NOTIFICATION OF A CIVILIAN PERSONNEL REQUIREMENT
AT JOINT FORCE COMMAND BRUNSSUM HEADQUARTERS

Our Requirement:
Title: Staff Officer (Technological Threat Analyst) – NATO 2030
Grade: 15
Duty Location: Brunssum, The Netherlands
Requirement filling date: as soon as possible
Closing date for applications: 8 November 2026

Our organisation
Joint Force Command Brunssum (JFCBS) provides a Joint headquarters to plan, prepare and conduct operations to support NATO's core tasks, at the Joint Operational level, as directed by SACEUR. The Operations Directorate is responsible for directing, monitoring, coordinating and assessing operational functions and advising the Chief of Staff (COS) regarding all regionally focused operational activities.
The J3 Division is responsible to Operations Director for the implementation and oversight of operational plans, procedures and techniques to ensure effective Command & Control (C2) of assigned forces in Baseline Activities and Current Operations (BACO) through Crisis up to Maximum Level Effort (MLE).
The Force Protection Branch is responsible to ACOS J3 for aligning and synchronizing FP measures from threats, to include non-conventional threats and terrorism, as well as hazards in order to preserve FOA.
The Hybrid Effects Section (HES) is responsible to integrate JFCBS staff in understanding, mitigating and countering hybrid threats in JOA-Centre. This done by analyzing hybrid incidents across the JFCBS Area of Interest and presenting them to the HQ for developing situational understanding and ultimately, to provide multidomain responses or mitigation options to the Commander JFCBS in order to deter, defeat and exploit hybrid threats that pose a destabilizing risk to the Alliance and NATO nations.
The incumbent provides the technical knowledge required to analyze and manage technical information derived from different sources like technical exploitation reports derived from Unmanned Systems (UxS), Improvised Explosives Devised (IED) threats and others. The main focus will be the fast evolving technology associated to emerging and hybrid threats to Force Protection in order to support the identification of trends and new Tactics, Techniques and Procedures (TTPs).

The main duties of Staff Officer (Technological Threat Analyst) are to:
- Collect, combine and analyse related reports received from NATO Command and Force structure HQs, JFCBS J2, and other organization to make technological trend analysis regarding hybrid, C-UxS and C-IED etc in order to assess adversary`s TTPs.
- Set the blue picture for C-ET capabilities and assets. Identify capability gaps and other shortfalls related to C-UxS/C-IED operations within AOR.
- Permanently monitor the developments regarding emerging technologies and how it affects Force Protection.
- Support the Hybrid Effects Section regarding risk management and assessment cycle activities and propose suitable mitigation measures against hybrid and emerging threats.
- Participate and represent JFCBS HQ at Working Groups, Workshops and Exercises including Technical Interoperability Exercises (TIEs) when necessary.

- Represent the section/branch in NSIP activities and other procurement related processes such as Joint Requirements Review Board.
- Propose projects or/and support projects processes as a Subject Matter Expert in line with technological developments IOT counter emerging threat technologies to Force Protection.
- To lead, prioritize and coordinate Technical Exploitation for JFCBS with Nations and across Allied Command Operations.

The incumbent may be required to undertake deployments in support of military operations and exercises, and/or TDY assignments, both within and without NATO boundaries. Such operational deployment may exceed 30 days duration up to 183 days in any period of 547 days, and may be on short notice. For NATO International Civilian Staff, acceptance of an employment contract linked to this post constitutes agreement to deploy in excess of 30 days if required.

Required Qualifications are:

- English – good – NATO Standard Language Proficiency 3333.
  (Listening, Speaking, Reading and Writing) in accordance with NATO standard agreement (STANAG) 6001.
  NOTE: The work both oral and written in this post and in this Headquarters as a whole is conducted mainly in English.
- University Degree or equivalent in related field/subject
  (equivalent is Higher Secondary Education AND completed advanced vocational training in relevant field leading to a professional certification or accreditation).
- Minimum 2 years' professional experience with unmanned systems and/or technical exploitation including awareness of new technologies and providing analysis and provisional recommendations for future development.
- Knowledge of technology and equipment focusing on detecting, tracking, and mitigating hybrid and/or emerging threats.
- Minimum 2 years' professional experience in the implementation of new technologies to counter threats.

Desirable Qualifications are:

- Knowledge of Intelligence Community practices (reporting, analysis)
- Knowledge of adaptive manufacturing/3D printing (materials, programs, limitations)
- Knowledge of Drone/UAV (hobby flying, military flight or repair).
- Completion of relevant courses / trainings.

The successful candidate possesses following personal attributes:

- ✓ Good communication skills, both oral and written - able to communicate at all levels;
- ✓ Good interpersonal skills including tact and diplomacy;
- ✓ Ability to collaborate and work with various stakeholders;
- ✓ Ability to work under pressure;
- ✓ Ability to work independently;
- ✓ Ability to effectively work in a complex and international environment;
- ✓ Good problem-solving skills.

The successfully selected candidate must be able to obtain and maintain a security clearance and is required to pass a medical examination before an employment contract offer is released. The medical examination will take place with our medical consultant. It is required to determine if the recommended candidate is fit to perform the duties and is deployable to NATO's areas of operation.

This requirement is in support of the **NATO 2030** agenda.

The successful candidate will be offered a 3-year definite duration contract as NATO International Civilian (NIC); remuneration will be exempt from taxation and allowances will be applied whenever applicable.

For serving NATO international Civilians: contract will be offered in accordance with the NATO Civilian Personnel Regulations and the additional Nations' guidance (MCM-0061-2023 for NATO 2030 Project Linked NICs). The selected staff member will get a definite duration contract regardless of the current contract, with the exception of the case when they have more than 10 years of service, in which case they will receive an indefinite duration contract.

Due date for receipt of applications: **Sunday, 8 November 2026, 23:59.**

Candidates have to apply electronically in NATO Talent Acquisition Program: https://nato.taleo.net/careersection/2/jobsearch.ftl?lang=en

IMPORTANT:
Please be aware that a Selection Board will only assess the information provided in the job submission form including the answers to the pre-screening questions and description of your work experiences. Your answers must be comprehensive and stand alone; do not rely on attached documents for essential information *(Attachments are supporting documents and should not be referred to in the job submission).* For example, if a pre-selection question asks you to justify how you meet the minimum experience requirement, you must explicitly detail in the answer box *how* your experience directly aligns with, or exceeds, the stated requirement. Simply stating you meet the requirement is insufficient; provide concrete examples and quantifiable details. These experiences should also be included in the description of your work experiences.

Only candidates meeting ALL essential required qualifications will be considered and be assessed in competition with other candidates.

Please note that 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.