Paper of the ***EuroDefense*** Associations

(13 May 2011)

The Convergence of External and Internal Security

Internal and external security will increasingly be difficult to distinguish conceptually

- Whether a terror act is being conducted by domestic terrorists or part of an asymmetrical form of warfare by another state or another foreign actor is, like many other comparable challenges, hard to distinguish and of less importance to the victims
- Maritime security, for instance, with elements like refugee management, oil platform security, gas pipeline security, port/harbor security, container security, ferry security, cruise ship security, oil tanker security, wind park security, waterway/ channel security, etc., is unlikely to be distinguishable with regard to internal or external threats and will require a coherent response (land likely to include civilian and military elements)
- The same applies to civilian air space management tasks and air defense as well as to urban security mission (police provides security in cities at home, the military is forced to provides security in cities abroad)
- A disease can have natural origins (brought into a country by tourists, birds, etc.) or be the result of a bio terror act, which can be conducted either by domestic (home grown) terrorists or by infiltrated groups originating from the outside
- Opponents, from the inside or the outside, are likely to recourse to means and methods that do not recognize any borders or geographic areas of responsibility and will not accept legal constraints
- The dissemination of high technology, materials, and know-how as well as the proliferation of means of mass destruction/disruption will provide malicious elements with extremely powerful means
- Our societies are increasingly vulnerable – organizationally, procedurally, mentally, technologically; opponents are likely to exploit those vulnerabilities, particularly through cyber- attacks.

The Convergence of Defense and Security

Just as external and internal security will be increasingly hard to distinguish, the same applies to defense and security

- To begin with, war and peace are no longer categories that can clearly be separated
- Defense missions will include a lot of security tasks
- Security tasks will increasingly become more demanding approaching smaller military challenges

- Technological requirements for defense and security will increasingly become overlapping and more demanding (jamming resistance, hardening against electromagnetic effects, surveillance, reconnaissance, intelligence, hacker resistance, etc.)

Additional Considerations

In addition to the developments mentioned above, there are a number of other considerations

- Geographical distance does not provide for security
- Many threats do not respect borders (cyber attacks, micro-organisms, …)
- Most of the challenges are too complex and encompassing to be solved by one nation, or even by one continent, alone
- Similarly, many challenges require responses that go beyond the financial resources of a single nation
- Many criminal actors and terrorists do not act in isolation; hence, international cooperation is essential for preventing, managing and combating crime

A Prerequisite for Any Solution: A Competitive and Innovative Technological and Industrial Base

The private sector holds most of the data, technologies and capabilities which security management requires.

What is required?

- Doctrine convergence and harmonization of security and defence requirements
- Common approaches to developing joint concepts for leadership, doctrine, planning and training.
- Experience in integration of huge and complex systems
- Experience in robust and resilient security solutions helpful (as for the military)
- Comprehensive solutions(from products to service to organizations)
- Managing complexity, ensuring interoperability, minimizing vulnerability
- Reducing manpower requirements
- Examples for interoperable overall solutions
  - Secure communication and encrypted data transfer
  - Control centers (situational awareness)
  - Border control, maritime surveillance & security, (air)port security, site protection
  - Urban security
  - Large event security

  - Logistics security (incl. container security)
  - Support in administrative work / process automation

The Example of Urban Security

Against the background of the convergence of internal and external security as well as defense and security, urban security provides a good point in case for what needs to be done

- In military terms, built-up terrain provides an environment that opponents prefer to operate in since it allows them to conceal and to intermingle with civilians (essential, especially if confronted with superior Western airpower)
- In security terms, cities are the areas where the density and complexity of human interactions is highest, thus also the vulnerability on the one hand and the level of difficulty to provide security on the other
- Urban areas are most vulnerable to disruption and provide most attractive targets
- Modern technologies, together with skilled soldiers and security personnel, provide solutions that significantly improve our security
- Urban security challenges often go beyond the remit of one security service, the "joint" concept applies in security affairs as well. The French Testbed for Urban Security (PPSL)[1] could serve as a training model for other European states
- Key capabilities
  - Surveillance, reconnaissance, intelligence: Wide-area and focus-capable surveillance, biometrics, stand-off CBRNE[2]-detection, intelligence-service integration, adaptive simulation and modeling (e.g., contaminant-dispersal or crowd-behavior modeling)
  - Situational picture generation: Data retrieval, mining, and fusion, interface integration, intuitive man-machine interfaces, localization and map referencing
  - Operations: Multi-service operational and technological interoperability ("jointness"), broad-bandwidth and secure voice/data communication, non-lethal / less than lethal effectors, rapid intervention in intermingled setting
  - Other factors: Trust-generation

1 PPSL: "The aim of the Pilot Centre for Urban Security (French acronym PPSL – Pôle Pilote de Sécurité Locale) […]is to enable security forces and rescue services to assess new technologies and verify that these meet operational requirements, in day to day work as well as in unforeseeable events […]. PPSL will ensure that the new solutions developed by industry will be suitable for end-users, adapted if necessary, and facilitate an easy and fast roll-out." (http://www.ppsl.asso.fr/eng/missions-objectifs.html)

2 CBRNE: Chemical, Biological, Radiological, Nuclear, Explosives.

Recommendations

In order to significantly improve European security and defence, *EuroDefense* recommends that the EU member states make a major effort in the area of security and defence research (technology and development).In the field of security in particular, it is recommended that the following steps be taken:

- As has been suggested in the ESRIF report,[3] the demand and supply side need to align with regulatory authorities early on in order to fit optimal ways to incentivize investments into security and to define useful standards and norms for a secure Europe. This will require transversal and transnational alignment on the public demand side, governments in particular. Only thus will they be in a position to shape and respond to innovation processes in security affairs
- In line with the described and observable convergence of security and defense missions, undoubtedly existing synergies between dedicated security and defense research programs should be identified and exploited. The current and foreseeable financial situation of European Union member states would not forgive us not drawing on existing expertise
- The recommendations of ESRIF with regard to increasing the research and technology budget for security research should be followed and mirrored within the European states themselves. Such an R&D/T drive must naturally be flanked with regulatory harmonization and implementation programs in order to reach operational maturity. Europe needs to be at the cutting edge of technology both in research and in usage, in order to be fully competitive on the global scale ("Good security solutions come also from Europe")
- Structurally, we recommend to build-up test beds and demonstrators and to network them among comparable sites in all European states in order to improve European-wide operational and technical interoperability and standard-definition; where those sites do not exist, we encourage Governments to support the set-up of these important facilities or to come to international usage of existing facilities.

3 European Security Research and Innovation Forum (2007-2009): An expert group initiated jointly by the European Commission and EU member states, tasked with devising a mid to long-term security research and innovation agenda, as well as setting the scene for such an agenda. The full report can be downloaded from the ESRIF website (www.esrif.eu).