NATO
NORTH ATLANTIC TREATY ORGANIZATION
INTERNATIONAL STAFF

OTAN
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
SECRÉTARIAT INTERNATIONAL

VACANCY NOTIFICATION/ NOTIFICATION DE LA VACANCE DU POSTE

Officer, Cyber Security – 261197

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 01-Sep-2026
Salary (Pay Basis): 8,273.12 (EUR) Monthly
Grade NATO Grade G17/G20
Clearance Level NS

Description

1. SUMMARY

The Joint Intelligence and Security Division (JISD) has two main missions: to provide strategic intelligence to NATO HQ decision makers and to protect NATO's personnel, information, and physical assets. JISD's Intelligence pillar, comprised of both military and civilian personnel, is responsible for ensuring the situational awareness of the North Atlantic Council (NAC), the Military Committee (MC) and the senior-level decision-makers on strategic issues of concern. Its functional areas address intelligence analysis and production, intelligence policy, and intelligence capability development. JISD's Security pillar is responsible for the overall coordination of NATO security among member Nations, NATO civil and military bodies as well as International Organizations and partner countries with which NATO cooperates. It is also responsible for the security of the NATO Headquarters (HQ), its personnel, information, physical assets, and for the protection of the Secretary General.

Within the JIDS's Security and Policy Oversight Branch, the Officer is responsible for the security accreditation of the NATO CIS and the maintenance of the Cyber Security policy framework. They will carry out the Cyber Security audits in NATO bodies as well as security surveys in non-NATO entities.

This position requires flexibility to travel occasionally.

2. QUALIFICATIONS AND EXPERIENCE

The incumbent must:

- possess a university degree, or an equivalent level of qualification, in cyber security, information systems or related subject;
- have 5 years of experience relevant to the position;
- have demonstrable experience in Cloud, and Edge Computing and its deployment models;
- possess excellent communication skills and strong analytical capabilities, including the ability to explain complex situations in a clear and concise manner; and
- possess the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; I ("Beginner") in the other.

The following would be considered an advantage:

- deep understanding in one or more of the following concepts: DevSecOps, Artificial Intelligence, Zero Trust, Data Centric Security, Software-Defined Networking, or Service Oriented Architecture;
- experience in the area of Vulnerability Assessment or Security Risk Assessment/ Management; or
- ability to assess incident findings or review threat hunting activities.

3. MAIN ACCOUNTABILITIES

Project Management: Coordinate cyber security audits and evaluations as directed by the Section Head including the follow-up on the audit findings. Advise on the planning and implementation of cyber security provisions in projects and its involvement with industry. Collaborate with other internal branches and divisions to assess the Cyber Security posture of NATO networks. Participate in security surveys with international partners and organisations. Draft clear policies, directives and guiding documents on Cyber Security, as required.

Expertise Development: Serve as a trusted advisor providing guidance to NATO Nations, NATO civil and military bodies, partner nations and international organisations. Proactively keep up-to-date with the latest cyber security trends, threats and technologies. Lead the education and training initiatives on security accreditation for relevant stakeholders.

Knowledge Management: Analyse briefings, discussions and investigations to assess the security programmes in place in NATO nations, NATO civil and military bodies, and non-NATO nations / international organisations. Update and maintain the Information and Knowledge Repository for increased situational awareness.

Stakeholder Management: Mediate between diverse stakeholder with different interests to build consensus. Translate complex technical information into comprehensive reports for national and/or security authorities. Represent the Cyber Security Section on the topics of Security Accreditation and Cyber Security to boards, committees and working groups, as directed by the Head, Cyber Security.

Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

Reporting Line: The Officer reports to the Head, Cyber Security.

Interactions: The incumbent will work closely with the other Officers in the Section, senior government and military personnel in NATO and partner nations, NATO civil and military bodies, and non-NATO nations and organisations.

Direct reports: N/A
Indirect reports: N/A

5. COMPETENCIES

The incumbent must demonstrate:

- Achievement: creates own measures of excellence and improves performance.
- Analytical Thinking: sees multiple relationships.
- Change Leadership: expresses vision for change.
- Impact and Influence: uses indirect influence.
- Initiative: is decisive in a time-sensitive situation.
- Organizational Awareness: understands the Organisation's politics.
- Teamwork: solicits inputs and encourages others.

6. CONTRACT

Contract to be offered to the successful applicant (if non-seconded): Definite duration contract of three years; possibility of renewal for up to three years, during which the incumbent may apply for conversion to an indefinite duration contract.

Contract clause applicable:
In accordance with the contract policy, this is a post in which turnover is desirable for political reasons in order to be able to accommodate the Organisation's need to carry out its tasks as mandated by the Nations in a changing environment, for example by maintaining the flexibility necessary to shape the Organisation's skills profile, and to ensure appropriate international diversity.
The maximum period of service foreseen in this post is 6 years. The successful applicant will be offered a 3-year definite duration contract, which may be renewed for a further period of up to 3 years. However, according to the procedure described in the contract policy the incumbent may apply for conversion to an indefinite contract during the period of renewal and no later than one year before the end of contract.
If the successful applicant is seconded from the national administration of one of NATO's member States, a 3-year definite duration contract will be offered, which may be renewed for a further period of up to 3 years subject also to the agreement of the national authority concerned. The maximum period of service in the post as a seconded staff member is six years.
Serving staff will be offered a contract in accordance with the NATO Civilian Personnel Régulations.

NOTE: Irrespective of previous qualifications and experience, candidates for twin-graded posts will be appointed at the lower grade. These circumstances are described in the IS directive on twin-graded posts.

7. USEFUL INFORMATION REGARDING APPLICATION AND RECRUITMENT PROCESS

Please note that we can only accept applications from nationals of NATO member countries. Applications must be submitted using e-recruitment system, as applicable:

- For NATO civilian staff members only: please apply via the internal recruitment portal (link);
- For all other applications: www.nato.int/recruitment

Before you apply to any position, we encourage you to click here and watch our video providing 6 tips to prepare you for your application and recruitment process.

Do you have questions on the application process in the system and not sure how to proceed? Click here for a video containing the information you need to successfully submit your application on time.

When submitting your application, please ensure that your Taleo Candidate Profile is updated and that your CV is correctly uploaded in the Taleo attachments section.

More information about the recruitment process and conditions of employment, can be found at our website (http://www.nato.int/cps/en/natolive/recruit-hq-e.htm)
Appointment will be subject to receipt of a **security clearance** (provided by the national Authorities of the selected candidate), approval of the candidate's **medical file** by the NATO Medical Adviser, verification of your study(ies) and work experience, and the successful completion of the **accreditation** and notification process by the relevant authorities.

NATO will not accept any phase of the recruitment and selection prepared, in whole or in part, by means of reference documents without proper quotes (plagiarism), or any tools available on internet, including but not limited to translation facilities, or generative artificial-intelligence (AI) 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 tools will be rejected without further consideration, and NATO reserves the right to take further steps in such cases as appropriate.

8. ADDITIONAL INFORMATION

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, and strongly encourages women to apply.

NATO is committed to fostering an inclusive and accessible working environment, where all candidates living with disabilities can fully participate in the recruitment and selection process. If you require reasonable accommodation, please inform us during your selection process.

Candidates will be required to provide documented medical evidence to support their request for accommodation.

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.

Due to the broad interest in NATO and the large number of potential candidates, telephone or e-mail enquiries cannot be dealt with.

Applicants who are not successful in this competition may be offered an appointment to another post of a similar nature, albeit at the same or a lower grade, provided they meet the necessary requirements.

The nature of this position may require the staff member at times to be called upon to travel for work and/or to work outside normal office hours.

The organization offers several work-life policies including Teleworking and Flexible Working arrangements (Flexitime) subject to business requirements.

Please note that the International Staff at NATO Headquarters in Brussels, Belgium is a non-smoking environment.

For information about the NATO Single Salary Scale (Grading, Allowances, etc.) please visit our website. Detailed data is available under the Salary and Benefits tab.

NATO does not charge any application, processing, training, interviewing, testing or other fee in connection with the application or recruitment process. For more info please click here.

Administratrice/Administrateur (Cybersécurité) - 261197

Emplacement principal : Belgique-Bruxelles
Organisation : OTAN SI
Horaire : Temps plein
Date de retrait : 01-sep-2026
Salaire (Base de paie) : 8,273.12 Euro (EUR) Mensuelle
Grade NATO Grade G17/G20
Niveau de l'habilitation de sécurité NS

Description :

1. RÉSUMÉ

La Division civilo-militaire Renseignement et sécurité (JISD) a deux missions principales : fournir du renseignement stratégique aux décideurs du siège de l'OTAN, et protéger le personnel, les informations et les biens matériels de l'Organisation. Le pilier « renseignement » de la JISD, composé de militaires et de civils, est chargé de fournir au Conseil de l'Atlantique Nord, au Comité militaire et aux décideurs de haut niveau les éléments d'information dont ils ont besoin au sujet des enjeux stratégiques qui intéressent l'OTAN. Ses domaines de compétence sont l'analyse et la production du renseignement, ainsi que l'élaboration des politiques et le développement des capacités en matière de renseignement. Le pilier « sécurité » de la JISD coordonne l'ensemble des questions relatives à la sécurité à l'OTAN, et travaille à cet effet avec les pays membres et les organismes civils et militaires de l'OTAN, ainsi qu'avec les organisations internationales et les pays partenaires avec lesquels l'OTAN coopère. Il s'occupe également de la sécurité du siège de l'Organisation et de son personnel, de la sécurité des informations et des biens matériels de l'OTAN, ainsi que de la protection de la/du secrétaire général(e).

Au sein de la Branche Supervision de la politique et de la sécurité, la personne titulaire du poste est responsable de l'homologation de sécurité des Systèmes d'information et de communication (SIC) de l'OTAN et de la tenue à jour du cadre relatif à la politique de cybersécurité de l'OTAN. Elle procède à des audits de cybersécurité dans des organismes OTAN, ainsi qu'à des visites d'examen dans des entités non OTAN.

Elle doit être disposée à effectuer des déplacements occasionnels.

2. QUALIFICATIONS ET EXPÉRIENCE

La personne titulaire du poste doit :

- posséder un diplôme universitaire – ou une qualification de niveau équivalent – dans le domaine de la cybersécurité ou des systèmes d'information, ou dans une discipline apparentée ;
- avoir cinq ans d'expérience dans un domaine d'activité pertinent ;
- avoir une expérience probante de l'informatique en nuage (*cloud*), de l'informatique en périphérie (*edge*) et de leurs modèles de déploiement ;

- avoir d'excellentes aptitudes à la communication et de solides compétences analytiques, et être capable d'expliquer de façon claire et concise des situations complexes ;
- avoir au minimum le niveau de compétence V (« avancé ») dans l'une des deux langues officielles de l'OTAN (anglais/français), et le niveau I (« débutant ») dans l'autre.

Seraient considérées comme autant d'atouts :

- une bonne connaissance d'au moins un des concepts suivants : DevSecOps, intelligence artificielle, confiance zéro, sécurité centrée sur la donnée, mise en réseau définie par logiciel, architecture orientée services ;
- une expérience dans le domaine de l'appréciation de la vulnérabilité ou de l'évaluation/la gestion des risques de sécurité ;
- la capacité d'évaluer des conclusions d'incident ou de faire le bilan d'activités relevant de la chasse aux menaces informatiques.

3. RESPONSABILITÉS PRINCIPALES

Gestion de projet – Coordonne des audits et des évaluations de cybersécurité selon les instructions de la/du chef de la Section, et assure le suivi des conclusions d'audit. Donne des conseils pour la planification et la mise en application des dispositions de cybersécurité dans le cadre de projets, et notamment de projets faisant intervenir le secteur privé. Travaille de concert avec d'autres branches internes et avec les autres divisions lorsqu'il s'agit d'évaluer la posture de cybersécurité des réseaux de l'Organisation. Participe à des visites d'examen avec des partenaires et organisations à l'échelle internationale. Rédige de façon claire des politiques, des directives et des documents d'orientation consacrés à la cybersécurité, selon les besoins.

Développement de l'expertise – Agit en tant que partenaire de confiance lorsqu'il s'agit de remettre des avis et des orientations aux pays membres et aux organismes civils et militaires de l'OTAN, ainsi qu'aux pays partenaires et à des organisations internationales. Se tient informé(e) des dernières tendances, menaces et technologies en matière de cybersécurité. Pilote des initiatives de formation théorique et pratique sur l'homologation de sécurité à l'intention des parties prenantes concernées.

Gestion des connaissances – Analyse des exposés, des débats et des recherches dans le but d'évaluer les programmes de sécurité en place dans les pays membres et les organismes civils et militaires de l'OTAN, ainsi que dans des pays non OTAN et d'autres organisations internationales. Actualise et tient à jour un référentiel d'information et de connaissance devant permettre d'améliorer la perception de la situation.

Gestion des parties prenantes – Assure la médiation entre diverses parties prenantes ayant différents intérêts dans une optique de consensus. Traduit des informations techniques complexes en rapports circonstanciés à l'intention des autorités nationales et/ou de sécurité. Représente la Section Cybersécurité pour les questions d'homologation de sécurité et de cybersécurité auprès de bureaux, de comités et de groupes de travail, selon les instructions données par la/le chef de la Section Cybersécurité.

S'acquitte de toute autre tâche en rapport avec ses fonctions qui pourrait lui être confiée.

4. STRUCTURE ET LIAISONS

Hiérarchie – La personne titulaire du poste relève de la/du chef de la Section Cyberdéfense.

Relations de travail – Elle est en contact étroit avec les autres administrateurs de la Section, avec de hauts responsables – gouvernementaux ou militaires – des pays de l'OTAN et des pays partenaires, avec des organismes civils et militaires de l'OTAN et avec des entités et organisations non OTAN.

Nombre de subordonné(e)s direct(e)s : s.o.
Nombre de subordonné(e)s indirect(e)s : s.o.

5. COMPÉTENCES

La personne titulaire du poste doit faire preuve des compétences suivantes :

- Recherche de l'excellence : crée ses propres critères d'excellence et améliore les performances.
- Réflexion analytique : discerne les relations multiples.
- Promotion du changement : exprime une vision pour le changement.
- Persuasion et influence : a recours à des techniques d'influence indirectes.
- Initiative : fait preuve de décision dans les situations où il faut agir sans attendre.
- Compréhension organisationnelle : comprend la structure de l'Organisation.
- Travail en équipe : sollicite des contributions et encourage les autres.

6. CONTRAT

Contrat proposé (hors détachement) : contrat d'une durée déterminée de trois ans ; renouvelable pour une période de trois ans maximum, au cours de laquelle le/la titulaire pourra demander qu'il soit transformé en contrat de durée indéterminée.

Clause contractuelle applicable :
Conformément à la politique des contrats, il s'agit d'un poste auquel il est souhaitable, pour des raisons politiques, d'assurer une rotation de manière à pouvoir répondre au besoin qu'a l'Organisation d'exécuter les tâches qui lui sont confiées par les pays dans un environnement en constante évolution, notamment en préservant la souplesse nécessaire à l'adaptation de son profil de compétences, et de veiller au degré de diversité approprié à son caractère international.
La durée de service maximale prévue à ce poste est de six ans. La personne retenue se verra offrir un contrat d'une durée déterminée de trois ans, qui pourra être reconduit pour une période de trois ans maximum. Toutefois, conformément à la procédure décrite dans la politique des contrats, elle pourra demander, au plus tard un an avant l'expiration de la deuxième période, que son contrat soit transformé en contrat de durée indéterminée.
Si la personne retenue est détachée de l'administration d'un État membre de l'OTAN, elle se verra offrir un contrat d'une durée déterminée de trois ans, qui, sous réserve de l'accord des autorités nationales concernées, pourra être reconduit pour une période de trois ans maximum. À ce poste, la durée de service d'un agent détaché n'excède pas six ans.
Les agents en fonction se verront offrir un contrat conforme aux dispositions du Règlement du personnel civil de l'OTAN.

NOTE: Quelles que soient leurs qualifications et leur expérience, les candidat(e)s retenu(e)s pour un poste à grade jumelé sont nommé(e)s au grade le moins élevé. Ces conditions sont décrites dans la directive du Secrétariat international relative aux postes à grades jumelés.

7. INFORMATIONS UTILES CONCERNANT LA PROCÉDURE DE CANDIDATURE ET DE RECRUTEMENT

On notera que seules les candidatures de ressortissant(e)s de pays de l'OTAN pourront être acceptées. Les candidatures doivent être soumises comme suit :

- pour les seuls agents civils de l'OTAN : via le portail de recrutement interne (lien) ;
- pour toutes les autres candidatures : via le lien www.nato.int/recruitment.

Il est recommandé de commencer par regarder ici une vidéo proposant six conseils destinés à aider les candidat(e)s à préparer leur dossier.

En outre, on trouvera ici une vidéo expliquant la marche à suivre sur le portail pour introduire son dossier de candidature et s'assurer de sa réception par l'OTAN dans les délais fixés.

Lors de la soumission de votre candidature, veuillez vous assurer que votre profil de candidat Taleo est à jour et que votre CV est correctement téléchargé dans la section des pièces jointes de Taleo.

On trouvera de plus amples informations concernant le processus de recrutement et les conditions d'emploi sur le site web de l'OTAN (http://www.nato.int/cps/fr/natolive/recruit-hq-e.htm).
La nomination se fera après vérification des diplômes et des antécédents professionnels de la/du candidat(e) retenu(e) et sous réserve de la délivrance d'une **habilitation de sécurité** par les autorités du pays dont la/le candidat(e) retenu(e) est ressortissant(e), de l'approbation de son **dossier médical** par la/le médecin-conseil de l'OTAN et de l'achèvement du processus d'**accréditation** et de notification par les autorités compétentes.

Dans le cadre de ses procédures de recrutement et de sélection, l'OTAN n'acceptera aucune réponse qui aura été produite, en tout ou en partie, sur la base de documents de référence non explicitement cités (plagiat) ou au moyen d'outils disponibles sur Internet, y compris, entre autres, d'outils de traduction ou d'outils d'intelligence artificielle (IA) générative. Elle se réserve le droit de vérifier si la personne candidate a eu recours à de tels outils. L'OTAN pourra rejeter sans autre examen tout dossier de candidature élaboré, en tout ou en partie, à l'aide de ces outils. Elle se réserve également le droit de prendre toute autre mesure qu'elle jugerait nécessaire.

8. INFORMATIONS COMPLÉMENTAIRES

L'OTAN est déterminée à promouvoir la diversité et l'inclusion, et elle s'attache à assurer l'égalité de traitement en matière d'emploi, d'avancement et de fidélisation indépendamment de toute considération liée au genre, à l'âge, à la nationalité, à l'origine ethnique, à la religion ou aux croyances, à la culture, à l'orientation sexuelle, ou au handicap. L'Organisation examinera les candidatures de ressortissant(e)s de tous les pays membres, et encourage vivement les femmes à postuler.

Attachée aux principes d'inclusivité et d'accessibilité, l'OTAN prend toutes les dispositions nécessaires pour que les personnes porteuses d'un handicap puissent participer au processus de recrutement. Si vous avez besoin d'aménagements spécifiques, veuillez le préciser pendant votre processus de sélection.

Toute demande d'aménagement doit être étayée par une attestation médicale.

Le développement de l'intégrité est un élément clé des tâches fondamentales de l'Alliance. En tant qu'employeur, l'OTAN attache une grande importance au respect des principes d'intégrité, de transparence et de redevabilité, conformément aux normes et aux pratiques internationales établies pour le secteur de la défense et de la sécurité s'y rapportant. Les candidat(e)s sélectionné(e)s doivent être des modèles d'intégrité et s'employer en permanence à promouvoir la bonne gouvernance dans le cadre de leur travail.

En raison du vif intérêt suscité par l'OTAN et du nombre élevé de candidatures potentielles, il ne pourra pas être donné suite aux demandes de renseignements adressées par téléphone ou par courrier électronique.

Les candidat(e)s qui ne seront pas retenu(e)s pour ce poste pourront se voir offrir un poste analogue, au même grade ou à un grade inférieur, pour autant qu'ils/elles remplissent les conditions requises.

De par la nature du poste, le/la titulaire peut parfois être amené(e) à voyager pour le travail et/ou à travailler en dehors des heures normales de service.

L'Organisation, en application de plusieurs politiques sur l'équilibre entre vie professionnelle et vie privée, propose notamment des possibilités de télétravail et d'horaire flexible sous réserve des exigences liées à la fonction.

Le Secrétariat international de l'OTAN est un environnement sans tabac.

Pour en savoir plus sur l'échelle unique de rémunération mise en place à l'OTAN (grades, indemnités, etc.), veuillez consulter notre site web. Des informations détaillées sont fournies sous l'onglet Salaires et allocations.

L'OTAN ne vous réclamera jamais de frais dans le cadre d'une procédure de recrutement, que ce soit pour le dépôt de votre candidature, le traitement de votre dossier, les ressources mises à disposition, les entretiens, les épreuves, ou autre. Pour plus d'informations, cliquez ici.