Applications are now invited for the post of Section Head (Programme Director Cyberspace Caps) – NATO Grade A-4, on the staff of the Supreme Headquarters Allied Commander Transformation (SACT), a NATO Strategic Command in Norfolk, Virginia, USA. Applications must be made on line: 
https://nato.taleo.net/careersection/2/jobsearch.ftl?lang=en

Closing date for applications: 30 October 2019

Location: Norfolk, Virginia, USA

- **Notes for candidates:** the candidature of NATO redundant staff at grade A-4 will be considered before any other candidates.
- **Notes for NATO Civilian Human Resources Managers:** If you have qualified redundant staff at grade A-4, please advise the HQ SACT Civilian HR Manager no later than the closing date.

Contract: Serving NATO International Civilian staff will be offered a contract in accordance with the NATO Civilian Personnel Regulations. Newly recruited staff will be offered a three year definite duration contract.

Salary: Starting basic salary (effective 1 January 2019) is 9,844.36 USD per month to which relevant allowances will be added.

For any queries, please contact the HQ SACT Recruitment Team at civilianpersonnel@act.nato.int
Post Context

ACT contributes to preserving the peace, security and territorial integrity of Alliance member states by leading, at Strategic Command level, Warfare Development required to enhance NATO’s posture, military structures, forces, capabilities and doctrines.

The Capability Development Directorate (CAPDEV) comprises two Divisions—Requirements and Capabilities. The Directorate supports SACT in his Capabilities Requirement Authority (CRA) role. It is responsible for a holistic through lifecycle Capability Development approach that infuses innovation and transformative efforts that are an integral part of the Warfare Development. This includes responsibilities for elicitation, development, capture and collection, quality review, traceability and visibility of capability requirements.

The Capabilities Division coordinates the development of capabilities from capability planning through acceptance and then disposal with the management entities, NATO Headquarters staff and the NATO Governance Structure. This entails synchronizing horizontally across capabilities to achieve coherent efforts and outcomes.

The Cyberspace Branch provides scientific, technical and operational expertise for the development and continuous improvement of modern and agile cyberspace capabilities. The Branch provides services and products through a competency-aligned structure to support appropriate product, programme coordination across DOTMLPFI lines of development throughout the lifecycle. The Branch supports cyber concepts development, capability requirements elicitation, architectures and federated interoperability.

The incumbent serves as the Section Head for Programme Director Cyberspace Capabilities/Principal Capability Systems Engineer section within the Cyberspace Branch.

Reports to: Branch Head (Cyberspace)/Portfolio Manager

Principal Duties: He/she will

a. Direct and supervise the work priorities of the cyberspace capabilities section, and coordinate cyberspace capability development activities within the section staff, other section heads, the branch head and the scientific/technical advisor.

b. Support the technical/scientific advisor in the development and maintenance of horizon scans, roadmaps, programs and associated technical contents, while supporting technical engagement activities and events.

c. Inform the development of the capability development part of the cyberspace Program of Work (PoW) and the associated resources (manpower and budget).

d. Coordinate and participate in the execution of activities to develop concepts, architectures, capability program plans, PoW activities, and contribute to organization and execution of exercises, experiments and the preparation of their respective products.
e. Manage and, when applicable, sponsor projects commissioned to other NATO organizations and Agencies, typically in the areas of capability definition, development, experimentation and operation.

f. Provide technical support to acquisition authorities during the procurement phase of proven solutions, and facilitate knowledge transfer to support capability employment once capabilities become operational.

g. Provide professional guidance and mentorship to section staff, and especially to newcomers to ensure rapid immersion and maximize opportunities for adoption of validated information system technologies and cyberspace operations solutions.

h. Ensure Lessons Learned (LL) is an integrated part of all Cyber activities. Ensure LL requests, planning, creation, collection, staffing and handling in accordance with the NATO LL Process is an integrated part of any activity.

i. Serve as a Capability Programme Director as needed.

j. Represent ACT on appropriate Cyber related committees, task force, panels and working groups.

**Essential Qualifications**

a. University Degree in Information technology, computer science, computer networking and communications., management information systems, accounting, economics, finance, business administration, public administration, operations research, project management or related discipline.

b. 4-6 years experience in cyberspace development activities, either in business or government.

c. 4-6 years experience in the management of heterogeneous technical, development and implementation engineering teams.

d. 4-6 years experience in management and technical leadership of engineering projects in the areas of requirements specification, architectural design, development, implementation, test and evaluation.

e. 4-6 years experience in systems specification, systems analysis and design, systems architectures, technology evaluation and insertion, technology procurement, prototyping, programming, integration, test, validation and in-service support.

f. Ability to work in team environments (both as a contributor and a leader).

g. Experience interacting/briefing with/to senior leadership at the Flag/General Officers level.

h. Excellent analytical, problem solving and verbal and written communication skills.

i. Expert-level certification in cyber security, at the level of CISSP or equivalent.

**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. Demonstrable experience in the employment of system engineering practices, including whole capability lifecycle from requirements elicitation to capability operation and decommissioning.

2. General knowledge of the organization and structure of NATO.

3. Experience working in the area of technology development and/or capability development.

b. Education/Training

Attributes/Competencies

• Managerial Responsibilities: This post has first-line managerial (reporting) responsibilities on the cyberspace capability section personnel (4 military, 2 civilians). This post requires as well the ability to understand and develop budgets, resource proposals and inform programmes of work, which calls for delegated responsibility over external work teams. This requirement calls for managerial skills, particularly in the areas of programme/project management, and resource management of heterogeneous individuals. The scope of influence for the incumbent is of several million Euros per year, for which he/she will exercise a significant amount of supervision, assessment and coordination.

• Professional Contacts: Daily and routine professional contact is required at the OF-5 level and above, with occasional interactions up to the OF-8, both inside and outside the command. Contact with contractors, senior staff and participation in briefings and internal review boards is undertaken regularly. The incumbent must have a keen sense of the boundaries of post authority and the direction that superior leadership would adopt in response to an evolving situation. The incumbent will be required to work along national representatives at the level of senior experts in multiple cyberspace fora.

• Contribution To Objectives: All activities within the Cyberspace Branch are directly linked to the Command’s Management Objectives Plan. Projects and Services are directly linked to Performance Indicators and Targets derived from Command Standing Objectives and Principal Activity Areas. The incumbent is often the first to notice an issue or shortfall requiring leadership and management intervention, and his/her work results may contribute to inform Command’s commitment to a particular long term strategy.

As ACT is focused on military capability transformation and the vast majority of modern capability is reliant upon some aspect of communications and information services, the capabilities developed will be instrumental in the collective output of NATO as a whole.
The performance of the incumbent shall have a substantial impact on the ability of the Alliance to operate in and through cyberspace, and will be directly determining the capabilities that SACEUR will have available for cyberspace.

He/she will be required to work in a normal office environment.