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

Analyst, Cyber Incident Response and Risk Management (241836)

Primary Location Belgium-Brussels
NATO Body NATO International Staff (NATO IS)
Schedule Full-time
Application Deadline 27-Jan-2025
Salary (Pay Basis) 6,118.54Euro (EUR) Monthly
Grade NATO Grade G15-G17
Clearance Level NS
Description

'PENDING BUDGET APPROVAL'

1.SUMMARY

The Joint Intelligence and Security Division (JISD), under the leadership of the Assistant Secretary General for Intelligence and Security (ASG I&S), comprises two principal pillars: Intelligence – headed by the Deputy ASG for Intelligence; and the NATO Office of Security (NOS) – headed by the Deputy ASG for Security.

The Intelligence pillar is responsible for ensuring the situational awareness of the North Atlantic Council (NAC) and the Military Committee (MC), for the analysis of the indications and warnings in support of the NATO Crisis Response System, and for the development of intelligence policies and capabilities for NATO. Its functional areas address: intelligence analysis and production, intelligence policy, and capability development. The Intelligence Production Unit (IPU), comprised of both military and civilian personnel, supports the NAC, MC and senior level decision makers on strategic issues of concern with intelligence-based analysis, briefings and other written products.

The Cyber Threat Analysis Branch (CTAB) is responsible for providing evidence-based assessments of the cyber threat landscape to empower NATO stakeholders to make risk-informed decisions. The multidisciplinary team combines all-source data with cutting edge technologies to support and enhance the Alliance leaderships' understanding on the nature of cyber competition and conflict. CTAB systematically identifies strategic patterns and trends in cyber space and generates tailored insights to support network defence and mission assurance with predictive analysis, cyber threat intelligence, and threat hunting. The Analyst is assigned to the CTAB. S/he assists in monitoring cyber-related developments, including cyber incident response and risk management, contributes to the production of cyber threat reporting and is primarily responsible for:

- Technical cyber threat intelligence analysis – track, pivot, and enrich data relating to malware, hosts, and networks (domain, IP, netflow, certificate etc.).
- Investigation of raw telemetry to provide intelligence insights in support of incident

response activities. Maintain campaign history to prioritize security detection on high impact threats.
- Extrapolation of behavioral patterns and identifiable characteristic, including network infrastructure registration and procurement patterns, exploit chain commonalities, use of common malware or post-exploitation toolkits.
- Producing intelligence assessments related to mission assurance, risk management, and incident response. Generate written (and oral) operational and strategic reports for various stakeholders. Communicate actionable insights in support of senior-level decision-making.
- Mentoring junior analysts to ensure accuracy of cyber threat analysis driven by NATO intelligence requirements, and actionable intelligence. Perform technical data checks and editorial work before release of finished intelligence products.
- Participating in NATO cyber related exercises.

2.QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- possess a university degree, preferably in the field of cyber security, information technology, security studies, statistics, data science or related studies;
- have at least 3 years in-depth experience in the area of cyber security operations centre, defensive cyberspace operations, or cyber threat analysis;
- have at least 2 years of recent experience in activities that derive intelligence on cyber-enabled threats (capabilities and intent of cyber threat actors) and cyber vulnerabilities to assist in developing cyber situational awareness;
- have knowledge of open source information, collection and analysis processes, and experience working with large datasets
- have recent and demonstratable experience with analytical frameworks for intrusion analysis such as MITRE ATT&CK, cyber kill-chain, diamond model, and/or analysis of competing hypothesis;
- be familiar with strategic issues and challenges facing the Alliance and NATO's geopolitical environment;
- have excellent drafting skills and experience in preparing alert bulletins, threat assessments, and intelligence reports;
- possess the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; II ("Elementary") in the other.

DESIRABLE

The following would be considered an advantage:

- experience as a serving or former member of an Allied intelligence or security service, national cyber center, or national cyber command;
- having held cyber security responsibilities in a government of a NATO Nation or in an International Organisation such as EU, UN, OSCE or NATO;
- experience in project management.

3.MAIN ACCOUNTABILITIES

Planning and Execution

Using all means available, investigate cyber threats to NATO and its Allies. Compile, draft or review reports as appropriate. Drafting of bespoke products in support of briefing requirements from all NATO HQ stakeholders. Share knowledge on cyber threats and related issues via briefings and reports in order to support decision making by the appropriate authorities. Collaborate with appropriate channels within the NATO HQ as well as with other stakeholders, such as the Office of

the Chief information Officer (OCIO), NATO Communication Information Agency (NCIA), Allied Command Operations (ACO) and counterparts in NATO Nations.

Knowledge Management

Act as main aggregator for a number of sources of information, effectively manage, coordinate, align and streamline inputs from all sources of information. Support the development, review and update of NATO's analytical products related to cyber security. Draft background briefs and presentations related to cyberspace for a variety of NATO and partner stakeholders. Contribute to information sharing with relevant NATO bodies in support of incident management and mission assurance.

Stakeholder Management

Liaise with and obtain input from security and intelligence services in NATO member countries, including through the existing mechanisms of the NATO Civilian and Military Intelligence Committees, as well as with the working-level of the Intelligence Steering Board in order to maintain and develop the flow of intelligence reporting to and within the Alliance. Establish and maintain close working relations within the NATO enterprise, including with the OCIO, ACO Cyberspace Operations Centre, and the NCIA. Establish cyber defence liaison with multiple industry partners and International Organisations in support of NATO cyber defence objectives.

Policy Development

Contribute to the development of policies, directives and guidance documents on cyber threats and related issues. Support the provisioning of incident advice and guidance to NATO Nations, NATO civil and military bodies and partner nations and international organisations.

Expertise Development

Develop and maintain technical, operational, and strategic expertise in all matters relating to cyber security, mentoring others as necessary. Provide expertise and operational support to the NATO civil and military bodies on the cyber landscape.

Project Management

Define priorities for and contribute to the development and presentation of technical and operational cyber defence requirements for NATO-wide capabilities and projects, including on aspects related to governance, finance, and delivery. Assist in development and presentation of technical and operational cyber defence requirements for NATO-wide capabilities and projects.

Perform any other related duties, as assigned.

4. INTERRELATIONSHIPS

The incumbent reports to the Head CTAB. They work in close coordination with other sections within JISD, as well as with other divisions in the International Staff, with the NATO Military Authorities, with national delegations as well as Allied capitals, and NATO Agencies. They also maintain good working relations in their field of competence with partner countries, other International Organisations and industry on cyber security related matters.

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;
- 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.

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.

Analyste (réponse aux cyberincidents et gestion des risques (241836)

Emplacement principal Belgique-Bruxelles
Organisation OTAN SI
Horaire Temps plein
Date de retrait 27-janv.-2025
Salaire (Base de paie) 6 118,54Euro (EUR) Mensuelle
Grade NATO Grade G15-G17
Niveau de l'habilitation de sécurité NS
Description

"SOUS RÉSERVE D'APPROBATION PAR LES AUTORITÉS BUDGÉTAIRES"

1.RÉSUMÉ

La Division civilo-militaire Renseignement et sécurité (JISD), placée sous l'autorité de la/du secrétaire général(e) adjoint(e) pour le renseignement et la sécurité (ASG/I&S), se compose de deux grands piliers : le pilier « renseignement », dirigé par la/le secrétaire général(e) adjoint(e) délégué(e) pour le renseignement (DASG/I), et le pilier « sécurité », à savoir le Bureau de sécurité de l'OTAN (NOS), dirigé par la/le secrétaire général(e) adjoint(e) délégué(e) pour la sécurité (DASG/S).

Le pilier « renseignement » est chargé de faire en sorte que le Conseil de l'Atlantique Nord et le Comité militaire aient une bonne connaissance de la situation, d'analyser les indices et les critères d'alerte à l'appui du système OTAN de réponse aux crises, et de mettre en place pour l'OTAN des politiques et des capacités en matière de renseignement. 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. L'Unité Production du renseignement (IPU), composée de civils et de militaires, éclaire le Conseil de l'Atlantique Nord, le Comité militaire et les décideurs de haut niveau sur les enjeux stratégiques au travers d'analyses du renseignement, d'exposés et d'autres rapports écrits.

La Branche Analyse des menaces cyber (CTAB) est chargée d'établir des évaluations du panorama des menaces cyber fondées sur des données probantes afin que les acteurs OTAN soient en capacité de prendre des décisions éclairées en tenant compte des risques. Cette équipe pluridisciplinaire agrège ainsi des données de toutes sources en utilisant des technologies de pointe pour aider les dirigeants de l'Alliance à comprendre plus finement la nature de la compétition et de l'affrontement dans l'espace cyber. La CTAB s'emploie par ailleurs à repérer de manière systématique les *patterns* et tendances d'ordre stratégique dans le cyberespace et produit des avis éclairés venant alimenter l'analyse prédictive, le renseignement sur les menaces cyber et la chasse aux menaces au profit de l'assurance de la mission et de la défense des réseaux. L'analyste est affecté(e) à la CTAB. Elle/Il contribue au suivi d'événements cyber, y compris à la réponse aux cyberincidents et à la gestion des risques, ainsi qu'à la production de rapports sur les menaces cyber. Elle/Il est principalement chargé(e) des tâches suivantes :

- Analyse technique du renseignement sur les menaces cyber – suivre les activités des acteurs malveillants, « pivoter » sur des événements et enrichir les données relatives

aux malware, aux hôtes et aux réseaux (domaine, IP, flux réseau, certificats, etc.).

- Étudier des données brutes dans le but de fournir des éléments de renseignement à l'appui des activités de réponse aux incidents. Tenir un historique des campagnes pour cibler les menaces à haut pouvoir destructeur à traiter en priorité.
- Extrapoler les *patterns* de comportement et les caractéristiques identifiables, notamment les enregistrements d'infrastructure réseau, les tendances d'achat, les caractéristiques communes des chaînes d'exploits, l'utilisation de boîtes à outils de post-exploitation ou de *malware* communs.
- Produire des évaluations de renseignement concernant l'assurance de la mission, la gestion des risques et la réponse aux incidents. Préparer des rapports stratégiques et opérationnels écrits (et oraux) à l'intention de diverses parties prenantes. Fournir des avis actionnables pour des décideurs de haut niveau.
- Encadrer les analystes juniors pour veiller à l'exactitude des analyses des menaces cyber répondant aux besoins en renseignement de l'OTAN, ainsi que du renseignement actionnable. Assurer la relecture des produits de renseignement et le contrôle des données techniques qui y figurent avant leur diffusion
- Participer aux exercices cyber de l'OTAN.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La/Le titulaire du poste doit :

- avoir un diplôme universitaire, de préférence dans le domaine de la cybersécurité, des technologies de l'information, de la sécurité, des statistiques, de la science des données ou dans un domaine apparenté ;
- avoir au moins trois ans d'expérience approfondie dans le domaine des opérations de cybersécurité, des opérations défensives dans le cyberespace ou de l'analyse des menaces cyber ;
- avoir au moins deux ans d'expérience récente dans des activités de production de renseignement sur les menaces faisant appel au cyber (capacités et intentions des acteurs malveillants) et sur les cybervulnérabilités, qui visent à améliorer la connaissance de la situation cyber ;
- avoir une connaissance des processus de collecte et d'analyse des informations de sources ouvertes, et avoir une expérience du travail avec d'importants volumes de données ;
- avoir une expérience récente et probante des cadres analytiques pour l'analyse des intrusions comme MITRE ATT&CK, les *cyber kill chains* (chaînes de destruction de la cybersécurité), le modèle diamant et/ou l'analyse d'hypothèses antagoniques ;
- être familiarisé(e) avec les problématiques et les défis stratégiques auxquels l'Alliance doit faire face, ainsi qu'avec l'environnement géopolitique de l'OTAN ;
- avoir d'excellentes aptitudes rédactionnelles et une expérience de la préparation de bulletins d'alerte, d'évaluations de la menace et de comptes rendus de renseignement ;
- avoir au minimum le niveau de compétence V (« avancé ») dans l'une des deux langues officielles de l'OTAN (anglais/français), et le niveau II (« élémentaire ») dans l'autre.

ACQUIS SOUHAITABLES

Seraient considérés comme autant d'atouts :

- faire partie du personnel actif ou avoir été membre d'un service de renseignement ou de sécurité d'un pays de l'Alliance, d'un centre cyber national ou d'un commandement cyber national ;
- avoir occupé un poste à responsabilités dans le domaine de la cybersécurité au sein de l'administration publique d'un pays de l'OTAN ou d'une organisation internationale (UE,

ONU, OSCE, OTAN, etc.)
- une expérience de la gestion de projet.

3. RESPONSABILITÉS PRINCIPALES

Planification et exécution
Analyse, en utilisant tous les moyens disponibles, les menaces cyber qui pèsent sur l'OTAN et les Alliés. Prépare, rédige ou réexamine des rapports, selon le cas. Élabore des produits sur mesure à l'appui des demandes d'exposés de toutes les parties prenantes du siège de l'OTAN. Partage ses connaissances sur les menaces cyber et les questions s'y rattachant dans des exposés et des rapports, afin d'éclairer les autorités compétentes dans leur prise de décision. Collabore avec les interlocuteurs appropriés au siège de l'OTAN, ainsi qu'avec d'autres parties prenantes telles que le Bureau du directeur des systèmes d'information (OCIO), l'Agence OTAN d'information et de communication (NCIA), le Commandement allié Opérations (ACO) et ses homologues dans les pays de l'OTAN.

Gestion des connaissances
Assume la fonction d'*agrégateur* principal pour un certain nombre de sources d'information : gère, coordonne, harmonise et rationalise les contributions fournies par toutes les sources d'information. Contribue à l'élaboration, à l'examen et à la mise à jour des produits analytiques OTAN en matière de cybersécurité. Prépare des notes d'information et des présentations sur le cyberespace à l'intention de différentes parties prenantes (OTAN et partenaires). Contribue au partage de l'information avec les organismes OTAN concernés afin d'améliorer la gestion des incidents et l'assurance de la mission.

Gestion des parties prenantes
Pour les besoins du maintien et du développement des flux de renseignements à destination de l'Alliance et au sein de cette dernière, se tient en liaison avec les services de sécurité et de renseignement des pays membres de l'OTAN et sollicite des informations de leur part, notamment grâce aux mécanismes en place au niveau des Comités du renseignement civil et du renseignement militaire de l'OTAN, et reste en relation, au niveau opérationnel, avec le Bureau directeur du renseignement. Établit et entretient des relations de travail étroites au sein de l'entreprise OTAN, notamment avec l'OCIO, le Centre des cyberopérations de l'ACO et la NCIA. Établit des contacts avec divers partenaires du secteur privé et d'autres organisations internationales dans le domaine de la cyberdéfense, à l'appui des objectifs de l'OTAN.

Élaboration des politiques
Contribue à l'élaboration des politiques, des directives et des documents d'orientation sur les menaces cyber et les questions s'y rattachant. Aide à fournir des avis et des orientations sur les incidents aux pays membres et aux organismes civils et militaires de l'OTAN, aux pays partenaires et à d'autres organisations internationales.

Développement de l'expertise
Développe et entretient son expertise stratégique, technique et opérationnelle sur toutes les questions ayant trait à la cybersécurité, et encadre ses collègues selon les besoins. Apporte une expertise et un soutien opérationnel sur l'ensemble des questions cyber aux organismes civils et militaires de l'OTAN.

Gestion de projet
Définit les priorités concernant les besoins techniques et opérationnels en matière de cyberdéfense

pour des capacités et des projets à l'échelle de l'OTAN, y compris sur des aspects liés à la gouvernance, aux moyens financiers et à leur concrétisation, et contribue à leur élaboration et à leur présentation. Aide à définir et à présenter les besoins en matière de cyberdéfense, qu'ils soient d'ordre technique ou opérationnel, pour des capacités et des projets à l'échelle de l'OTAN.

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

4. STRUCTURE ET LIAISONS

La/Le titulaire du poste relève de la/du chef de la CTAB. Elle/Il travaille en étroite coordination avec les autres sections de la JISD, avec les autres divisions du Secrétariat international, avec les autorités militaires de l'OTAN, avec les délégations et les capitales des pays de l'Alliance, ainsi qu'avec les agences de l'OTAN. Elle/Il entretient également de bonnes relations de travail avec les pays partenaires, d'autres organisations internationales et le secteur privé pour les questions de cybersécurité ayant trait à son domaine de compétence.
Nombre de subordonné(e)s direct(e)s : sans objet.
Nombre de subordonné(e)s indirect(e)s : sans objet.

5. COMPÉTENCES

La/Le titulaire du poste doit faire preuve des compétences suivantes :

- Réflexion analytique : discerne les relations multiples.
- Flexibilité : s'adapte à des situations imprévu
- 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. 13 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