**SUPREME HEADQUARTERS ALLIED POWERS EUROPE**

**TALEO Job Number: 210013**

**Vacancy Number: A08/0121**

**Post Number: OSC CYPX 0140**

**Job Title: Senior Engineer (Requirements)**

**NATO Grade: A-3**

**Basic Monthly Salary (12 x per year): 6.882,73 €, tax free**

**Closing Date: Sunday 18 April 2021**

SHAPE is looking for a Senior Engineer (Requirements) to support the management and the synchronization of cyberspace security requirements. If you have experience in the cyberspace field and you wish to work in a challenging and fast moving policy and operational area in an international environment, this post will be ideal for you.

## GENERAL BACKGROUND:

SHAPE, the Supreme Headquarters Allied Powers Europe, is the Headquarters of Allied Command Operations (ACO), one of the two major military commands of the North Atlantic Treaty Organisation (NATO). ACO safeguards an area extending from the northern tip of Norway to the eastern border of Turkey. This equates to nearly two million square kilometres of land, more than three million square kilometres of sea, and a population of about 320 million people.

## POST DESCRIPTION:

**Location:** Casteau/Mons, 60 Km south of Brussels (Belgium)
**Division:** J6 Cyberspace

### Post Context/Post Summary

SHAPE provides an integrated Strategic Effects framework, employing a multi-domain and multi-region focus to create a 360-degree approach, with the flexibility to enable, upon direction, a seamless transition from Baseline Activities and Current Operations (BACO) up to the Maximum Level of Effort (MLE). SHAPE supports SACEUR in fulfilling his terms of reference, as directed by the North Atlantic Council.

The Cyberspace Directorate is responsible for directing, monitoring and coordinating all cyberspace functional area activities and staff functions across ACO.
The J6 Cyberspace Division provides the strategic staff functions for cyberspace aspects within ACO's strategic direction, planning and risk management to support NATO-led operations, initiatives, exercises and activities.

The Cyberspace Strategic Plans & Policy Branch provides military Subject Matter Expertise advice, strategic direction and oversight of all cyberspace functional area activities across ACO.
The incumbent is one of five staff primarily involved in the management and synchronization of cyberspace requirements.

**Principal Duties**

The incumbent's duties are:

1. Monitor and contribute to ACO Operational Requirements in support of SACEUR's Vision and Mission Set, providing specialist advice on INFOSEC and Alliance cryptography;
2. Provides advice to CyOC operational planners regarding strategic INFOSEC requirements and limitations;
3. Advise on strategic Cyberspace security risk management to support ACO CISOA;
4. Identifies cryptographic options and requirements supporting COMSEC, TRANSEC and all other cryptographic aspects relevant to NATO AOM;
5. Provide ACO interface for Cyberspace Security to NATO Bodies including NOS, NPAG, NPMA;
6. ACO lead in identifying operational requirements (Operational Requirements Authority) for ACO CIS Security including cryptography;
7. Plans for the continuing maturity of the Cyberspace Security and cryptographic capabilities of NATO;
8. Ensures coherence of operational requirements between Cyberspace Security related projects and all other Cyberspace related projects;
9. Utilizes information and requirements gathered from Policy documents and technical assessments and identifies operational requirements with regard to NATO's AOM mandate;
10. Liaises with NATO commands on operational requirements, manning levels, financial and technical resources required to protect NATO information;
11. Advises ACT on INFOSEC and Crypto operational requirements for capability development and the NDPP;
12. Support ACO strategic initiatives as tasked, including cryptographic modernization and FMN;
13. Closely coordinate with J6 Cyberspace / Service Management and NCIA to ensure a unified approach to cyberspace capabilities lifecycle management.
14. Participates in various committees and working groups.

**Special Requirements and Additional Duties**

The incumbent may be required to perform like duties elsewhere within the organisation as directed.
The incumbent is required to undertake operation deployments and/or TDY assignments both within and without NATO's boundaries.
The employee may be required to perform a similar range of duties elsewhere within the organisation at the same grade without there being any change to the contract:
- May be required to augment within the Cyberspace Operations Centre (CyOC) (may require shift work for the duration of the assignment);
- May be required to undertake operational assignment/secondment within CyOC or Comprehensive Crisis Management Operation Centre (CCMOC) (may require shift work for the duration of the assignment);
- May be required to serve as a Staff Officer within the CyOC;
- May be required to contribute to the daily and weekly CyOC reports;

- May be required to undertake operational assignment/secondment within Comprehensive Crisis Management Operation Centre (CCMOC) (may require shift work for the duration of the assignment);
- May be required to formally represent ACOS J6 Cyberspace at NATO meetings;
- May be required to formally represent ACOS J6 Cyberspace at Bi-SC and ACO meetings;
- May be required to make presentations of the SHAPE position on Cyber related subjects/issues on behalf ACOS J6 Cyberspace at NATO, Bi-SC and ACO meetings;
- May be required to make general SHAPE and Cyber related presentations, and provide Cyber training as part of SHAPE contribution to NATO Cyber Training, on behalf ACOS CYBER or as requested;
- May be required to participate in the activities of a Mission Network Secretariat a Mission Network where NATO is the Federator and/or Integrator;
- May be required to participate in the activities of the SCs Programme Management Office (PMO) for common funded programmes.

The work is normally performed in a Normal NATO office working environment.
Normal Working Conditions apply.
The risk of injury is categorised as: No risk / risk might increase when deployed.

**Essential Qualifications**

**a. Professional/Experience**

1. Minimum of 4 years of recent working experience on Cyberspace/CIS requirements matters in a large organization preferably having geographically dispersed elements.
2. Minimum 2 years experience in Cyberspace or Cyberspace related post supporting field operations or missions Experience should demonstrate a positive history of:

- planning and oversight of subordinate elements and colleagues in the delivery and employment of communications and information services and systems;
- developing and managing information exchange requirements and operational requirements;
- development of cyberspace activities within technology intensive programmes, particularly, reviewing, analysing, evaluating performance and accepting, conducting mid- and long-range information management/information technology (IM/IT) planning, programming, and budgeting; and/or allocating and distributing resources.

3. Minimum 2 years of experience developing national defence policies, plans, operations and decision making processes.

**b. Education/Training**

University Degree preferably in computer science, engineering disciplines, statistics or similar numerate discipline, operations research or related discipline but other university degrees such a political science, law, business will be considered and 4 years post related experience, or Higher Secondary education and completed advanced vocational training in that discipline leading to a professional qualification or professional accreditation with 5 years post related and 2 years functional related experience.

**c. Language**

English - SLP 3333 (Listening, Speaking, Reading and Writing)
NOTE: The work both oral and written in this post and in this Headquarters as a whole is conducted mainly in English.

**Desirable Qualifications**

**a. Professional Experience**

1) Project Management: PRINCE II or Project Management Professional (PMP) or internationally recognized equivalent certification;
2) Service Management: ITIL version 3 or internationally recognized equivalent certification;
3) IT Governance: COBIT5 or internationally recognized equivalent certification;
4) CIS Security: CISSP or CISM or internationally recognized equivalent certification.

**Attributes/Competencies**

**a. Personal Attributes**

Able to work in a multilateral environment.
The incumbent will need to display a high degree of professionalism, technical expertise, organisational, coordination and communication skills in the performance of his/her duties. The rapidly changing NATO / CYBERSPACE environment and increasingly constrained resource situation creates a requirement to solve numerous complex problems and challenges, which shall require the incumbent to draw upon a comprehensive ability to reason, analyse, act with persuasion and diplomacy. The post requires a self-starter, analytical and conceptual thinker. Team worker. Must impact/ influence activities within the various stakeholders' organization.

**b. Professional Contacts**

The incumbent needs to develop very good working relationship with other entities such as the NATO C3S, the NATO Office of Security, the NATO Office of Resources, Military Committee Agencies such as DACAN and SECAN, the Crypto producing Nations' NCSA, as well as Cyberspace Security staff within the subordinate Commands.

**c. Contribution To Objectives**

Establishes cryptographic Direction and Guidance for the NATO CIS Group and the subordinate Commands for Alliance Operations and Missions (AOM). Maintains close coordination with the NATO cryptographic community. Develops and maintains cryptographic subject matter expertise relating to Alliance Operations and Missions. Ensures ACO and AOM wide collaboration and compliance on all cryptographic aspects.

This post reports to OSC CYPX 0010 – Branch Head, OF-5.
There are no reporting responsibilities.

**REMARKS**

Duration of contract: Serving staff members will be offered a contract according to the NATO Civilian Personnel Regulations (NCPR). Newly recruited staff will be offered a definite duration contract of three years normally followed by an indefinite duration contract.

Given the COVID-19 situation the selection process for this post will proceed in phases at dates to be fixed according to the evolution of current limitations. On-line testing might be considered.

**HOW TO APPLY FOR A NATO CIVILIAN POST AT SHAPE**

Applications are to be submitted using NATO Talent Acquisition Platform (NTAP) (https://nato.taleo.net/careersection/2/jobsearch.ftl?lang-en). Applications submitted by other means (e.g. mail, e-mail, fax, etc) are not accepted.

NTAP allows adding attachments. A copy of the qualification/certificate covering the highest level of education required by the job description must be provided as an attachment.

**Essential information must be included in the application form**. Particular attention should be given to Education and Experience section of the application form. Each question should be answered completely. Expressions such as “please see attached CV, please see annex / enclosed document” or invitations to follow links to personal webpages are not acceptable and will be disregarded. All answers should be in English (preferably) or in French.

Shortlisted candidates will be requested to provide original documentary evidence and a set of copies supporting statements in their applications.

Current and past civilians working for NATO or any Coordinated Organization, shall indicate their last grade and step held (next to job title), and specify the name of employing NATO body or Coordinated Organization.

Remarks:
A) Only nationals from the 30 NATO member states can apply for vacancies at SHAPE.
B) Applications are automatically acknowledged within one working day after submission. In the absence of an acknowledgement please make sure the submission process is completed, or, re-submit the application.
C) Qualified redundant staff of the same grade interested in this post should inform this office, via their HR/Personnel Office by not later than vacancy’s closing date.
D) Candidates’ individual telephone, e-mail or telefax enquiries cannot be dealt with. All candidates will receive an answer indicating the outcome of their application.