EuroDefense *(DEUTSCHLAND)*

The President

EuroDefense (Deutschland), Postfach 51 06 47, D-50942 Köln

Ralph D. Thiele
Colonel (ret.)
Postfach 51 06 47
50942 Köln
Germany
Mobil: +49 (151) 50436061
Fax: +49 (221) 8875720
E-Mail: Ralph.D.Thiele@web.de

6 February 2019

Accelerating Defence Innovation via SMEs

Remarks at the sallux and ECR Group Conference

European Defence cooperation: Unintended effects of current policies!

1. Hybrid & Disruptive

The EU global strategy aims at building "*a stronger union*" based on a "*unity of purpose*". It focuses increasingly on self-protection[1] and strategic autonomy. While this ambition is timely vis-à-vis a disruptive, diverse, and fast developing security environment it may well be not sufficient. Hybrid threats and disruptive technologies are driving factually Europe´s security requirements in particular as an increasing number of actors builds their strategies on the rule of force. Some decisionmakers may not have grasped it yet to the full extent. At least the necessary sense of urgency is hardly noticeable.

Technological upheavals suggest that the portfolio of hybrid hazards will rapidly expand. Computers are becoming faster and ubiquitous. Other fundamental breakthroughs include robotics, nano- and biotechnology, artificial intelligence and sensor technology. Machines are getting smaller and more powerful every day. They connect symbiotically with people's lives. In the increasingly developed knowledge society, knowledge proliferates not only legally, but very often also through systematic theft of intellectual property. Communication technologies are backing this development. The enormous potential of AI and Big Data plays an important role.

In the past, military Research and Development put defence at the cutting edge of technology, with the civilian sector eventually taking advantage of those innovation. Today, in many areas, the situation has reversed. SMEs have a key role in dealing with innovation. There are many SMEs that have clearly better innovation performance, that are highly innovative and reach productivity levels way beyond those of large companies as they develop and use their internal strategic resources effectively (e.g. managerial and workforce skills, ICT, R&D, etc.), to include collaborating closely with external partners. We must find better

[1] Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi. THE SECURITY STRATEGIES OF THE US, CHINA, RUSSIA AND THE EU. LIVING IN DIFFERENT WORLDS.JUNE 2018. https://storage.googleapis.com/upi-live/2018/06/fiia_report56_web_security-strategies.pdf

ways to explore the security and defence related potential of emerging technologies and involve industry sooner and more closely.

The European Union and member nations governments should support SME driven innovation by fostering a sound business environment, helping SMEs to develop and use their internal strategic resources effectively, and building an ecosystem accelerating innovation to the benefit of European prosperity, security, and defence.

2. NEO & Digital Transformation

Already today security and defence cooperation are high on the European agenda.

- Member States have launched the Permanent Structure Cooperation (PESCO) in Defence.
- The Commission has proposed the launch of a European Defence Fund to support the development of defence capabilities, from research to prototype thus strengthening the industrial base.
- A Preparatory Action has been launched to strengthen the research side.
- A European Defence Industrial Development Programme (EDIDP) has been proposed to support the co-financing of prototypes development thus strengthening capabilities.
- There have been calls for a European DARPA as a catalyst for disruptive innovation in Europe.[2]

As much as I agree to these initiatives, I hesitate to believe that there is already a sufficient comprehensive, viable vision how to build out of this a stronger, autonomous Europe. We need to deliver better and we need clearer vision & guidance. Two closely interlinked trends have been setting the frame for such approach:

Digital Transformation enables Network Enabled Operations (NEO)

Security organizations and Armed Forces must structure a new business model with core and support processes basing command capability on modern, interoperable, scalable and service-oriented IT as an indispensable basis for network enabled operations. Imperative is to network relevant actors, units and facilities as well as sensors and effectors with each other.

The use of the information space is a multiplier for success in the field. Information is requested, obtained, evaluated, condensed, merged, made available and used for own operations in a better quality and more up-to-date manner than ever before. This accelerates planning and decision-making processes and leads to superior effectiveness in operations. Related fields are:

- Solid knowledge base;
- Evaluation of dynamic, complex processes;
- Common, comprehensive situational awareness; and
- Fast, flexible, precise operational management.

[2] Elżbieta Bieńkowska. Opening speech at the 11th Annual Conference on European Space Policy. Brussels. 22 January 2019. https://ec.europa.eu/commission/commissioners/2014-2019/bienkowska/announcements/11th-annual-conference-european-space-policy-opening-speech_en

In the future, security organizations and armed forces will control and coordinate many processes in real time and over long distances. The prerequisite enabling success is the standardization and modularization of many individual process steps and the programming of virtually editable models of these modules. These are necessary to plan, control and monitor both organizational and operational processes. Communication is increasingly shifting from the higher-level software to the embedded intelligence of individual components. AI and Big Data permit the evaluation and operational/logistical use of the mass data collected.

Digital Transformation changes Industry and Economy

The digitalization of industry and economy is a growth driver, a primary lever for novel business models and services. Industry 4.0, the emerging environment in which computers and automation come together in a new way with remotely connected robotics guided by computers equipped with artificial intelligence permitting the learning of algorithms permitting robotics control and adaptation with very limited human interface, is revolutionizing collaboration, production and services as well as the fundamentals of successful competition. Particular importance is attached to the integrity of networks in the critical infrastructure sectors such as transport, energy supply, banks, hospitals, etc.

Along with these dynamic developments the complexity that decision-makers in companies, security organizations and the armed forces must master is increasing. This explains the dramatically increasing importance of cyber security, which ultimately determines the continued existence of security and defence actors and their continued success.

3. Acceleration & Innovation

To accelerate defence innovation, we need to draw together – on national and European levels - innovative minds in the security and defence realm, innovative companies and private industry into organic entrepreneurship centres. Such centres should target both the private sector and security/defence. These will likely require multi-stakeholder agreements and cooperation on European level and beyond.

I would anticipate that the strategic roadmap to building such ***Acceleration Centres for Security and Defense Innovation*** should look toward a process of development through several phases and build in particular on SMEs. To this end respective approaches and options must be identified along the entire value chain of the civilian and military command and control core, as well as support, processes – both conceptually and operationally – in relation to service functions. Evaluating the strategic fit of these processes requires a creative, analytical and structured approach.

I recommend a portfolio strategy identifying a search filter to gradually move from an anticipated long list of ideas to concrete, actionable scenarios. The following steps should guide the project:

- Define portfolio logic as a search filter.
  The fundamental directions of a strategic reorientation need to be defined as well as the requirements profile of security and armed forces for potential target industries.
- Identify potential options.
  A list of promising ideas and potential options for fields of innovation needs to be developed.

- Evaluate options.
  A structured evaluation of all options with regard to their strategic fit takes place in this phase on the basis of the defined catalogue of criteria.
- Formulate strategic roadmap.
  Formulation of the innovation strategy and its essential elements ready for decision.

As a result of the project, a valid innovation strategy will become available thus optimising the Research, Development & Innovation environment for SMEs to strengthen the innovation capacity of SMEs to the benefit of a strong and secure Europe.

4. Frogs & Eagles

One prevalent feature of the majority of multinational collaborative defence programmes has been the focus on large, expensive and platform-based systems. Many decision makers have been paralyzed by managing huge platform programs. The potential of developing synergetic, interoperable systems optimized for high-end performance in capable C4I systems has been ignored. This has led to institutionally and conceptually fragmented capabilities that do not meet given security challenges.

Security and defence at European level require to change paradigm, to change established cooperation, and to change mindsets. This is true not only for public authorities, but also for business and industry. We need an innovative ecosystem where Frogs & Eagles can grow up well.

- Frogs – i.e. SMEs that master and drive innovation and disruptive technologies &
  Eagles – i.e. Lead System Integrators that master the orchestration of high-tech solutions into an interoperable, superior network-enabled system.
- Frogs – i.e. specialists and professionals that master technological and other challenges &
  Eagles – i.e. generalists and decision-makers that understand complex, dynamic systems and have the gift and education to master and orchestrate the set of tools at their disposal.

Transferring the upcoming hybrid and disruptive technological challenges into a viable, security/defence capability that also pays off on European and global markets is at the core of meeting complex security requirements.

SMEs have a critical role in driving disruptive innovation while larger industry has a key role in Lead System Integration. This approach focuses on optimization at the systems level versus the platform level. It does not favour any particular technology or platform. It enables the trading of risk, cost and capability, and it opens competition at multiple work levels, giving particularly small and medium sized companies from around Europe valid opportunities to compete.