SUPREME HEADQUARTERS ALLIED POWERS EUROPE

TALEO Job Number: 250469

Vacancy Number: G29/24

Post Numbers: OSC OICA 0160 & OSC OICA 0170

Jobs Title: Cyber Intelligence Analyst

NATO Grade: 15

Basic Monthly Salary (12 x per year): 6,467.30 €, tax free

Closing Date: Monday 31 March 2025

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 Operations (OPS) Directorate delivers comprehensive situational awareness, enabling the identification of crises, and supports estimates, response options and planning. In monitoring NATO's current operations, it enables SACEUR's direction and guidance to be disseminated, ensuring coherent Joint Effects, whilst providing comprehensive assessments to NATO HQ.

The Division for Intelligence, J2, as part of SHAPE Operations Directorate, is the primary entity supporting SACEUR, SHAPE staff, and the ACO Intelligence Enterprise regarding situational awareness and situational understanding (SA and SU), Indications and Warning (I&W) and intelligence Operations.

SHAPE MDSIC is the analytical and collection hub for ACO intelligence. MDSIC is a central authority driving the SHAPE intelligence cycle and enabling timely, predictive strategic intelligence. It coordinates and delivers timely predictive intelligence to support senior leadership and decision makers on strategic level threats. It ensures adherence to the Intelligence Cycle at the strategic level to establish the permanent ACO SA and SU.

The Branch consists of five sections: J22 Collation, J22 Analysis, J22 Current Intelligence, J23 Current Intelligence operations, and J23 Future Intelligence Operations. The analytical hub of ACO intelligence, the J22 Analysis Section, coordinates intelligence production across the NATO intelligence enterprise. It consists in two cells:
- NATO Strategic Direction East Analysis Cell (NSD-E).
- NATO Strategic Direction South Analysis Cell (NSD-S).

Principal Duties

The incumbent's duties are:

1. As directed by the Section Head, conduct all-source strategic intelligence analysis focusing on cyber threats to ACO and its components in accordance with SACEUR's priorities.
2. Maintain technical knowledge of cyber threats and vulnerabilities and incorporate them in intelligence assessments to the Cyber Operations Centre (CyOC) and other cyber subject-matter experts (SMEs).
3. Mentor military intelligence analysts (cyber) in the subject matter expertise and tradecraft required to enable the military analysts to fulfil their intelligence analyst duties.
4. Coordinate intelligence requirements with the CyOC.
5. Direct and coordinate the production of strategic intelligence reports to ACO subordinate intelligence producers (including the NATO Intelligence Fusion Centre - NIFC) for cyber threats and provision of intelligence support in accordance with SACEUR's priorities.
6. As directed by the Section Head, provide intelligence briefs and assessments on designated cyber threats in accordance with SACEUR's priorities.
7. Liaise with relevant ACO, ACT, NATO HQ, NIFC, USCYBERCOM J2, USEUCOM J2, and other national organisations, by invitation or direction, regarding cyber threats intelligence production.
8. Maintain strategic situational awareness of NATO crisis response operations.
9. Support SHAPE J3, J35, and J5 with cyber-specific intelligence in support of crisis planning and other activities.
10. Provide support to NATO's comprehensive approach to crisis management operations.
11. Represent SHAPE at forums or meetings as directed by Section Head.
12. Other tasks as directed by the Section Head or Branch Head.

Special Requirements and Additional Duties

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.
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

The incumbent must:

1. Have at least 2 years in-depth experience in the area of cyber threat analysis, a cyber security operations centre, or defensive cyberspace operations.
2. Have at least 2 years of recent experience in activities that derive intelligence on cyber enabled threats (capabilities and intent of cyber threat actors) and cyber vulnerabilities to assist in developing cyber situational awareness.
3. Have knowledge or experience of open-source information, the intelligence cycle (to include collection and analysis processes) and large datasets.
4. Be familiar with strategic and geopolitical issues and challenges facing the Alliance.
5. Have excellent drafting skills and experience in preparing, writing, and briefing threat assessments, and intelligence reports.

b. Education/Training

University Degree preferably in the field of cyber security, information technology, security studies, data science or related studies and 2 years function related experience, or Higher

Secondary education and completed advanced vocational training leading to a professional qualification or professional accreditation with 4 years post related experience.

c. Language
English - SLP 3333 (Listening, Speaking, Reading and Writing)

Desirable Qualifications
a. Professional Experience
1. Experience from an international environment gained from deployment(s) to NATO operation(s).
2. Experience from liaising with international partners on strategic intelligence cooperation and exchanges.
3. Single-source experience from several intelligence fields of trade.
4. Knowledgeable or familiarity with the use of NATO-specific intelligence software.

b. Education/Training
1. Ethical Hacking Course
2. Basic Intelligence Systems Core Training (BISCT) provided by BICES GROUP EXECUTIVE or equivalent.
3. NATO Intelligence Functional Systems Training (NIFST) provided by NATO Communications and Information Academy (NCI Academy) or equivalent.

Attributes/Competencies
• Personal Attributes: The incumbent is responsible for analyzing complex problems based on incomplete information from multiple sources and disciplines of intelligence. This requires the application of critical thinking and structured analysis, constructive thinking, judgement, original thought and an imaginative approach to identify threats, vulnerabilities and opportunities, including possible courses of action (COAs), to provide timely, accurate and predictive intelligence assessments in support of SACEUR's mission. The incumbent is also responsible for mentoring military Intelligence Analysts (Cyber) in the subject matter expertise and tradecraft required to enable the military analysts to fulfil their intelligence analyst duties.

• Professional Contacts: The analyst is responsible for mentoring military Intelligence Analysts (Cyber) in the subject matter expertise and tradecraft required to enable the military analysts to fulfil their intelligence analyst duties as cyber specialists.
The incumbent works as part of a team of military and civilians of mixed ranges of rank and experience. Moreover, the incumbent is required to ad hoc teams of extremely varied skill sets and knowledge as part of broader intelligence teams, working with technical, operations and planning staff. The analyst is required to engage daily with senior officers up to OF-6 level and formally brief Flag Officers / General Officers on a regular basis. The analyst will also represent SHAPE with external organisations, making routine and regular engagement with counterparts at NATO HQ, NIFC and ACO commands. The analyst is also required to represent SHAPE at ACO, NATO and international conferences.

• Contribution To Objectives: The incumbent is essential to develop and maintain a professional and experienced intelligence analysis capability with the required subject matter expertise in cyber, technical cyber skills and ensure continuity beyond rotating military personnel in the Intelligence Analyst (Cyber) team. The expertise is required not only to support technical subject matter experts in the CyOC, but also to contribute to the wider intelligence effort of SHAPE J22 Branch in providing SACEUR and the SHAPE staff with intelligence assessment across all PMESII factors and all operational domains.

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.

Selected candidates will be invited to the Hirevue stage in mid-April 2025, and finalists will be contacted for an interview to be held in early June 2025.

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.

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.

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.

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.

More information to be found on these links:
6 Tips for Applying to NATO
Application Process

Shortlisted candidates will be requested to provide original documentary evidence and a set of copies supporting statements in their applications. Appointment is subject to obtaining a NS security clearance and a medical certificate.

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) 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) 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.