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, Defensive Cyberspace Operations - 260031

Primary Location: Mons-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 22-Feb-2026
Salary (Pay Basis): 6,713.06 (EUR) Monthly
Grade NATO Grade G15
Clearance Level NS

Description

1. SUMMARY

The Cyber and Digital Transformation Division (CDT) oversees all aspects of cyber and digital transformation across the entire NATO Enterprise, advancing the Alliance's agenda on those issues. As a fully integrated civilian-military Division, it combines the strategic insight of the International Staff (IS) with the operational expertise of the International Military Staff (IMS), enabling coherent, credible, and actionable advice to NATO's senior decision-making bodies. CDT is structured around three core directorates: Strategy and Policy, Capability Development and Plans, and Readiness and Operations.

The Readiness and Operations Directorate ensures that NATO's digital and cyber capabilities are operationally viable, exercised, and maintained at readiness. It serves as the primary link with the NATO Integrated Cyber Defence Centre (NICC), ensuring the execution of the NICC Enterprise Coordinator function, working seamlessly across NATO HQ and SHAPE. In July 2024, Allies agreed to establish the NICC to enhance the protection of NATO and Allied networks, and the implementation of cyberspace as a domain of operations. Bringing together civilian and military personnel from across the NATO Enterprise, Allies and industry, the NICC enhances situational awareness, ensures collective protection and defence, and integrates operational activities.

Within the Directorate, the Cyber Operations Section (CYOP) combines two core functions, comprising the provision of authoritative risk guidance to the NATO Enterprise CIS Operational Authority (ECISOA) as the Single Point of Accountability (SPA) for cybersecurity, and the provision of a strong liaison element with key cybersecurity stakeholders (ACO, ACT and NCIA among all). The Section ensures that NATO's cyber operations reinforce Alliance-wide efforts through the co-leadership of Defensive

Cyberspace Operations (DCO), together with the NATO Cyberspace Operations Centre (CyOC). The Section supports the planning, coordination and execution of DCO on NATO networks through the DCO Planning and Coordination Cell (DPCC).

The incumbent is located in NICC/SHAPE, Mons with a dual reporting line to both the Senior Section Member in SHAPE and to the Head CYOP, and is responsible for supporting the management of the DCO lifecycle, including the proposal, planning, conduct, assessment and follow-up phases defined in the DCO process, and ensuring appropriate and timely communication and cooperation amongst the relevant NATO Enterprise stakeholders (CyOC, JISD, and NCIA) within and through the NICC. The incumbent provides support to all DPCC meetings, facilitating discussions and contributing to the decision-making process. The incumbent also supports the development and realization of DCO activities in close coordination with the cyber incident management and cyber risk management processes.

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- possess a university degree, or an equivalent level of qualification, from an institute of recognised standing, preferably in information and communications technology or a cybersecurity related discipline;
- have at least 3 years of experience in cybersecurity, preferably in a large organisation;
- possess experience in developing and implementing processes and procedures in support of cybersecurity operations, and experience in program or project planning;
- have good knowledge of the principles, policy and procedures governing cybersecurity in a large organization, preferably in a military context;
- be able to prepare and deliver clear and concise presentations and reports to both technical and non-technical audiences;
- demonstrate strong stakeholder's management skills;
- possess good analytical, problem solving, and verbal and written communication skills;
- possess the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; I ("Beginner") in the other;
- be flexible and willing to work outside of normal office hours and able and willing to travel when required, including weekly travel to NATO HQ.

DESIRABLE

The following are considered an advantage:

- understanding of NATO's organization, security policies and directives;
- cybersecurity certifications such as CISSP, CCSP, CISM;
- a post-graduate degree in cybersecurity;
- a good knowledge and experience planning, coordinating and executing advanced cybersecurity operations in federated environments,
- experience with cybersecurity procedures such as threat hunting, adversary

emulation, red teaming and vulnerability management;
- a good understanding of current and emerging cybersecurity technologies and how enterprises are employing them to drive digital business;
- experience in cyber incident management and cyber risk management best practices and processes;
- knowledge of NATO's cybersecurity environment.

3. MAIN ACCOUNTABILITIES

Policy Development

Contribute to the development of policies, directives, guidance and administrative documents relating to DCO. Provide advice to the CYOP Section Head on DCO policies, activities, processes and procedures. Provide advice and guidance on DCO to NICC stakeholders, NATO Nations, NATO civil and military bodies, partner nations and international organisations. Develop high-level strategic documents and advice to support the DCO processes and procedures carried out through the NICC.

Planning and Execution

Propose, plan, keep oversight on, assess and follow-up DCO activities in close coordination with the relevant NATO Enterprise stakeholders. Coordinate DCO activities within the context of the NICC. Identify, develop and test new processes in support of DCOs.

Expertise Development

Identify cybersecurity capabilities within the NATO Enterprise, as well as new ones to be developed in support of DCO. Maintain full understanding of project and programme plans, provide expertise and support in the resolution of issues. Keep abreast with the latest technology developments in the incumbent's areas of responsibilities, and provide appropriate advice. Propose updates and improvements based on lessons identified from real life experience and exercises.

Stakeholder Management

Establish and maintain a network of relations with key civilian and military experts in the NICC, including working seamlessly across SHAPE and NATO HQ. Develop close cooperation and working relations with the relevant NATO stakeholders involved in the lifecycle of Enterprise security processes and practices, with a focus on DCO. Be comfortable in supporting and interacting with executive/senior-level boards and committees.

Knowledge Management

Draft background briefs, progress reports, prepare presentations, and other items for high- level meetings. Contribute to effective information sharing with the relevant NATO bodies and stakeholders (e.g. NATO Cyber Risk management Group (CRMG), the NATO Board of CISOA (BCISOA), etc.) that may contribute to and support DCO activities. On the basis of briefings, discussions and operational activities, provide advice on evolving security programmes in NATO nations, NATO civilian and military bodies, and non-NATO entities.

Financial Management

Support the management of a predetermined budget for assigned projects.

4. INTERRELATIONSHIPS

As CDT's presence within the NICC increases, the incumbent reports to the most senior Section member permanently located in SHAPE and through him/her to the Head, Cyber Operations Section and NICC Enterprise Coordination Office. The incumbent also replaces the Senior Officer in SHAPE when needed. The incumbent works in close cooperation with all NICC stakeholders and has a technical dependence from the DCO team leader in the Cyber Ops Section.

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

5. COMPETENCIES

The incumbent must demonstrate:

- Analytical Thinking: Sees multiple relationships.
- Flexibility: Adapts to unforeseen situations.
- Impact and Influence: Takes multiple actions to persuade.
- Initiative: Is decisive in a time-sensitive situation.
- Organizational Awareness: Understands organisational climate and culture.
- Teamwork: Cooperates.

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.

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.

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 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.

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 (opérations défensives dans le cyberespace) - 260031

Emplacement principal : Mons-Bruxelles
Organisation : OTAN SI
Horaire : Temps plein
Date de retrait : 22-fev-2026
Salaire (Base de paie) : 6,713.06 Euro (EUR) Mensuelle
Grade NATO Grade G15
Niveau de l'habilitation de sécurité NS

Description :

1. RÉSUMÉ

La Division Cyber et transformation numérique (CDT) supervise tous les aspects relatifs au cyber et à la transformation numérique dans l'ensemble de l'entreprise OTAN et fait avancer les travaux de l'Alliance sur ces questions. En tant qu'entité civilo-militaire pleinement intégrée, elle combine l'acuité stratégique du Secrétariat international (SI) et l'expertise opérationnelle de l'État-major militaire international (EMI), ce qui lui permet de formuler des avis cohérents, crédibles et exploitables à l'intention des organes décisionnels de haut niveau de l'OTAN. La Division CDT est divisée en trois grandes directions : la Direction Stratégie et politique, la Direction Planification et développement des capacités et la Direction Préparation et opérations.

La Direction Préparation et opérations a pour rôle de veiller à ce que les capacités numériques et cyber de l'OTAN soient viables sur le plan opérationnel, qu'elles fassent l'objet d'exercices et que leur état de disponibilité opérationnelle soit maintenu. Elle assure la liaison principale avec le Centre OTAN intégré pour la cyberdéfense (NICC), assume la fonction de coordonnateur NICC au niveau de l'entreprise OTAN et exerce ses activités de manière flexible entre le siège de l'Organisation et le SHAPE. En juillet 2024, les Alliés sont convenus d'établir le NICC afin d'améliorer la protection des réseaux de l'Organisation et de ses pays membres, et de tirer davantage parti du cyberespace comme domaine d'opérations. Réunissant des civils et des militaires venant de toute l'entreprise OTAN et des pays de l'Alliance, ainsi que des experts du privé, le NICC contribue à améliorer la connaissance de la situation et à assurer la protection et la défense collectives, et s'occupe également des activités opérationnelles.

Relevant de la Direction Préparation et opérations, la Section Opérations cyber remplit deux grandes fonctions : elle fournit, en sa qualité d'autorité unique en matière de cybersécurité, des orientations faisant foi sur les risques à l'autorité d'emploi des SIC (CISOA) de l'entreprise OTAN, et elle assure une liaison solide avec les parties prenantes jouant un rôle clé en matière de cybersécurité (Commandement allié Opérations, Commandement allié Transformation, Agence OTAN d'information et de communication, etc.). La Section, qui codirige les opérations défensives dans le cyberspace (DCO) avec le Centre des cyberopérations de l'OTAN (CyOC), veille à ce que les cyberopérations menées par l'OTAN contribuent aux efforts fournis à l'échelle de l'Alliance, et elle assure également la planification, la coordination et l'exécution des DCO sur les réseaux de

l'OTAN au travers de la Cellule Planification et coordination des DCO (DPPC).

La personne titulaire du poste à pourvoir exerce ses fonctions au NICC, dans les bâtiments du SHAPE, à Mons. Relevant à la fois de l'agent le plus haut placé dans la hiérarchie de la Section au SHAPE et de la/du chef de la Section Opérations cyber, elle contribue à la gestion du cycle de vie des DCO, notamment des phases de proposition, de planification, de conduite, d'évaluation et de suivi définies dans le processus relatif aux DCO, et veille à ce que les acteurs concernés de l'entreprise OTAN (CyOC, Division civilo-militaire Renseignement et sécurité (JISD) et NCIA) communiquent et coopèrent de manière appropriée et en temps opportun. En outre, elle contribue aux réunions de la DPCC en facilitant les débats et en participant au processus de prise de décision, et participe à l'élaboration et à la réalisation des activités ayant trait aux DCO en assurant une coordination étroite avec les processus de gestion des incidents cyber et de gestion des risques cyber.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La personne titulaire du poste doit :

- posséder un diplôme universitaire, ou une qualification équivalente, délivré par un institut de valeur reconnue, de préférence dans le domaine des technologies de l'information et de la communication (TIC) ou dans un domaine en lien avec la cybersécurité ;
- avoir au moins trois années d'expérience dans le domaine de la cybersécurité, acquise de préférence au sein d'une grande organisation ;
- avoir déjà élaboré et mis en œuvre des processus et des procédures à l'appui d'opérations de cybersécurité, et avoir une expérience de la planification de programme ou de projet ;
- avoir une bonne connaissance des principes, des politiques et des procédures de cybersécurité applicables au sein d'une grande organisation, de préférence dans un contexte militaire ;
- être capable de préparer et de présenter des exposés et des rapports clairs et concis à un public de spécialistes ou de non-spécialistes ;
- avoir de solides compétences en matière de gestion des parties prenantes ;
- posséder de bonnes capacités d'analyse et de résolution de problèmes, ainsi que de bonnes capacités de communication, tant à l'oral qu'à l'écrit ;
- 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 ;
- faire preuve de flexibilité et être disposé(e) à travailler en dehors des heures normales de service, et être apte et disposé(e) à effectuer des déplacements lorsqu'il y a lieu, notamment pour se rendre au siège toutes les semaines.

ACQUIS SOUHAITABLES

Seraient considérés comme autant d'atouts :

- une compréhension du fonctionnement de l'OTAN et de ses politiques et directives de sécurité ;

- des certifications en cybersécurité (p. ex. CISSP, CCSP ou CISM) ;
- un diplôme de deuxième ou de troisième cycle en cybersécurité ;
- une bonne connaissance et une expérience de la planification, de la coordination et de l'exécution d'opérations de cybersécurité avancées dans des environnements fédérés ;
- une expérience des procédures de cybersécurité (chasse aux menaces, émulation d'attaque, *red teaming*, gestion des vulnérabilités, etc.) ;
- une bonne compréhension des technologies de cybersécurité actuelles et émergentes, et de la manière dont les entreprises les emploient pour développer l'activité numérique ;
- une expérience des bonnes pratiques et des processus en matière de gestion des incidents cyber et de gestion des risques cyber ;
- une connaissance de l'environnement de cybersécurité de l'OTAN.

3. RESPONSABILITÉS PRINCIPALES

Élaboration des politiques

Contribue à l'élaboration des politiques, des directives, des orientations et des documents administratifs en lien avec les DCO. Donne à la/au chef de la Section Opérations cyber des avis sur les politiques, les activités, les processus et les procédures ayant trait aux DCO. Fournit aux parties prenantes du NICC, aux pays membres et aux organismes civils et militaires de l'OTAN ainsi qu'aux pays partenaires et à des organisations internationales des avis et des orientations sur les DCO. Établit des documents stratégiques de haut niveau et remet des avis à l'appui des processus et des procédures relatives aux DCO exécutés au travers du NICC.

Planification et exécution

Propose, planifie, supervise, évalue et suit les activités ayant trait aux DCO, le tout en étroite coordination avec les parties prenantes concernées de l'entreprise OTAN. Coordonne, au sein du NICC, les activités relatives aux DCO. Recherche, développe et met à l'essai de nouveaux processus, à l'appui des DCO.

Développement de l'expertise

Recense les capacités de cybersécurité qui existent au sein de l'entreprise OTAN et en cherche de nouvelles à développer, à l'appui des DCO. Se tient parfaitement au fait des plans de projets et de programme, et apporte son expertise et son aide pour résoudre les problèmes. Se tient informé(e) de l'évolution des technologies dans ses domaines de compétence et rend des avis éclairés en la matière. Propose des mises à jour et des améliorations sur la base des enseignements tirés de situations réelles et d'exercices.

Gestion des parties prenantes

Établit et entretient un réseau de relations avec les principaux experts civils et militaires du NICC, et exerce ses fonctions de manière flexible entre le SHAPE et le siège de l'OTAN. Entretient une coopération et des relations de travail étroites avec les parties prenantes de l'Organisation qui sont impliquées dans le cycle de vie des processus et pratiques de sécurité de l'entreprise OTAN, notamment en ce qui concerne les DCO. Se sent à l'aise lorsqu'il s'agit d'apporter un soutien aux organes et aux comités exécutifs ou de haut niveau, et d'interagir avec eux.

Gestion des connaissances

Rédige des notes d'information et des rapports d'activité, et prépare des présentations et d'autres documents pour des réunions de haut niveau. Contribue au partage efficace de l'information avec les organismes et parties prenantes de l'OTAN qui sont susceptibles de contribuer aux activités ayant trait aux DCO (p. ex. Groupe de gestion du risque cyber (CRMG), Comité des autorités opérationnelles des SIC (BCISOA), etc.). À partir d'exposés, de débats et de rapports d'activités opérationnelles, formule des avis sur l'évolution des programmes de sécurité dans les pays membres et les organismes civils et militaires de l'OTAN ainsi que dans des entités non OTAN.

Gestion financière

Contribue à la gestion d'un budget prédéfini pour les projets qui lui sont confiés.

4. STRUCTURE ET LIAISONS

La Division CDT étant de plus en plus présente au sein du NICC, la personne titulaire du poste relève de l'agent basé de manière permanente au SHAPE le plus haut placé dans la hiérarchie de la Section et, par son intermédiaire, de la/du chef de la Section Opérations cyber et du Bureau du coordonnateur NICC au niveau de l'entreprise OTAN. Elle remplace, le cas échéant, la personne qui occupe le poste d'administrateur sénior au SHAPE visée ci-dessus. Enfin, elle travaille en étroite coopération avec les parties prenantes du NICC et relève, pour tout ce qui est technique, du chef de l'équipe DCO de la Section Opérations cyber.

Nombre de subordonné(e)s direct(e)s : sans objet.
Nombre de subordonné(e)s indirect(e)s : sans objet.

5. COMPÉTENCES

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

- Réflexion analytique discerne les relations multiples.
- Flexibilité : s'adapte à des situations imprévues.
- Persuasion et influence : prend différentes mesures à des fins de persuasion.
- Initiative : fait preuve de décision dans les situations où il faut agir sans attendre.
- Compréhension organisationnelle : comprend le climat et la culture de l'Organisation.
- Travail en équipe : coopère.

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.

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.

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, au moyen d'un outil d'intelligence artificielle (IA) générative, notamment d'un modèle conversationnel comme ChatGPT (*Chat Generative Pre-trained Transformer*) ou de tout autre générateur de texte. L'Organisation se réserve le droit de vérifier si la/le candidat(e) a eu recours à de tels outils. Tout dossier de candidature élaboré, en tout ou en partie, à l'aide d'une application d'IA générative ou créative pourra être rejeté sans autre

examen, à la seule discrétion de l'OTAN. Cette dernière 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.