and international security, research and business initiatives and foster a broad participation of large, medium-sized and even small-sized companies in a transatlantic collaborative approach. It focuses on optimization at the systems level versus the platform level. It does not favour any particular technology or platform. It enables the tradeing of risk, cost and capability, and it opens competition at multiple work levels, giving small and large companies from around the world equal opportunities to compete.

The Situational Awareness Environment would provide the framework for a multitude of industries that could enable the SAE with services and applications mastering all kinds of information, knowledge, evaluation etc. Sensors, effectors and other platforms and actors could be pluged in. The SAE could be scaled and tailored to individual/national requirements. It would support by its structure, processes and services, national and international security requirements and foster integrative, global business.

Creating greater coherence within NATO through situational awareness requires closer links with the private sector. In the past, military Research and Development put defence at the cutting edge of technology, with the civilian sector eventually taking advantage of those innovations. Today, in many areas, the situation has reversed. Industry has a wealth of expertise, including cyber defence, fuel cell energy and light logistics. We must find better ways through public-private partnerships to explore the military potential of emerging technologies, and involve industry sooner and more closely. A strong, strategic NATO-EU partnership would deliver many benefits, in political and operational terms, as well as financially.

In doing so, it encourages, indeed demands, *best of industry* solutions and innovation. This would strengthen

- National security of involved nations
- Euro Atlantic security
- National, regional and global business

This would directly benefit security forces, taxpayers and private industry alike.