Research Report

Industrial analysis for the prioritised action of cyber defence of the Capability Development Plan

15.CPS.SC.028 & 15.ESI.SC.260

Executive summary

Susanne Søndergaard, Jacopo Bellasio, Jan Gaspers & Eun A Jo

RAND Europe

RR-1473-EDA
February 2016
Prepared for the European Defence Agency (EDA)

RAND EUROPE

The present study was ordered by the EDA. The contractor who has undertaken the study remains responsible for its content.

Executive Summary

The present study was ordered by the EDA. The contractor who has undertaken the study remains responsible for its content.

Study context

Cyber defence was identified as a priority by the participating Member States (pMS) in the Capability Development Plan of 2010, alongside a number of other areas for capability development. A pilot Industrial Analysis for cyber defence in Europe was undertaken by RAND Europe in order to assess the extent to which European industry could cater for current and emerging cyber defence requirements. This assessment was framed in the context of Crisis Management Operations (CMO) conducted under the Common Security and Defence Policy (CSDP) and aimed also to identify any critical dependencies on industries outside Europe.

Methodology

In order to answer the question whether European industry is at present able to deliver the Cyber Defence capabilities required to conduct CSDP CMO, the study team undertook a number of different activities:

1) Identification of **current** CSDP CMO cyber defence requirements (Chapter 3).
2) Review of European threat assessments to identify **future** cyber defence requirements (Chapter 4).
3) Landscaping exercise of existing cyber security and defence European industry (Chapter 5).
4) Analysis of the extent to which European industry covers the range of required current and future cyber defence technology and provision of recommendations (Chapter 6).

Based on a document review conducted in light of the cyber threats expected to drive military capability requirements and market developments as well as several validation rounds, including with the EDA and the EUMS (EU Military Staff), this study identified nine cyber defence materiel technological capability areas that underpin the conduct of cyber defence in the context of CSDP CMO. Five of these technological capability areas were established Technology Areas and four were new or emerging Technology Areas. The **established** Technology Areas are:

- Fundamental Technologies
- Devices
- Intrusion Mitigation
- Critical Infrastructure Protection
- Security Management System.

The **emerging** Technology Areas are:

- Civil and Business Infrastructure Protection
- Command and Control
- Autonomously/Remotely Piloted Platforms/Systems
- Hacktivism Control

Each Technology Area further contains a variable number of Technology Fields, comprising underlying technologies and services characterising the input required from each Technology Area for engaging in CSDP CMO.

Headline findings

A landscaping exercise was conducted in order to collect online data on 504 companies operating in the cyber security domain in Europe. The analysis of the data indicates that at present this is a diverse and vibrant industrial sector. A number of companies could be identified that covered all established and emerging technologies, although, as summarised below, the coverage provided by companies is markedly uneven both in terms of different Technology Areas and Technology Fields and as regards different EU regions. However, the assessment conducted as part of this study provided a purely quantitative overview of the industrial base, without attempting an assessment of the quality of services and products available. Furthermore, due to time and resource constraints, the analysis undertaken was limited by a set of assumptions that are presented in the following chapters.

With reference to Technology Areas, for established technological capability requirements, European industry appears to offer a solid coverage across EU Member States. However, within each Technology Area, a number of Technology Fields enjoy very limited coverage and industrial activity within the EU. This holds true also for established Technology Areas that appear broadly speaking to be well served (i.e. Fundamental Technologies; Devices; Intrusion Mitigation; Security Management Systems). In particular, the Technology Field of Biometrics appears to be lagging behind in terms of industrial activity within the EU. Similarly, within the Technology Area of Intrusion Mitigation, there is a paucity of industrial actors in the Technology Fields of Forensic, and of Distributed Denial of Service Protection and Mitigation.

It is worth noting, however, that only a handful of companies were identified as active in the Technology Area of Critical Infrastructure Protection. The industrial coverage in this Technology Area appears thus to be very limited at European level, despite this being an established technological requirement for engaging in CSDP CMO.

Similarly, companies have been identified for all the emerging technological requirements areas, but the number of industrial actors within these TAs appears to be especially limited. Furthermore, in some cases, such as for Autonomously/Remotely Piloted Platforms/Systems, a more qualitative assessment of products would be required to determine whether companies identified are actually in a position to respond to the cyber security and defence military needs of this TA.

The research indicates that the majority of companies reviewed have clear and advertised links with the defence establishment. It is worth noting, however, that it was not possible to identify any cyber security company focusing on delivering products and services exclusively for the military or the defence establishment. The research team only encountered companies that were active either in both the military and civilian domains or in the civilian domain exclusively

No significant discrepancies appear to characterise the group of companies identified as operating only within one Technology Area vis-à-vis the broader industrial population. However, the ratio of such companies appears to be higher for Technology Areas concerned with hardware, rather than software, capability development.

Analysis of geographic coverage across the European Union seems to suggest that a significant gap exists between Northern and Central Europe on the one hand, where the majority of identified companies are located, and Southern and Eastern Europe on the other. In the latter two regions, the industrial base appears to be thinner, although this gap is mitigated by the presence of companies with offices across multiple EU countries and regions.

A significant role in the EU Cyber Defence industrial base is also played by companies whose main headquarters are located outside the EU. These companies comprise 9.5 per cent of the total population registered in our database. At the level of individual Technology Areas, the incidence of non-EU based companies is in line with that of the overall population, oscillating between 10 and 13 per cent of companies active in each Technology Area.

Avenues for further work

The landscaping exercise has proved to be a complex undertaking since comprehensive information on the cyber security and defence industrial sectors has so far not been collected or organised in a systematic way, even by industry members. As a result, one clear gap identified within the EU industrial landscape for Cyber Defence (CD) CSDP CMO is that of a central point of contact, tasked with maintaining an active network between different industrial players and organisations so as to facilitate the exchange of information and capabilities within this field.

The study was conducted with a number of assumptions in mind, which are outlined in the main body of the text. The reader should note that these assumptions impose a number of constraints and limitations on the study and its findings.