SUPREME HEADQUARTERS ALLIED POWERS EUROPE

TALEO Job Number: 260226

Vacancy Number: G13/26

Post Number: OSC COOA 1050

Job Title: Analyst (SA in support of DCO)

NATO Grade: G11

Basic Monthly Salary (12 x per year): 5,234.63€, tax free

Closing Date: 10 March 2026

POST CONTEXT/POST SUMMARY

Supreme Headquarters Allied Powers Europe (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 directs monitors and coordinates all Cyberspace Operations (CO), Electronic Warfare (EW), Electro Magnetic Spectrum (EMS) activity and Communications and Information Systems (CIS) functional area activities and staff functions across ACO.

The Cyberspace Operations Centre (CyOC) is NATO's only Theatre Component for cyberspace, providing persistent, centralized and comprehensive cyberspace situational awareness, Command and Control (C2) and execution. The CyOC is within the SHAPE establishment but with different roles and responsibilities.

The Cyberspace Situational Awareness Branch is to provide the Cyberspace Operations Centre (CyOC)'s ability to incorporate the various aspects of cyberspace situational awareness, from all sources, which creates the theatre-wide cyberspace situational awareness, and integrate the cyberspace perspective into a single coherent dimension of the 360-degree approach.

The Cyberspace Situational Awareness Support Section analyses technical cyberspace vulnerability assessments and instigates consequence mitigating activities.

The incumbent is to define NATO's 'enhanced' Cyberspace SA and liaise with external stakeholders to achieve the to be drawn up Defensive Cyberspace Operations (DCO) requirements.

2. Principal Duties

The incumbent's duties are:

1) Support the planning, coordination, conduct and evaluation of Defensive Cyberspace Operations.
2) Define the role of CyOC's enhanced Cyberspace Situational awareness (SA) in DCO and drawing up Defensive Cyber Operations (DCO) requirements;
3) Initiate and oversee the design, implementation and maintenance of large-scale data proessing systems to collect data from various data sources;
4) Implement technical processes and business practices to transform collected data into meaningful and valuable information within the CyCOP;
5) Support the relations with cyberspace community of interest stakeholders at political, military and technical levels. Liaise with NATO Command Structure bodies (NCS), NATO Force Structure entities (NFS) and Partner Nations to assess cyberspace interoperability and readiness against ongoing missions or contingency plans;
6) Support the NATO Cyberspace risk management processes and analysis;
7) Oversee maintenance and review of cyberspace aspects of contingency plans for SACEUR's missions and activities across the Area of Responsibility (AOR);
8) Support development of the means to exploit the Cyberspace Situational Awareness and Decision Support System and other tools contributing to Cyberspace Situational Awareness;
9) Support strategic and operational decision making during and following a cyber event;
10) Author staff documents (e.g., point papers, PowerPoint presentations, etc.) as required;
11) Support CyOC strategic initiatives; taskings and other duties as required;
12) Support NATO Exercises as required.

3. Special Requirements and Additional Duties

The employee may be required to perform a similar range of duties elsewhere within the organization at the same grade without there being any change to the contract.

May be required to undertake operational assignment/secondment within SHAPE Comprehensive Crisis and Operations Management Centre (CCOMC) (may require shift work for the duration of the assignment);

- May be required to formally represent section head at meetings;

- May be required to make presentations of the SHAPE position on cyberspace-related subjects/issues on behalf of section head/branch head;

The work is normally performed in a Normal NATO office working environment.

Normal Working Conditions apply.

4. Essential Qualifications

a. Professional/Experience

1) Minimum of 1 year of experience with planning, overseeing or conducting military operations in joint HQ.
2) Minimum of 1 year in Computer Incident Response within a large international, governmental or military organization.
3) Minimum of 1 year in a military environment, with operational experience including experience in Operational Centre's of higher formations.
4) Experience and ability to develop extensive networks of cyber stakeholders.

5) Recent experience in defensive cyberspace operations.
6) University Degree and 1 year function related experience, or Higher Secondary education and completed advanced vocational training leading to a professional qualification or professional accreditation with 2 years post related experience. *The additional job specific qualifications and experience is described under Professional/Experience paragraph (4/a). In case of ambiguity the required job specific experience have priority over the standard education and training levels and experience described here.*
7) 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.*

5. Desirable Qualifications

a. Professional Experience

1) Previous experience in serving NATO and/or other military organization
2) Recent experience in cyber security incident handling

b. Education/Training

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) Analyst course (i.e. SANS and other similar)
4) CISSP, CISM and CRISC certifications and other similar
5) Course: JPL-OP-3555 - NATO Comprehensive Operations Planning Course (COPC)
6) Course: CCC-SM-32208 - NATO CIS Operational Planning
7) Course: COP-CD-31954 - Integrating Cyberspace Considerations into Operational Planning

6. Attributes/Competencies

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, team worker, analytical skills, Data visualization, and conceptual thinker. Must impact/ influence activities within the various stakeholders' organization.
• Professional Contacts: The incumbent needs to develop very good working relationship with other entities such as the J6, NCISG, NCIA, CTAB, CDT, , the NATO Office of Security (NOS), the NATO Office of Resources (NOR), and other various NATO Nations, as well as Cyberspace staff within the subordinate Commands.
• Contribution To Objectives: Support the operationalization of Cyber Defence. Maintains close coordination with the NATO Cyberspace community. Develops and maintains Defensive Cyber Operations subject matter expertise relating to Alliance Operations and Missions.
.

This post reports to:
OSC COOA 0010 - Section Head (Cyberspace Situational Awareness Support)/Principal Analyst (Strategic Information Sharing) - A4/G20

CONTRACT:

The successful candidate will fill this post as a Project Related NATO International Civilian (PLN) with a three-year definite duration contract within the NATO 2030 Agenda. On expiry of this term the PLN will be deleted or absorbed into the ceiling pending approval or will exceptionally be considered for extension.

REMARKS:

The salary will be the basic entry-level monthly salary defined by the NATO Grade of the post, which may be augmented by allowances based on the selected staff member's eligibility, and which is subject to the withholding of approximately 20% for pension and medical insurance contributions.

NATO is committed to diversity and inclusion, and strives to provide equal access to employment, advancement, and retention, independent of gender, age, nationality, ethnic origin, religion or belief, cultural background, sexual orientation, and disability. NATO welcomes applications of nationals from all member Nations.

Building integrity is a key element of NATO's core tasks. As an employer, NATO values commitment to the principles of integrity, transparency, and accountability in accordance with international norms and practices established for the defence and related security sector. Selected candidates are expected to be role models of integrity, and to promote good governance through ongoing efforts in their work.

We believe that all people are capable of great things. Because of this, we encourage you to apply even if you do not meet all of the criteria listed within this job description.

Applicants who prove to be competent for the post but who are not successful in this competition may be offered an appointment in another post of a similar nature, which might become vacant in the near future, albeit at the same or lower grade, provided they meet the necessary requirements.

ADDITIONAL INFORMATION

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. More information to be found on these links:

6 Tips for Applying to NATO
Application Process

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. The application should be in English. Shortlisted candidates will be requested to provide original documentary evidence and a set of copies supporting statements in their applications. After submitting your application, you will receive an acknowledgement of receipt of your application.

Remarks:
A) Only nationals from the 32 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) Candidates' individual telephone, e-mail or telefax enquiries cannot be dealt with. All candidates will receive an answer indicating the outcome of their application
D) NATO will not accept any phase of the recruitment and selection prepared, in whole or in part, by means of generative artificial-intelligence (AI) tools, including and without limitation to chatbots, such as Chat Generative Pre-trained Transformer (Chat GPT), or other language generating tools. NATO reserves the right to screen applications to identify the use of such tools. All applications prepared, in whole or in part, by means of such generative or creative AI applications may be rejected without further consideration at NATO's sole discretion, and NATO reserves the right to take further steps in such cases as appropriate