Synopsis – Cyber Situation Awareness Package

Contents

Executive Summary

1. Introduction
   1.1 Background
   1.2 Aim
   1.3 Scope
   1.4 Assumptions

2. Mission Need
   2.1 Main Characteristics
   2.2 Threat Analysis
   2.3 System Employment Concept

3. Required Operational Capabilities
   3.1 Architecture
   3.2 CIS Infrastructure Discovery
   3.3 Threat Management
   3.4 Cyber Real-Time Sensor Interface
   3.5 Cyber SA Functional Areas Service
   3.6 Cyber Command and Control
   3.7 Decision Tool
   3.8 Security
   3.9 Through-Life Support

4. Review of Lines of Capability (DOTLMPFI)

5. In-Service Date

Annexes

A. Situation Awareness Definition
B. Glossary of Terms
C. References
Executive Summary

The Cyber Defence Concept puts responsibilities on military commanders at all operational levels to put in place measures to mitigate the risk of cyber-attack. An important prerequisite is to provide situation awareness (SA) for the commander and his staff. This SA is based on a general and specific threat landscape from which the risk of cyber-attack can be observed, understood, evaluated. Based on this SA, informed decisions can be made to mitigate the risk of cyber-attack. The threat landscape is formed from a baseline of general threats augmented by specific (real-time sensor) threat intelligence used to build the 'known' threat picture. There will be unknown threat vectors that need to dealt with in a more dynamic and reactive way.

The purpose of the CySAP Project is to describe the requirements, potential solutions and acquisition routes that can be used to put in place a capability to identify and manage the risk of cyber-attack within an EU-led operation - through, for example, provision of a 'common and standardised cyber defence planning and management functional area service'.

This CST will be developed into from an agreed scope of user requirements to system requirements within a Common Staff Requirement with supporting Business Case and Through Life Management Plan (TLMP). Acquisition options can then be considered with a view to initiating a combined acquisition programme to put in place a portfolio of capability modules that CMS can draw upon for exercises and operations.

The Target effect is for commanders to have a clear understanding of the specific and real-time threat landscape applied to the communication and information systems (CIS) supporting his CSDP operation. In addition, the Target effect is to equip the commander with the tools (competent personnel, effective procedures and platforms) to manage risks during the planning and conduct phases of an operation; primarily this shall result in the application of
well-informed decision-making. The outcome shall be a cyber-environment sufficiently benign to enable freedom of action in the remaining operation environments of maritime, land, air and space.
1. Introduction
This section comprises the background, aim and scope for the Project by describing the capability being addressed.

1.1. Background
Cyber Space is today widely recognised as the 5th operational domain along with the traditional physical domains land, sea, air and space. The success of CSDP civilian missions and military operations in the physical domains are increasingly dependent on the availability of, and the access to, cyberspace. This paradigm shift should be considered in the preparation and conduct of EU-led operations as the unpredictability and asymmetry of cyber threats could impose tremendous limitations on the effectiveness of military operations.

The recently released Cyber Security Strategy for the EU (Reference 1) recognises Cyber Defence as one of the strategic priorities of the EU. This was reinforced by the European Council Conclusions of 19/20 December 2013 (Reference 2) where Members States, with the support of the European Defence Agency, welcomed concrete projects focused on inter alia “…training and exercises, improving civil/military cooperation based on the Cyber Security Strategy as well as the protection of assets in EU missions and operations.”

The European Council also recalled that “…Cooperation in the area of military capability development is crucial to maintaining key capabilities, remedying shortfalls and avoiding redundancies. Pooling demand, consolidating requirements and realising economies of scale will allow Member States to enhance the efficient use of resources and ensure interoperability…”.

According to this view, Member States in the framework of European Defence Agency (EDA) has, since 2011:

• identified cyber defence as one of ten priorities in its Capability Development Plan (CDP) (Reference 3); moreover, the current (Strand B) Evaluation Report contributing to the 2014 CDP update (Reference 4) has concluded that “there is a
quantitative shortfall in required capability” to “ensure effective use of cyberspace” and identified that there are associated high operational risks for CSDP Illustrative Scenarios;

• established a dedicated Project Team (PT) to identify collaborative options for cyber defence at the EU level; the PT also prepared a “Strategic Context Case” (Reference 7) to describe the capability development strategy for Cyber Defence in all the dimensions pMS are concerned including in particular the context of Common Security and Defence Policy (CSDP) and associated Crisis Management Operations (CMO).

The EU concept for cyber defence for EU-led Operations (Reference 5) defines the key responsibilities of strategic, operational and tactical commanders. The Cyber Defence Capability Requirements document (Reference 6) was agreed by the EU Military Committee (EUMC) in March 2013. On the basis of these requirements and the Strategic Context Case (Reference 7) for the EDA Project Team Cyber Defence (PT), EDA has undertaken action to identify collaborative options and pooling and sharing initiatives for cyber defence at the EU level.

1.2. Aim

This CST for a Cyber SA Package (CySAP) outlines the operational user-requirements for a modular capability to help manage the risk of cyber-attack on CIS used within HQs used for national and multinational operations through providing cyber Situation Awareness (defined at Annex A). The CST is developed from the Food-For-Thought Paper presented to the EDA Steering Board (SB) on 30 May 2013 (Reference 8). The CST shall be used to initiate the ‘Programme Preparation Phase’ described at (Reference 9) within a Category B Project which will define the Common Staff Requirement and associated Business Case and Through Life Management Plan. These will be derived from the capability needs of the contributing Member States (cMS).

1.3. Scope
The scope of the CySAP is defined by a set of capability modules based on user requirements that fit together within an architectural framework drawn from the EDA Project Team framework contract for Cyber Defence Capability, Work Package WP1 (Reference 10 – Cyber Defence Reference Architecture). The principal mandate for the Project comes from the EU Concept for Cyber Defence (Reference 5), which describes the responsibilities that rests with commanders at the strategic, operational and tactical levels. Consequently, the CySAP primarily addresses the needs of commanders and non-specialist HQ staff with no special “cyber-background”. A modular approach provides a mix of capabilities that cMS can call on to meet a particular operation's requirements and to provide the user requirement of cyber SA and decision-making assistance. Each module must have a stand-alone utility as well as the ability to coherently interoperate. A modular approach will provide a mix of capabilities that cMS will be able to call on to meet a particular operation’s requirements. The scope is expanded within Section 3, Required Operational Capabilities/User Requirements.

1.4. Assumptions.

1.4.1. It is assumed that the scope is restricted to managing risk through SA within the CIS infrastructure at classifications of SECRET and below. This comprises networks and associated software applications, functional area services and hardware.

1.4.2. It is assumed that the scope includes CIS used to support CSDP operations and CIS used to exchange and manage information within the EU mission network(s).

1.4.3. It is assumed that the scope initially excludes an interface to ISR sensors (other than cyber-attack sensors), weapon systems, logistics platforms, effectors and other capability platforms but in the future the CySAP should be able to be developed to include these platform and other operational network enabled capabilities.
1.4.4. It is assumed that within each operation, HQs and associated CIS infrastructure will have the services of a Security Operations Centre.

1.4.5. It is assumed that each cMS will have agreed business continuity and recovery policies that can be implemented within the CySAP.

1.4.6. It is assumed that this is a ‘pooling and sharing’ project.
2. Mission Need

This section addresses the ‘mission needs’ and refers in non-technical terms to identified capability gaps and perceived threats/risks that need to be addressed. It is the foundation of the Business Case that later expands on the justification for the Project - described in terms of envisaged benefits and desired outcomes.

2.1. Main Characteristics

The Cyber Defence Concept describes the requirement to prevent, detect, respond to, recover from and learn lessons from cyber-attacks. Based on this conceptual outline of HQ responsibilities there needs to be the ways and means to enable HQs’ staff to:

- visualise and interpret the threat landscape as presented by the SOC and other sources;
- picture the symptoms of all stages of a cyber-attack that affects the conduct of the operation;
- to enhance the management of the risk of cyber-attack;
- and to enable fast and effective restoration of CIS and other capabilities affected by cyber-attacks.

The main user requirement is to picture/visualise the risk of cyber-attack through a CySAP. Using this risk management approach will provide the benefit of HQ staff being able to understand:

- the likelihood of attack to be assessed and described against a baseline defined during the operation planning phases.
- an understanding of the impact of an attack so that counter-measures can be planned under the legal regulations, which the preferred option could be executed.
The risk of cyber-attack is characteristically diverse and the likelihood and impact of such an attack is susceptible to being subject to constant change. The impact on the operation caused by a cyber-attack may be:

- **Direct**, affecting the operational CIS used during the operation;
- **Indirect**, affecting host nation infrastructure such as telecommunications and power supplies;
- **Tangible**, such as data exfiltration, denial of service, physical damage to material;
- **Intangible**, such as damaged reputation, loss of confidence in CIS confidentiality, integrity and availability.

The attack may provoke also a combination of effects: direct tangible, direct intangible, indirect tangible, indirect intangible. The CySAP project should be able to manage these impacts scenarios.

### 2.2. Threat Analysis

Section 3 of the EDA Study on Cyber Threat Intelligence (Reference 11) highlights 'key relevant points' in the context of Cyber Threat Intelligence for EU-led operations. The sharing of CTI is described in Section 4 and includes technical standards, frameworks and systems. In addition, the Final Report of the General Secretariat of the Council Cyber Threat Intelligence Project (Reference 13) includes Use Case studies for cloud computing resource attack and classified network deployable package infiltration. The Report is classified *Restricted EU/Restreint UE* and provides an analysis of current capabilities supporting operations (Unclassified systems: Maritime Security Centre Horn of Africa, MERCURY, HERMES; and classified Secret Office Local Area Network (SOLAN) deployed to FHQ via Satcom Deployable Package).

The conclusion is that the threat of cyber-attack is growing and that the potential impact on operations could be severe. Whilst many Cyber Defence capabilities are
in place or in course of development, there remains a lack of capability to provide HQs’ staff with adequate cyber situational awareness.

2.3. System Employment Concept

The CySAP shall be a highly flexible and scalable capability that can be applied to a range of operational (scenarios) within EU, national or other coalition/combined operations. It can be employed within HQs across all operational levels from the military strategic to the tactical. In the absence of a permanent military C2 structure, the EU has three strategic options for commanding and controlling military operations:

- First, there is the recourse to NATO assets and capabilities using the Berlin-Plus arrangements. In this case the preferred option is to establish the EU Operation Headquarters at SHAPE.
- Second, the EU can have recourse to the Member States’ assets and capabilities. In this case the OHQ/FHQ will be provided by the Member States able to provide the HQ/FHQ capacity.
- Third, the EU can activate its Operations Centre in the EU Military Staff to plan and conduct as autonomous EU operation.

In these cases, where appropriate, the CySAP capability should be used by multinational augmentees, and should be managed within the Pooling & Sharing Code of Conduct.

In the second case the CySAP should be managed by the Parent Nation.

The own modular configuration will permit to the CySAP to be employed at different level (OHQ, FHQ, Component Command), in relation to the complexity of the operation and of the assigned forces, taking into account that, in average, there will be need at least a CySAP for each mission network; i.e.

- a static package should be placed at the EU OHQ (managed by a Task Force C4, provided by the Parent Nation of the OHQ);
• a deployable package should be provided to the OHQ by the Parent Nation together the DCM to ensure the set-up of a Mission Network to link the OHQ to the FHQ in the theatre (the CIS assets are a responsibility of the Parent Nation);
• a deployable package should be available for the FHQ to link with another tactical mission network the FHQ with the Component Commands.

The CySAP needs the technical support of a SOC (Security Operation Centre). It is the responsibility of the Parent Nation of an EU OHQ/FHQ to provide the support of the national SOC.

3. Required Operational Capabilities and User Requirements

This section develops the scope into target user requirements for the modules within the CySAP. It is envisaged that as requirements are developed, the function and scope of this modules will be refined. The following nine functional models address user requirements in order to put in place the required operational capabilities:

3.1. Architecture. The architecture module is the framework upon which the CySAP capability requirements shall be defined and built. It is an essential requirement that CySAP is developed in architectural terms consistent with the NATO Architecture Framework v3 and concurrent CSDP architectural products. Particular reference shall be made to the Cyber Defence Reference Architecture developed as the initial work package of the EDA Framework Project on Cyber Capabilities (Reference 10). Also, Chapter 8 of the EDA Study on Cyber Threat Intelligence (Final Report dated 5 December 2013) (Reference 11) describes the ‘State of the Art Operational System Architecture’. Finally the General Secretariat of the Council (GSC) Network Defence Centre (NDC) conducted a study reported at Reference 13 which also provides a relevant architectural landscape. The main benefit from this module will be the deduction of processes that will inform the flow of information within the CySAP – and associated interfaces. It is mandatory to integrate open standards in the architecture to allow modifications and national extensions.
3.2. **CIS Infrastructure Discovery.** In building situation awareness, an accurate **CIS infrastructure picture** is first needed of ‘own/friendly (CIS Infrastructure) forces’. Also, where a Service Orientated Architecture is used, analysis is need of Service information sources. This is essential so the staff supporting the commander can determine the span of responsibility for CIS infrastructure at all levels of classification within the operation and how a cyber-attack might affect the conduct of the operation. This is also important because CIS infrastructure shall be interconnected with other networks and associated information systems. Such interconnections (and associated dependencies) represent vulnerabilities and associated risks to be managed. The source of information for this ‘own infrastructure picture’ may either come from within the CySAP Project or, will be provided by Security Operation Centre systems external to the Project as defined within information exchange requirements and open interface standards. Any reconfiguration of the CIS network should result in a real time updating to the data contained by the CySAP. Appropriate gateways/ interfaces and updating procedures are essential to ensure that decisions are always based on accurate and up-to-date information.

3.3. **Threat Management.** The CySAP shall be dependent on intelligence product drawn from reference sources. The threat management module will represent the initial intelligence product derived during the operation planning phases and continued to be updated throughout the operation. The module shall need to match intelligence product requirements with CONOPS requirements (to provide the operation’s environmental context) and with CIS Infrastructure Picture information presented by the Infrastructure Discovery Module as well as other external sources. The establishment and maintenance of this database could be an external interface with associated specification, service level agreement and/or statement of requirement. The ‘State of the Art for Information Sources’ is described in chapter 5 of the Reference 10. Aside from this threat reference source, processes (derived in the Architecture module) are required to define the threat analysis.
requirements. A look at Actors and Processes are outlined in chapter 6 of Reference 11.

3.4. **Cyber Real-Time Sensor Interface.** The requirement for the threat management module is to provide *inter alia* a background threat level and more dynamic information including indicators and warnings (I&W) to be monitored by personnel and by supporting systems/software. In addition, operation-specific real-time sensor information is needed from the *CIS Infrastructure Picture*. This shall require a collaborative interface arrangement with the Security Operations Centre (SOC). Sensors can also comprise information sources from national ‘reach-back’ agencies and people such as HQ staff and CIS specialists trained to identify symptoms of cyber-attack.

3.5. **Cyber SA Functional Area Service.** Dynamic risk management functionality is needed through evaluation of information derived from the previous 3 modules: own CIS Infrastructure Picture (and highlighted vulnerabilities), Threat Product; and Real-Time Sensors. The requirement for the CySAP Functional Area Service (FAS) is to compare this information with business continuity and recovery policies. The following specific functionality is required (in no specific order of priority):

3.5.1. **CIS Infrastructure criticality and vulnerability assessment.**

This sub-module presents information to enable staff to determine the critical areas and associated dependencies of the CIS Infrastructure Picture and to map and assess associated vulnerabilities.

3.5.2. **Threat Evaluation – likelihood assessment.** This sub-module provides a measured indication of the likelihood of an attack based on an evaluation of the threats.

3.5.3. **Cyber-attack damage and impact assessment.** This sub-module is required to monitor and assess the conduct of a cyber-
attack and to provide an assessment of the impact and damage. In addition it should be used to assist in the prediction of the impact of identified threats should the CIS Infrastructure come under cyber-attack.

3.5.4. Lessons. This module provides functionality to describe and map (on network illustrations) the features of a cyber-attack (such as source, impact, scale, recovery action) and enables the export of lessons to the HQs’ extant lessons identified application (such as the EU Lessons Management Application).

3.6. Cyber Command and Control (C2). Part of, or linked to, a Cyber SA FAS is the module enhancing decision-making within the wider C2 environment. Visualisation of threats, risk, and real-time situation needs to be made by commanders and specialist staff. Consideration is needed on what information needs to be available on other operational pictures available to HQs. This module is required to outline the visualisation (to J6 and Cyber Staff) and COP representation to (non-technical) staff and the commander.

3.7. Cyber Defence Decision Support: Part of, or linked to, a Cyber SA FAS is a module to assist HQ decision-making. Given the likely fast pace of cyber-attack and associated difficulty of identifying and interpreting symptoms of an attack, a module shall be needed to simplify and accelerate the decision-making process. This comprises:

3.7.1. A tool for decision-making that enables a 'what-if' approach to be developed where the implications of actions can be determined.

3.7.2. A tool for business continuity options analysis based on existing business continuity plans.
3.8. **Security.** A foremost requirement to be developed is the security of the CySAP capability itself which by its nature will be at risk of attack. The CySAP should have greater levels of availability, confidentiality and integrity than the protected system. National security accreditation authorities need to be involved at the earliest opportunity and requirements incorporated within the CSR and supporting products. The other aspects to consider are:

3.8.1. Application of national Information Assurance regimes.
3.8.2. Compliance with national regulations and accreditation arrangements.
3.8.3. Security requirements for interconnection of CySAPs between HQs (potentially via unprotected networks).
3.8.4. Personnel security level requirements.
3.8.5. Security requirements to be adopted during Programme.
3.8.6. Cross-domain information sharing.

3.9. **Through Life Support.** There needs to be a specific module that describes the CySAP though life support. This shall comprise the following sub-modules:

3.9.1. **Training/awareness.** Given the 'Materiel' and 'Personnel' capabilities of the CySAP, an associated training needs analysis should be addressed by cMS and, within the TLMP, details of what through-life training capabilities and exercise planning factors (such as cyber-attack scenarios) need to be put in place.

3.9.2. Service Provision arrangements (eg. threat intel product source)
3.9.3. Licenses (particular software functionality updates, certificates and crypto key management)
3.9.4. Host CIS Change Control (to manage changes in national CIS infrastructure)
3.9.5. Mid-life Update (to enable the CySAP to react to the changing threat landscape to CIS)
3.9.6. Open interfaces to enable connections with other CIS on a flexible basis – supporting future mission network integration.

4. **Review of Lines of Capability Development (DOTMLPFI)**

This section briefly outlines the lines of development to be addressed on the development of the CSR and supporting documents.

4.1. **Doctrine and Concept.** Cyber Defence Doctrine is not within the scope of this project albeit a recommendation for Member States in the Stocktaking Study of Military Cyber Defence Capabilities in the EU (Final Report PR-469-EDA dated March 2013) (Reference 12).

4.2. **Organisation.** Due reference should be made of the organisation relationships between Cyber Defence capabilities.

4.3. **Training.** It is assumed that there shall be training needs specific to the CySAP to be addressed within the scope of the Project. This has been identified as a separate sub-module within the scope [1.3.9.1].

4.4. **Materiel.** The scope of the CySAP shall be structured upon a reference and target architecture. This architecture shall make clear the materiel and logistics support elements to be included within the Programme Preparation.

4.5. **Leadership/knowledge.** There is a requirement for the identification of leader(s) who within cMS will be the ‘sponsor’ or lead CySAP capability implementation.

4.6. **Personnel.** Linked to the training line of development (and potential training needs analysis to be conducted), the CSR will need to propose the minimum numbers and types of personnel employed to support and operate the CySAP, (together with their operational trained standard of competence).
4.7. Facilities. The CySAP will need to be hosted by both static and deployable HQs with associated support arrangements. This is primarily a materiel support issue but may link to other facilities.

4.8. Interoperability. This is a key capability development feature addressed throughout the CST and comprises:

4.8.1. Procedural, SOPs
4.8.2. Organisational, policy relationships
4.8.3. Technical, standards – reference architecture

5. In-Service Date

This section outlines an estimated time-line that the project initiation and follow-on stages could follow. This is important because cMS need to align national capability strategies, armament options and budgetary planning.

5.1. The Target is to achieve CySAP initial operating capability within one or more cMS HQs by end-2016. This is based on an iterative approach where the capability modules described in the Scope will be developed in an integrated way but enable lower levels of capability with lower levels of implementation risk to be introduction into service ahead of others.

5.2. Milestones. An outline of target milestones is as follows:

- Common Staff Target (CST) Steering Board approval by end-May 2014.
- CSR Steering Board approval by end-2014.
- 2015: Prototype/capability demonstrations options/scenario development
- 2015: Establish Adhoc Programme Group (AHPG)
• 2015: Initiation of Adhoc Programme and agreement of MoU
• 2016: IOC – to be defined in CSR.
Situation Awareness Definition for the CySAP

The success of military operations depends on the ability of processing and assessing information in order to gain an adequate understanding of the crises situation. Often, these activities are referred to as situational / situation awareness\(^1\) or situational understanding. This section addresses how SA as a military, a psychological and a technical concept is understood and what contributions from social media are associated with it. In understanding SA, one has to consider its importance and its application in different fields that are usually not addressed explicitly. However, this application in different domains and importantly, the difference in their understanding of SA make for a lot of misunderstandings.

We distinguish here between three perspectives. Generally, SA is viewed as a cognitive process from a Human Factors perspective; it is used as an aggregated concept in the military; and finds visualization support in computer science and software development. First, for the Human Factors branch – which has its roots in psychology – SA is about the cognitive processes immanent in the human mind to construct an understanding of the current environment. Secondly, the military pin their approach on the overall SA concept with a focus on gaining SA in support of operational planning processes. Thirdly, the information scientist focuses on information visualization to support SA. The figure below depicts these three views graphically.

Figure 1) Situation Awareness from three different perspectives

\(^1\) Situational awareness is commonly used in the military in the meaning of “knowing what is going on right now”. Situation awareness stands for a broader understanding of the crises situation; it is used for the broader situational picture over a longer period. For practical implications in this CST we use SA in the latter sense.
## Glossary of Terms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2</td>
<td>Command and Control</td>
</tr>
<tr>
<td>C2COE</td>
<td>Command and Control Centre of Excellence</td>
</tr>
<tr>
<td>C4</td>
<td>Command, Control, Communications &amp; Computers</td>
</tr>
<tr>
<td>C4ISR</td>
<td>Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance</td>
</tr>
<tr>
<td>CCDCOE</td>
<td>Cooperative Cyber Defence Centre of Excellence</td>
</tr>
<tr>
<td>CD</td>
<td>Cyber Defence (see below)</td>
</tr>
<tr>
<td>CDMA</td>
<td>NATO’s Cyber Defence Management Agency</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CERT-EU</td>
<td>Computer Emergency Response Team – European Union</td>
</tr>
<tr>
<td>CIS</td>
<td>Command Information System</td>
</tr>
<tr>
<td>CMO</td>
<td>Crisis Management Operations</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-The-Shelf</td>
</tr>
<tr>
<td>CSDP</td>
<td>Common Security and Defence Policy</td>
</tr>
<tr>
<td>DLOD</td>
<td>Defence Line of Development</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>EC3</td>
<td>European Cyber Crime Centre</td>
</tr>
<tr>
<td>ECI</td>
<td>European Critical Infrastructures</td>
</tr>
<tr>
<td>ECTEG</td>
<td>European Cybercrime Training and Education Group</td>
</tr>
<tr>
<td>EDA</td>
<td>European Defence Agency</td>
</tr>
<tr>
<td>EEAS</td>
<td>European External Action Service</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Network and Information Security Agency</td>
</tr>
<tr>
<td>ESDC</td>
<td>European Security and Defence College</td>
</tr>
<tr>
<td>ESDP</td>
<td>European Security &amp; Defence Policy</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>ESS</td>
<td>European Security Strategy</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EU BG</td>
<td>European Union Battle Group</td>
</tr>
<tr>
<td>EU Sitcen</td>
<td>European Union’s Situation Room/Centre</td>
</tr>
<tr>
<td>EUMC</td>
<td>European Union Military Committee</td>
</tr>
<tr>
<td>EUMS</td>
<td>European Union Military Staff</td>
</tr>
<tr>
<td>EUCSS</td>
<td>European Union Cyber Security Strategy</td>
</tr>
<tr>
<td>FCC</td>
<td>frameCyberCap</td>
</tr>
<tr>
<td>FHQ</td>
<td>Force HQ</td>
</tr>
<tr>
<td>HQ</td>
<td>Head Quarters</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>ISAF</td>
<td>International Security Assistance Forces</td>
</tr>
<tr>
<td>J6</td>
<td>Military Staff Function with CIS (and CD) responsibility</td>
</tr>
<tr>
<td>JSP</td>
<td>Joint Service Publication</td>
</tr>
<tr>
<td>KSA</td>
<td>Knowledge, Skills and Attitudes</td>
</tr>
<tr>
<td>LoI</td>
<td>Letter of Intent (to provide a standby OHQ)</td>
</tr>
<tr>
<td>milCERT</td>
<td>Military Computer Emergency Response Team</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NEC</td>
<td>Network Enabled Capability</td>
</tr>
<tr>
<td>NICE</td>
<td>National Initiative for Cyber Security Education</td>
</tr>
<tr>
<td>NIS</td>
<td>Network on Information Security</td>
</tr>
<tr>
<td>NC3A</td>
<td>NATO's Command Control and Communications Agency</td>
</tr>
<tr>
<td>OPSEC</td>
<td>Operational Security</td>
</tr>
<tr>
<td>OHQ</td>
<td>Operational HQ</td>
</tr>
<tr>
<td>OSCE</td>
<td>Organization for Security and Co-operation in Europe</td>
</tr>
<tr>
<td>OTA</td>
<td>Operational Task Analysis</td>
</tr>
</tbody>
</table>
Definitions of cyber defence and associated terms can be found in Reference 5, the EU Concept for Cyber defence.
References:

2. EU Council Conclusions of 19/20 December 2013 (EUCO 217/13 dated Dec 13)
4. EEAS 0037/14 dated 19 Feb 14.
5. EEAS 02305/12, dated 20 December 2012, EU Concept for Cyber Defence for EU-led Operations.
6. EEAS 00713/13, dated 27 March 2013, Cyber Defence Capability Requirements
7. Strategic Context Case of the EDA Project Team Cyber Defence (as approved by the EDA SB Cap in October 2012).
8. Food-For-Thought Paper presented to EDA Steering Board (SBID 2013/05).
11. EDA Study on Cyber Threat Intelligence (Final Report dated 5 December 2013).
13. DGA CIS/SSICS/005 dated 6 Feb 2013 covering the Final Report of the GSC Cyber Threat Intelligence Project. [Restricted EU/Restreint UE]