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

Digital Transformation - Security Architect - 250465

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 06-Apr-2025, 11:59:00 PM
Salary (Pay Basis): 7,970.25Euro (EUR) Monthly
Grade: NATO Grade G17-G20

Description

1. SUMMARY

The Defence Investment (DI) Division is responsible for facilitating the development and adoption of cutting-edge, innovative and interoperable capabilities, critical to ensuring the Alliance's ability to undertake the full spectrum of missions and operations. Key lines of effort include:

- developing and implementing policies and programs to ensure the Alliance can rely on a capable and competitive transatlantic defense industrial base;
- facilitating and promoting multinational cooperation through a series of specific initiatives tackling critical capability requirements;
- leading the development and implementation of projects and major capability programmes in the land, maritime, air and space domains and in doing so addressing all policy, political-military, technical and practical aspects;
- leading NATO's policy and engagements in the aviation domain;

- pursuing interoperability through standardization and developing with Allies new approaches to operational challenges, supported, among others, by operational experimentation and innovation;
- maintaining the Alliance's technological edge through exploring and driving adoption of emerging and disruptive technologies, with a particular focus on autonomous systems;
- understanding, adapting to, and pro-actively addressing climate change's implications on armaments;
- informing and responding to the Alliance's evolving capability needs through the NATO Defence Planning Process (NDPP) implementation;
- providing oversight to NATO Agencies involved in capability development and delivery (in particular NATO Communication and Information Agency and NATO Support and Procurement Agency);
- working with a range of key stakeholders within NATO including the Strategic Commands and externally with NATO Partners and relevant international and regional organisations including the EU, as well as with industry and academia.

The NATO Digital Staff (NDS) is an integrated staff composed of members of the International Military Staff (IMS) and International Staff (IS) Defence Investment Division at the heart of NATO's Digital Transformation. The staff maintains digital subject matter expertise for providing the highest quality advice, policy and leadership to ensure the Alliance's technological edge, enable data-driven decision-making and release the potential of multi-domain operations. The NDS is responsible for the establishment, maintenance and evolution of NATO as a digital, data-driven decision-making organisation where the power and potential of interoperable digital technologies and a data-centricity are fully exploited for the benefit of the Alliance. Led by the Director NDS, the Staff supports different NATO senior policy committees and in particular, the Military Committee, the Digital Policy Committee (DPC) and the Cyber Defence Committee. It functionally operates under the co-ordinated executive management authority of the Director General of the IMS and the Assistant Secretary General for Defence Investment.

The Cyber Defence (CD) Branch acts as the Staff lead for cyberspace operations, information assurance, and cyber defence. This includes: supporting the Military Committee in its governance roles for cyberspace as a domain of operations and for cryptography; supporting the DPC and its substructure in the expertise domains of Communications and Information Systems (CIS) Security, cyber defence, cryptography, as well as Identity and Access Management (IAM), including Public Key Infrastructure (PKI); and the improvement of knowledge within these domains.

The Digital Transformation Security Architect leads Strategy and Policy development in support of the DPC's governance on technical Cyber Defence, specifically on establishing CIS security for the Digital Backbone and other initiatives supporting Digital Transformation. The incumbent enables the implementation of new security concepts such as Zero Trust by developing strategies, policies, as well as technical and implementation directives that define CIS security standards through the DPC. Moreover, the incumbent supports the branch in accelerating the development of interoperability standards in the field of CIS security and technical Cyber Defence in support of a security by design approach (e.g. secure cloud, secure information sharing, data centric security).

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- possess a Masters' degree or equivalent qualification in computer science, software engineering, systems engineering, or electronics engineering or in another relevant field from an university or institute of recognised standing;
- have at least 5 years of recent experience working in a professional IT systems or software engineering environment with a focus on CIS security;
- possess strong analytical and conceptual skills with the ability to create original concepts and theories on CIS security;

- have demonstrated experience in analysing complex issues, developing concepts, advising senior management and presenting results to non-technical audiences;
- have an up-to-date knowledge of current techniques and advances in computer or software engineering, particularly in the area of state-of-the art and emerging CIS security technologies and frameworks, to include, but not limited to, Zero Trust and Data Centric Security;
- have comprehensive knowledge of the principles of computer and communications security, networking, and the vulnerabilities of modern operating systems and applications;
- possess the following minimum levels of NATO's official languages (English/French): V ("Advanced"); I ("Beginner") in the other.

DESIRABLE

The following would be considered an advantage:

- demonstrated experience in coordinating teams and/or chairing committees/working groups;
- formal Information Assurance qualifications (e.g. Certified Information Systems Security Professional, Certified Advanced Security Practitioner, Security, SANS Institute certifications);
- a programme or project management certification or equivalent experience (e.g. PRINCE2, PMP, MSP).

3. MAIN ACCOUNTABILITIES

Expertise Development

Apply expertise, consider options and provide recommendations for continued improvement in CIS security strategy, standardisation and design, and policy development for the adoption of modern security principles such as Zero Trust. Assess financial soundness of cost estimates and business cases in CIS security capabilities and solutions.

Knowledge Management

Manage the content of NDS web pages and associated repositories dedicated to communications. Ensure that the corporate expert domain knowledge required to support communications is retained through appropriate information management and training.

Information Management

Ensure the effective management of communications information within the Branch, Staff and associated committee structures.

Policy Development

Facilitate NATO C3 strategy, policy and standards development in CIS security and Cyber Defence to meet the security standards needed, to persist future and current threats and to defend against peer adversaries in line with NATO strategic objectives.

Project Management

Oversee the management of committees and groups supporting the development of CIS security directives and standards and support the work of these committees and groups. Coordinate related activities within the NATO Enterprise and manage any supporting contracted work.

Representation of the Organization

Represent the interests of NATO when interacting with external bodies.

Stakeholder Management

Represent the Cyber Defence branch in committees and working groups and participate in meetings at NATO Staff level, NATO committee level and with relevant external bodies. Develop and enhance a network of key stakeholders in the CIS security and Cyber Defence communities both within and outside NATO. This includes other International Organisations and industrial and standardisation bodies. Assess, manage and consolidate the network within the broader interests of the NDS. Support the management

of stakeholder relationship within NATO Enterprise, including the NATO Military Authorities and the Office of the Chief Information Officer.

Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

The incumbent reports to the Head of NDS/Cyber Defence. The incumbent liaises with, and provides technical support and expertise, as directed, to NATO Bodies in their work, in areas related to CIS security and Cyber Defence. The incumbent also liaises with other national and international bodies dealing with CIS security or Cyber Defence.
Direct reports: N/A
Indirect reports: N/A

5. COMPETENCIES

The incumbent must demonstrate:

- Analytical Thinking: Makes complex plans or analyses;
- Clarity and Accuracy: Checks own work;
- Conceptual Thinking: Applies learned concepts;
- Customer Service Orientation: Takes personal responsibility for correcting problems;
- Impact and Influence: Takes multiple actions to persuade;
- Initiative: Is decisive in a time-sensitive situation;
- Organisational Awareness: Understands organisational climate and culture;
- 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. Advancement to the higher grade is not automatic, and will not normally take place during the first three years of service in the post.

Under specific circumstances, serving staff members may be appointed directly to the higher grade, and a period of three years might be reduced by up to twenty four months for external candidates. 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.

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.

Architecte sécurité (transformation numérique) - 250465

Emplacement principal : Belgique-Bruxelles
Organisation : OTAN SI
Horaire : Temps plein
Date de retrait : 06-avr.-2025, 23:59:00
Salaire (Base de paie) : 7 970,25Euro (EUR) Mensuelle
Grade : NATO Grade G17-G20

Description

1. RÉSUMÉ

La Division Investissement de défense (DI) est chargée de faciliter le développement et l'adoption de capacités de pointe, innovantes et interopérables, qui sont indispensables à l'Alliance pour mener toute la gamme de ses missions et opérations. Ses principaux axes de travail sont les suivants :

- élaborer et mettre en œuvre des politiques et des programmes visant à faire en sorte que l'Alliance puisse compter sur une base industrielle de défense transatlantique solide et compétitive ;
- faciliter et promouvoir la coopération multinationale au travers d'initiatives spécifiques visant à répondre aux besoins capacitaires critiques ;
- piloter l'élaboration et la mise en œuvre de projets et de programmes capacitaires de grande ampleur dans les milieux terrestre, maritime, aérien et spatial et, ce faisant, aborder toutes les questions de fond et les questions politico-militaires, techniques et pratiques ;
- piloter la politique et l'action de l'OTAN dans le domaine de l'aviation ;
- promouvoir l'interopérabilité au travers de la normalisation et élaborer avec les Alliés de nouvelles approches face aux défis opérationnels, notamment au travers d'activités d'expérimentation opérationnelle et d'innovation ;
- aider l'Alliance à conserver son avance technologique en étudiant des technologies émergentes et des technologies de rupture, en particulier dans

le domaine des systèmes autonomes, et en s'employant à favoriser leur adoption ;

- développer les connaissances liées au changement climatique, favoriser l'adaptation à celui-ci et prendre des mesures proactives concernant ses implications pour le secteur de l'armement ;
- suivre l'évolution des besoins capacitaires de l'Alliance et y répondre, au travers de la mise en œuvre du processus OTAN de planification de défense (NDPP) ;
- jouer un rôle de supervision auprès des agences de l'OTAN qui interviennent dans le développement et la mise à disposition de capacités, en particulier l'Agence OTAN d'information et de communication (NCIA) et l'Agence OTAN de soutien et d'acquisition (NSPA) ;
- travailler avec divers intervenants majeurs au sein de l'OTAN, notamment les commandements stratégiques, et, à l'extérieur, avec les partenaires de l'OTAN, avec des organisations régionales et internationales concernées (notamment l'Union européenne), ainsi qu'avec le secteur privé et les milieux universitaires.

Le Secrétariat numérique de l'OTAN (NDS) est une entité composite regroupant des membres de l'État-major militaire international (EMI) et de la Division Investissement de défense du Secrétariat international (SI) ; il est au cœur de la transformation numérique de l'OTAN. Le NDS entretient dans le domaine du numérique des compétences spécialisées qui lui permettent d'offrir des conseils, des avis et un leadership de la plus haute tenue, et ainsi d'aider l'Alliance à conserver son avance technologique, à mettre les données au service de la prise de décision et à exploiter pleinement le potentiel des opérations multimilieux. Il est chargé d'asseoir l'OTAN en tant qu'organisation où la prise de décision s'appuie sur le numérique et les données, où la puissance et le potentiel de technologies numériques interopérables sont exploités à plein pour le bien de l'Alliance et où la donnée joue un rôle central, et de faire en sorte qu'elle le demeure et qu'elle continue d'évoluer sur cette voie. Placé sous l'autorité d'une directrice/d'un directeur, le NDS apporte un soutien à différents comités d'orientation de haut niveau de l'OTAN, et

en particulier au Comité militaire, au Comité des orientations pour le numérique (DPC) et au Comité de cyberdéfense. Il opère sous l'autorité exécutive coordonnée de la directrice générale/du directeur général de l'EMI et de la/du secrétaire général(e) adjoint(e) pour l'investissement de défense.

La Branche Cyberdéfense (CD) est l'élément du NDS qui est responsable des opérations dans le cyberespace, de l'assurance de l'information et de la cyberdéfense. Elle a notamment pour tâches d'épauler le Comité militaire dans ses missions de gouvernance de la cryptographie et de gouvernance du cyberespace en tant que milieu d'opérations ; d'aider le DPC et sa structure subordonnée dans ses domaines d'expertise que sont la sécurité des systèmes d'information et de communication (SIC), la cyberdéfense, la cryptographie et la gestion des identités et des accès (IAM), y compris l'infrastructure à clés publiques (PKI) ; et de contribuer à l'amélioration des connaissances dans ces domaines.

L'architecte sécurité (transformation numérique) est chargé(e) de diriger l'élaboration de stratégies et de politiques relatives à la gouvernance technique de la cyberdéfense par le DPC ; plus spécifiquement, elle/il participe aux travaux concernant la sécurité des SIC de la dorsale numérique de l'OTAN et à d'autres initiatives en lien avec la transformation numérique. La personne titulaire du poste contribue à la mise en œuvre de nouveaux concepts de sécurité tels que le « confiance zéro » en élaborant, à travers le DPC, des stratégies, des politiques, des directives techniques et des directives d'exécution fixant les normes de sécurité des SIC. En outre, elle participe aux travaux de la Branche visant à accélérer l'élaboration de normes d'interopérabilité dans les domaines de la sécurité des SIC et des moyens techniques de cyberdéfense, à l'appui d'une approche de type « sécurité dès la conception » (cloud sécurisé, partage d'informations sécurisé, sécurité centrée sur les données, etc.).

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La personne titulaire du poste doit :

- avoir un diplôme de niveau master ou posséder une qualification de niveau équivalent en informatique, en génie logiciel, en ingénierie systèmes, en génie électronique ou dans une autre discipline pertinente, délivré(e) par une université ou un institut de valeur reconnue ;
- avoir au moins cinq ans d'expérience récente dans un environnement en rapport avec l'informatique ou le génie logiciel professionnels, et plus précisément avec la sécurité des SIC ;
- avoir une excellente capacité d'analyse et de solides compétences conceptuelles ; être capable notamment de créer des concepts pratiques et théoriques originaux sur la sécurité des SIC ;
- avoir une expérience probante de l'analyse de questions complexes, du développement de concepts, du conseil à de hauts responsables, et de la présentation de résultats à un public non spécialisé ;
- être au fait des dernières techniques et avancées en génie informatique ou logiciel, et plus particulièrement de celles concernant les technologies et cadres de pointe et émergents en sécurité des SIC (confiance zéro, sécurité centrée sur les données, etc.) ;
- avoir une connaissance approfondie des réseaux, des principes sous-tendant la sécurité des communications et la sécurité informatique, et des vulnérabilités des systèmes d'exploitation et applications modernes ;
- 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.

ACQUIS SOUHAITABLES

Seraient considérées comme autant d'atouts :

- une expérience probante de la coordination d'équipes et/ou de la présidence de comités ou de groupes de travail ;
- des qualifications officielles en assurance de l'information (p. ex. *Certified Information Systems Security Professional*, *Certified Advanced Security Practitioner*, certification en sécurité, certification SANS Institute) ;
- une certification en gestion de programme ou en gestion de projet (p. ex. PRINCE2, PMP, MSP) ou une expérience équivalente.

3. RESPONSABILITÉS PRINCIPALES

Développement de l'expertise

Utilise ses connaissances pour formuler, après examen des différentes options, des recommandations propres à assurer une amélioration continue de la stratégie en matière de sécurité des SIC ainsi que de la normalisation et des concepts dans ce domaine, et des recommandations pour les politiques d'adoption des principes de sécurité modernes tels que le « confiance zéro ». Évalue la validité financière des estimations de coût et des dossiers de décision relatifs aux capacités et solutions de sécurité des SIC.

Gestion des connaissances

Gère le contenu des pages web du NDS et de ses bases documentaires consacrées aux communications. Veille, par des formations et une gestion de l'information appropriées, à la préservation des connaissances spécialisées formant la mémoire collective nécessaire au maintien des fonctions de communication.

Gestion de l'information

Veille à la gestion efficace des informations relatives aux communications, au sein de la Branche, du Secrétariat et de la structure des comités associés.

Élaboration des politiques

Facilite l'élaboration des stratégies, politiques et normes C3 de l'OTAN liées à la sécurité des SIC et à la cyberdéfense, pour permettre à l'Alliance de répondre à ses besoins en matière de sécurité, de résister aux menaces actuelles et futures et de se défendre contre des adversaires de puissance équivalente, conformément aux objectifs stratégiques de l'OTAN.

Gestion de projet

Supervise la gestion des comités et des groupes qui contribuent à l'élaboration de directives et de normes sur la sécurité des SIC, et les épaule dans leurs travaux. Coordonne les activités en lien avec ces travaux au sein de l'entreprise OTAN et assure la gestion des éventuelles externalisations effectuées à l'appui de ceux-ci.

Représentation de l'Organisation

Représente les intérêts de l'OTAN dans le cadre des interactions avec des organismes extérieurs.

Gestion des parties prenantes

Représente la Branche Cyberdéfense dans des comités et des groupes de travail, participe à des réunions de services et de comités de l'OTAN et se rend à des réunions avec des entités externes concernées. Crée et développe un réseau regroupant les principales parties prenantes de la communauté de la sécurité des SIC et de la communauté de la cyberdéfense, tant à l'intérieur qu'à l'extérieur de l'OTAN (ce qui englobe d'autres organisations internationales, ainsi que des organismes industriels et normatifs). Évalue, gère et consolide ce réseau en se concentrant sur les domaines présentant un intérêt pour le NDS. Contribue à la gestion des relations entre les différents acteurs concernés au sein de l'entreprise OTAN, y compris les autorités militaires de l'OTAN et le Bureau du directeur des systèmes d'information.

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

4. STRUCTURE ET LIAISONS

La personne titulaire du poste relève de la/du chef de la Branche Cyberdéfense du NDS. Elle se tient en liaison avec les organes de l'OTAN et leur apporte, selon les instructions, un soutien et une expertise techniques pour leurs travaux dans les domaines liés à la sécurité des SIC et à la cyberdéfense. En outre, elle se tient en liaison avec d'autres organismes nationaux et internationaux compétents en matière de sécurité des SIC et de cyberdéfense.

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 : fait des analyses ou des plans complexes.
- Clarté et précision : vérifie son travail.
- Réflexion conceptuelle : applique les concepts acquis.
- Souci du service au client : s'engage personnellement à résoudre les problèmes.
- 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 : 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. La promotion au grade le plus élevé n'est pas automatique et n'est en principe pas accordée au cours des trois premières années passées dans le poste.

Lorsque certaines conditions sont réunies, l'agent en fonction peut être nommé immédiatement au grade le plus élevé, et la période de trois ans peut être réduite, d'un maximum de vingt-quatre mois, pour les candidat(e)s externes. 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.

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.

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.