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

Head, Cyber Threat Assessment Branch (241631)

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 15-Dec-2024
Salary (Pay Basis): 8,754.21 Euro (EUR) Monthly
Grade: NATO Grade G20
Clearance Level CTS
Description

This campaign will also recruit a Senior Analyst (G17/20) within this same branch (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.

Intelligence is responsible for ensuring the situational awareness of the North Atlantic Council and the Military Committee, 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 joint civilian and military Intelligence Production Unit (IPU) delivers strategic intelligence-based analysis to support North Atlantic Council (NAC) and Military Committee (MC) decision making on strategic issues of concern. The IPU produces a range of planned and tasked intelligence products on regional issues in Eurasia, Africa and the Middle East, and on transnational issues such as hybrid operations, terrorism, instability, weapons of mass destruction and energy security.

The Cyber Threat Analysis Branch (CTAB) is responsible for providing evidence- and intelligence-based assessments of the cyber threat landscape to empower NATO stakeholders to make risk-informed decisions. CTAB delivers strategic assessments on the cyber threats to NATO, but also provides situational awareness for NATO stakeholders. The multidisciplinary team combines all-source data with cutting edge technologies to support

and enhance the Alliance leadership's 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 incumbent will oversee the work of the Cyber Threat Assessment Branch and guide the development of cyber assessments of interest to the Alliance. They will lead staff efforts to produce quality cyber threat analyses to meet the growing Allied demand, to better understand the cyber threat landscape and what it means for NATO.

They will be primarily responsible for:

- Providing threat related assessments;
- Applying innovative thinking, performance analysis and modern computer engineering principles to solve complex technological problems;
- Supporting the development of improved data analytics capabilities for CTAB and the IPU;
- Collaborating with relevant stakeholders within NATO, Allies, Partners, and Industry;
- Advise IPU leadership on budgetary needs for CTAB;
- Chairing intelligence-driven working groups, including the annual NATO Cyber Threat Intelligence Conference;
- Maintaining a proficiency in current and emerging cyber threats and attacks, as well as security vulnerabilities.

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- possess a university degree, preferably in the field of cyber defence, information technology, political science, international security or other related studies;
- have at least 8 years related experience, out of which at least 5 years in the area of cyber defence operations or analysis and 2 years managerial experience in leading and mentoring a diverse team;
- have in-depth knowledge and experience related to the technical developments in the cyber threat landscape;
- have recent experience in activities that derive intelligence on cyber threats (capabilities and intent of cyber threat actors) and cyber vulnerabilities to assist in developing cyber situational awareness;
- be familiar with strategic issues and challenges facing the Alliance and NATO's geopolitical environment;
- have held cyber defence responsibilities in a government of a NATO Nation or in an International Organisation such as EU, UN, OSCE or NATO;
- have extensive experience working for a national intelligence or security service;
- have excellent communication skills (both written and oral), and experience in preparing alerts and reports;
- possess the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; I ("Beginner") in the other.

DESIRABLE

The following would be considered an advantage:

- experience with the nexus between technology and policy;
- experience in the field of data analytics, data science, or machine learning;
- experience synthesising qualitative and quantitative information from a large variety of sources, create original insight, and communicate in written, verbal and graphical forms.

3. MAIN ACCOUNTABILITIES

People Management

Oversee the work of the Cyber Threat Analysis Branch and provide guidance and direction. Provide tasking and oversight for CTAB projects and ensure they are delivered within required deadlines. Promote transparency in decision-making, equal access to opportunities for all staff and an inclusive management culture. Ensure that all staff under their responsibility are clear on Organizational, Divisional and Directorate objectives. Collaborate with Executive Management on personnel matters. Provide regular and fair feedback on performance, informally as appropriate and via the Performance Review and Development (PRD) system. Participate in a collegial review of performance to discuss possible development and mobility opportunities for individuals, identify high potentials and help ensure common standards are applied in the process. Participate in recruitment procedures for vacant posts in the Division, in accordance with NATO guidelines and with the best interests of the Organization in mind.

Planning and Execution

Oversee production of all CTAB intelligence products based on monitoring and analysing cyber related information from all available sources and provide timely and relevant operational and strategic intelligence assessments. Coordinate production and cooperate with other NATO Intelligence Enterprise bodies. Determine input into short- and medium-term work plans and manage implementation of projects to achieve branch objectives. Propose to the Chain of Command production projects as necessary in response to changing developments and current events. Plan and develop processes and capabilities to systematically identify strategic patterns and trends in cyber space and generate tailored insights to support network defence and mission assurance with predictive analysis and cyber threat intelligence. Find opportunities to automate and innovate NATO's cyber threat intelligence capability.

Stakeholder Management

Establish and maintain close working relations with contacts to security and intelligence services of Allied nations. Carry out appropriate liaison with other Allied entities, IS and IMS

Divisions, and members of other NATO authorities. Establish and maintain relationships with industry partners and International Organisations (including the EU) to support the CTAB mission. Provide support to the North Atlantic Council (NAC), the Military Committee and other relevant customers by providing sound cyber threat analysis in briefings, assessments and other appropriate analytical products.

Serve as a key interlocutor for the NATO cyber community. Represent IPU/JISD at meetings, conferences, and seminars as required. Represent the IPU at a senior level with both internal and external stakeholders when directed by the Director IPU or JISD leadership.

Organisational Efficiencies

Review and prepare presentations, speaking notes, background briefs, and other forms of intelligence production; report on challenges or questions with which the IPU is concerned. Facilitate information-sharing, with proper information handling procedures, with a view to transferring knowledge across CTAB, the IPU, and with key cyber interlocutors. Contribute to NATO representation by developing and communicating information supportive of NATO's interests.

Project Management

Support the development and presentation of technical and operational cyber defence requirements for NATO-wide capabilities and projects that have a direct impact on CTAB or the IPU. Manage projects and/or programmes as directed by the IPU Director. Assist in the management of cyber intelligence capability initiatives and any resulting actions.

Act as Chairperson of cyber threat intelligence workshops and conferences as required and appropriate. Brief and lecture groups, represent the Alliance at conferences, workshops or seminars as directed. Conduct and lead bilateral meetings on cyber threats with national intelligence counterparts.

Financial Management

Determine and verify the correct use of assigned financial resources, and advise the JISD Chain of Command on appropriate annual funding. Take responsibility of the budget related to CTAB's capability development.

Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

The incumbent reports to the Director, IPU. They will work in close coordination with other Sections within the Division, as well as with other Divisions in the International Staff, with

the NATO Military Authorities, with national Delegations as well as Alliance capitals, and other NATO Agencies. They will also maintain good working relations in their field of competence with industry, partner countries and relevant International Organisations on cyber defence related matters.

Direct reports: 7
Indirect reports: N/a.

5. COMPETENCIES

The incumbent must demonstrate:

- Achievement: Creates own measures of excellence and improves performance;
- Change Leadership: Personally leads change;
- Clarity and accuracy: Monitors data or projects;
- Conceptual thinking: Applies learned concepts;
- Flexibility: Adapts own strategy;
- Impact and Influence: Takes multiple actions to persuade;
- Initiative: Plans and acts up to a year ahead;
- Leadership: Promotes team effectiveness;
- Organisational Awareness: Understands organisational Climate and culture;
- Self-Control: Responds calmly.

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.

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.

Chef de la Branche Analyse des menaces cyber (241631)

Emplacement principal : Belgique-Bruxelles
Organisation : OTAN SI
Horaire : Temps plein
Date de retrait : 15-déc.-2024
Salaire (Base de paie) : 8 754,21Euro (EUR) Mensuelle
Grade NATO Grade G20
Niveau de l'habilitation de sécurité CTS
Description

Cette campagne recrutera également un Analyste Senior (G17/20) au sein de cette même branche (En attente d'approbation du budget)

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, 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, fournit des analyses du renseignement de niveau stratégique à l'appui des décisions du Conseil de l'Atlantique Nord et du Comité militaire sur les grands enjeux stratégiques. L'IPU élabore divers produits de renseignement, planifiés ou établis sur demande, sur des problématiques régionales en Eurasie, en Afrique et au Moyen-Orient, et sur des questions transnationales telles que les opérations hybrides, le terrorisme, l'instabilité, les armes de destruction massive et la sécurité énergétique.

La Branche Analyse des menaces cyber (CTAB) est chargée d'établir des évaluations du panorama des menaces cyber fondées sur des données probantes et du renseignement afin que les acteurs OTAN soient en capacité de prendre des décisions éclairées en tenant compte des risques. La CTAB produit des évaluations stratégiques sur les menaces cyber pesant sur l'OTAN et tient les parties prenantes de l'Organisation informées de la situation. 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.

La/Le titulaire supervise les travaux de la CTAB et encadre la conduite d'évaluations cyber présentant un intérêt pour l'Alliance. Elle/Il pilote les travaux visant à produire des analyses des menaces cyber de qualité et à répondre ainsi à la demande croissante des Alliés désireux de mieux comprendre le panorama des menaces cyber et ce qu'il implique pour l'OTAN.

La/Le titulaire du poste est principalement chargé(e) de ce qui suit :

- produire des évaluations de la menace ;
- appliquer des principes de réflexion novatrice, d'analyse des performances et d'ingénierie informatique moderne pour résoudre des problèmes technologiques complexes ;
- contribuer à l'amélioration des capacités d'analyse des données de la CTAB et de l'IPU ;
- collaborer avec les parties prenantes concernées au sein de l'OTAN, des pays de l'Alliance, des pays partenaires et du secteur ;
- remettre des avis à la direction de l'IPU sur les besoins budgétaires de la CTAB ;
- présider des groupes de travail guidés par le renseignement, notamment la conférence annuelle OTAN sur le renseignement sur les menaces cyber ;
- tenir à jour ses compétences concernant les attaques et les menaces cyber actuelles et émergentes ainsi que les failles de sécurité.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La/Le titulaire du poste doit :

- avoir un diplôme universitaire, de préférence dans le domaine de la cyberdéfense, des technologies de l'information, des sciences politiques, de la sécurité internationale ou dans un domaine apparenté ;
- avoir au moins huit ans d'expérience utile, dont au moins cinq en rapport avec les opérations ou l'analyse dans le domaine de la cyberdéfense et deux en lien avec la gestion ou l'encadrement d'une équipe diversifiée ;
- posséder une expérience et des connaissances approfondies concernant les développements techniques dans le panorama des cybermenaces ;
- avoir participé récemment à des activités de production de renseignement sur les menaces cyber (capacités et intentions des acteurs malveillants) et sur les cybervulnérabilités, qui visent à améliorer la connaissance de la situation cyber ;
- être au fait des problématiques et des défis stratégiques auxquels l'Alliance doit faire face, ainsi que de l'environnement géopolitique de l'OTAN ;
- avoir occupé un poste à responsabilités dans le domaine de la cyberdéfense au sein de l'administration publique d'un pays de l'OTAN ou d'une organisation internationale (UE, ONU, OSCE, OTAN, etc.) ;
- avoir travaillé un certain temps dans un service de renseignement ou de sécurité d'un pays de l'Alliance ;

- avoir d'excellentes aptitudes de communication (orale et écrite) et une expérience de la préparation de bulletins d'alerte et de rapports ;
- 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 des interactions entre technologies et politique ;
- une expérience dans le domaine de l'analyse des données, de la science des données ou de l'apprentissage automatique ;
- une expérience de la synthèse d'informations qualitatives et quantitatives provenant d'un large éventail de sources, de la formulation de points de vue originaux, et de la communication sous forme écrite, verbale et graphique.

3. RESPONSABILITÉS PRINCIPALES

Gestion des personnes

Supervise les travaux de la CTAB et donne des orientations et des directives. Confie des tâches dans le cadre des projets dont la CTAB est chargée, en supervise l'exécution et veille à ce que ces projets soient menés à bien dans les délais impartis. Promeut la transparence dans le processus décisionnel, l'égalité des chances pour tous les membres du personnel et un encadrement inclusif. Veille à ce que tous les membres du personnel placés sous sa responsabilité comprennent bien les objectifs de l'Organisation, de la Division et de la Direction. Travaille en collaboration avec la Division Gestion exécutive pour les questions liées au personnel. Fournit régulièrement aux membres de son équipe un retour honnête sur leurs performances, tant de manière informelle, quand la situation s'y prête, qu'au travers du système de mesure et de développement des performances (PRD). Participe à un examen collégial des performances afin d'envisager les possibilités de perfectionnement professionnel et de mobilité pouvant être offertes à chacun(e), de déceler les éléments à fort potentiel et de veiller à ce que des normes communes soient appliquées au cours de ce processus. Participe aux procédures de recrutement destinées à pourvoir les postes vacants au sein de la Division, en suivant les directives OTAN et en cherchant à servir au mieux les intérêts de l'Organisation.

Planification et exécution

Supervise l'établissement des produits de renseignement au sein de la CTAB, et donc le suivi et l'analyse des informations liées au cyber provenant de toutes les sources disponibles, et fournit en temps opportun des évaluations de renseignement opérationnel et stratégique d'intérêt. Coordonne la production et coopère avec les autres organismes de l'architecture du renseignement à l'OTAN. Définit les contributions aux plans de travail à court et à moyen terme et gère la mise en œuvre des projets, de façon à atteindre les objectifs de la Branche. Propose à la chaîne hiérarchique des projets de production en fonction des besoins, de l'évolution de la situation et de l'actualité. Conçoit et établit des processus et des capacités permettant de repérer de manière systématique les *patterns* et tendances d'ordre stratégique dans le cyberespace, et produit des avis éclairés venant

alimenter l'analyse prédictive et le renseignement sur les menaces cyber au profit de l'assurance de la mission et de la défense des réseaux. Propose des pistes permettant d'automatiser et d'innover la capacité OTAN de renseignement sur les menaces cyber.

Gestion des parties prenantes

Établit et entretient des relations de travail étroites avec les services de sécurité et de renseignement des pays de l'Alliance. Assure la liaison nécessaire avec d'autres entités des pays de l'Alliance, les autres divisions du SI et de l'EMI et d'autres autorités de l'OTAN. Noue et entretient des relations avec les partenaires du secteur et avec les organisations internationales (dont l'UE) au profit de la mission de la CTAB. Apporte son concours au Conseil de l'Atlantique Nord, au Comité militaire et à d'autres clients concernés en produisant des analyses approfondies des menaces cyber (exposés, évaluations et autres produits analytiques appropriés).
Est l'interlocutrice/l'interlocuteur clé de la communauté cyber de l'OTAN. Représente l'IPU/JISD aux réunions, conférences et séminaires, selon les besoins. Représente l'IPU à un niveau élevé auprès d'intervenants internes et externes lorsque la directrice/le directeur de l'IPU ou les haut(e)s responsables de la JISD le demandent.

Efficacité organisationnelle

Révise et prépare des exposés, des notes d'orateur, des notes d'information et d'autres produits de renseignement, et fait rapport sur les défis ou questions qui intéressent l'IPU. Facilite l'échange d'informations, dans le respect des procédures appropriées en matière de manipulation de l'information, pour qu'un transfert de connaissances puisse s'opérer au sein de la CTAB et de l'IPU et avec les principaux interlocuteurs cyber. Contribue à la fonction de représentation de l'OTAN en élaborant et en communiquant un message qui serve les intérêts de l'Organisation.

Gestion de projet

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 qui ont une incidence directe sur la CTAB ou l'IPU. Assure la gestion de projets et/ou de programmes, suivant les instructions qui lui sont données par la directrice/le directeur de l'IPU. Apporte son concours à la gestion d'initiatives touchant aux capacités de renseignement cyber ainsi que de toutes les mesures pouvant en découler.
Préside des conférences et ateliers consacrés au renseignement sur les menaces cyber, selon les besoins. Fait des exposés et donne des conférences à des groupes de participants et représente l'Alliance à l'occasion de conférences, d'ateliers ou de séminaires, suivant les instructions reçues. Dirige des réunions bilatérales sur les menaces cyber avec des représentants des services de renseignement des pays de l'Alliance.

Gestion financière

Détermine les ressources financières nécessaires, veille à ce qu'elles soient employées correctement et éclaire la chaîne hiérarchique de la JISD sur le financement annuel approprié. Assume la responsabilité de la gestion du budget lié au développement capacitaire de la CTAB.

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 directrice/du directeur de l’IPU. Elle/Il travaille en étroite concertation avec les autres sections de la Division, 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 d’autres agences de l’OTAN. Elle/Il entretient également de bonnes relations de travail dans son domaine de compétence avec le secteur, avec les pays partenaires et avec les organisations internationales concernées pour les questions touchant à la cyberdéfense.

Nombre de subordonné(e)s direct(e)s : 7
Nombre de subordonné(e)s indirect(e)s : sans objet.

5. COMPÉTENCES

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

- Recherche de l’excellence : crée ses propres critères d’excellence et améliore les performances.
- Promotion du changement : dirige personnellement le changement.
- Clarté et précision : contrôle des données ou des projets.
- Réflexion conceptuelle : applique les concepts acquis.
- Flexibilité : adapte sa propre stratégie.
- Persuasion et influence : prend différentes mesures à des fins de persuasion.
- Initiative : planifie et agit jusqu’à un an à l’avance.
- Aptitude à diriger : stimule l’efficacité de l’équipe.
- Compréhension organisationnelle : comprend le climat et la culture de l’Organisation.
- Maîtrise de soi : réagit avec calme.

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.

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.