EuroDefense *(Germany)*

PO Box 52 02 25
50951 Cologne
www.eurodefense-deutschland.de

Cologne, 16 May 2018

Implementing PESCO in the Cyber Domain

1. Rapid developments

With the treaty of Lisbon (2009) the European Union member states have enabled a gradual process of development from national to integrated European security and military forces. PESCO (Permanent Structured Cooperation) offers the appropriate framework for it. On June 23rd 2017, the European Council decided that within three months, member states shall provide a list of criteria and binding commitments for PESCO including a precise timetable for implementation.

In the context of a changed security environment and novel, hybrid threats, the use of the informational sphere plays a decisive role. Digital revolution brought along a rapid development of diverse, qualitatively new information- and communication-systems. Military weaponry and command and control processes are changing substantially. Besides the classic warfare areas land, sea, air and space, now, also cyber space is becoming a military theatre. However, decisive elements of cyber security – including military cyber security - are chiefly outside of military control, so a comprehensive and conceptual, cross-departmental examination is indispensable.

Already on May 18th, the Council agreed to the desired goal of PESCO, to *“strengthen European security and defence”*. To this end, “*concrete collaborative projects and initiatives need to be identified […]”*. EuroDefense (Germany) therefore offers an implementation proposal in the cyber domain that also suggests the better use of SMEs’ competences in innovation.

2. Fields of action

For all individual EU member states, the challenge is now, to transfer PESCO, as stated in Art. 42, para 6 of the Treaty on European Union (TEU), from theory to practical action. From the point of view of EuroDefense (Germany), following fields of action deserve special attention:

- Forces / capabilities of the first hour
  The concept of the EU battlegroups is in need for a revision. So far, civil and military forces and capabilities for stabilizing operations, deployments or if needed with regards to the mutual assistance clause (Art. 42 TEU and Art. 222 *Treaty on the Functioning of the European Union* / TFEU), which could act rapidly in case of an unforeseen distress are missing. Even more, a common understanding of their use is absent as well.

- Crisis management (foreign deployments) and command and control of the EU

One core competence of the EU is the harmonized use of civilian and military tools for crisis management. For the civilian part, operational leadership structures are long established – for the military, they still are not. These are to be created in combination with the existing civilian structures, preferably as a combined European operational headquarters for strategic-operational planning, preparation, command and control of missions.

- External and internal security
  Trough transnational, international terrorism, organized crime and some forms of hybrid warfare, borders between internal and external security are becoming blurred. There is a need for a permanent organizational solution for strategic early warning, constantly updated situational awareness and a preferably instant coordination between national and international forces (military, intelligence services, border security forces, police) as well as European Agencies (Frontex, EuroPol, EDA, EU-Satcen), especially for border and coastal protection.

- Common training
  Training of security forces and military personnel should be harmonized and made more efficient in the context of PESCO. In addition to an achievable cost reduction, the uniformity of operative and tactical thought processes of participating civilian and military personnel is of particular value. An essential precondition however is, that PESCO-nations come to an agreement regarding common requirements for missions, training and equipment.

- Cyber
  Securing networks and guaranteeing their integrity is one of the biggest challenges of increasing interconnectedness of civilian and military security forces, their leadership and with them PESCO itself. Protecting critical infrastructure is vital with regards to requirements for external and internal security of member states as well as the EU and NATO itself.

3. Common training in the cyber realm

EuroDefense (Germany) is suggesting to strengthen PESCO through common training in the cyber domain. Reasoning: Among plenty of deficiencies in dealing with cyber security, one of the most critical deficits lies with decision-makers of national/multinational security- and defense politics. They often only inadequately understand chances and risks of information technology and the challenges of mitigating associated threats. On the other hand, technical experts comprehend too little of the conceptual and political framework. Therefore, the EU would be well advised to train and educate civilian and military leaders of all its institutions in cyber security. It can resort to existing foundations like the NATO-recommended generic reference curriculum for cybersecurity and integrate national initiatives like the recently founded Cyber Cluster with academia and industry at the University of the Armed Forces of the Federal Republic of Germany Munich (UniBwM).

Subsequent topics are of particular relevance:

- Cyberspace and the basics of cyber security

- Risk-vectors
- Interrelation of defensive and offensive cyber capabilities
- National and international cybersecurity organizations, policies and standards
- Cybersecurity management in a national and international context
- Technical possibilities of attribution and political implications

Hands-on training and technology-handling should provide an impression for practical challenges. Scenario exercises and communication in teams strengthen sensitivity and capabilities for upcoming leadership tasks. High leadership levels are to be included as well, as especially their learning success leads to systemic improvements. Simulation-based exercises in a multi-national inter-agency environment can comprehensively prepare participants for handling future challenges.

Since its foundation, the European Defense Agency (EDA) has been tasked, “*to support the Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future*”. It is therefore suited to provide a functional training authority for the cyber-realm as well. However, it is of importance to include all stakeholders – in particular civilian stakeholders – in a comprehensive approach. This would also ease a development, where military and civilian technology-users regularly add cybersecurity specifications to their tender offers.

4. Small and medium enterprises (SMEs)

Training in the cyber-realm should explicitly include industry and academia. IT enterprises are essential due to their extensive supply chains and their ability to set rules and standards as well as advance technological developments with upfront investment. The emerging cyber cluster around the UniBwM was already mentioned as an example.

Furthermore, SMEs can significantly contribute to successfully meeting the enormous dynamics of national and international cyber challenges. The EU council, in its conclusion of November 14th, reinforces the need to “*enhance the effectiveness of CSDP and the development and maintenance of Member States’ capabilities, supported by a more integrated, sustainable, innovative and competitive European Defence Technological and Industrial Base (EDTIB)*” for implementing the EU global strategy in the area of security and defence, while referring to the council conclusion of December 2013. For that matter, the particularly pronounced competence for innovation of SMEs should be used more extensively than so far. For years, efforts have been made to use that potential, for example through the institution of an SME-representative in Germany. However, so far it has only mildly contributed to strengthening SMEs in the security sector.

EuroDefense (Germany) suggests to install a periodic – e.g. annual – innovation exchange, in which the industry gets the opportunity to introduce its ideas. With special industrial policy interest, relevant innovative industry approaches could be focused and bundled. A public funding should be considered. A common cyber training program offers an excellent starting point for a cyber- innovation exchange.