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

Director Readiness and Operations - 251868

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 4-Jan-2026
Salary (Pay Basis): 12,722.61 (EUR) Monthly
Grade NATO Grade G23
Clearance Level CTS

Description:

1. SUMMARY

The Cyber and Digital Transformation Division (CDT) is the principal institutional engine to advance the Alliance's agenda on cyber defence, digital transformation, and hybrid resilience. The Division is led by an Assistant Secretary General (ASG), supported by a civilian Deputy ASG and a military Deputy ASG (Flag or General Officer), ensuring a joint leadership model. As integrated civilian-military organisation, the Division combines the strategic insight of the International Staff (IS) with the operational expertise of the International Military Staff (IMS), enabling coherent, credible, and actionable advice to NATO's senior decision-making bodies. In its role as the NATO Chief Information Officer (CIO) function it brings Information and Communications Technology (ICT) coherence across NATO Enterprise's civil and military bodies. The ASG/CDT as NATO CIO is empowered to implement the Allies' vision for the NATO Enterprise, is accountable to the Secretary General and is responsible for the development of Enterprise directives and advice on the acquisition and use of information technologies and services.

The Directorate Readiness and Operations ensures that NATO's digital and cyber capabilities are operationally viable, exercised, and maintained at readiness. It plays a pivotal role in translating developed capabilities into operational outputs and enduring services, supporting real-time cyber defence efforts, digital situational awareness, and service assurance across NATO missions. It leads on training, exercises, operational preparedness, and serves as the primary link with the NATO Integrated Cyber Defence Centre (NICC). Feeding back experiences and lessons identified from operations into strategy, policy, plans, capability development, and readiness, the directorate enables continuous improvement and reinforces NATO's resilience and responsiveness in the information and cyber domains.

The Director, Readiness and Operations provides advise to CDT leadership in cyber and digital matters and directs the execution of operational functions as well as coordinating the NICC and developing and implementing relevant policies and plans. The Director ensures

that new digital capabilities are fully integrated into operations, reliably sustained, and aligned with mission requirements. The incumbent also oversees the development of operational guidance, training, and exercises to maintain readiness across the Alliance and deputises for the DASG, as instructed.

Key challenges the successful candidate will confront in the next three years include:

1. Following the establishment of the NATO Integrated Cyber Defence Centre (NICC) which marked a significant milestone in adopting an integrated civil-military approach to cyber incident response efforts as well as the planning and conduct of Defensive Cyberspace Operations, ensuring that future milestones are kept and the implementation remains a key focus area.

2. As the cyber domain contribution to multi-domain operations (MDO) is of key importance, supporting the further operationalization of the cyber domain to ensure adequate execution of MDO and hence its contribution to deterrence and defence.

3. Ensuring that your team contributes to the ability to synchronize Enterprise and Alliance Operations and Missions network protection efforts, which is a key issue in the mid-to long run.

In addition to completing the application form, including the pre-screening questions, candidates will be asked to summarise their views on the key challenges (and possible other) challenges, and how they would address them if selected for the position. This essay will be evaluated as part of the assessments (see full instructions on how to apply at the end of the vacancy notice).

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- possess a university degree, or an equivalent level of qualification, in information and communications technology or in a cyber-security or STEM related discipline;
- have 15 years' relevant and progressively responsible experience, out of which at least 8 years in cybersecurity functions, leading large, within sizeable governmental organisations or industry;
- have at least 5 years experience in leading, guiding, and developing a diverse team of cybersecurity and information technology professionals (both managers and experts) in a large, multicultural organisation;
- have substantial experience managing programmes or initiatives involving multiple stakeholders and organisational change;
- have strong skills in building consensus, influencing senior stakeholders and navigating complex environments;
- have experience overseeing cybersecurity operations, including incident response, cybersecurity threats and risk management;
- be conversant and have an up-to-date knowledge of current cyber threat vectors, dedicated protective measures and market leading technologies;
- 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:

- a graduate degree (Masters or Ph.D.) in a field relevant for this position;
- previous experience in senior cybersecurity management positions (eg CISO);
- proven experience in developing and implementing security controls and monitoring information security operations;
- deep understanding of current and emerging digital and cybersecurity technologies and how enterprises are employing them to protect digital business;
- certifications relevant for the job in the field of cybersecurity (CISSP, CISM, CCSP, etc.), programme/project management (PMP or PRINCE2, etc.), and information technology (ITIL, COBIT, CGEIT, etc.).

3. MAIN ACCOUNTABILITIES

Vision and Direction

Support the management team of CDT in developing strategic goals and objectives in the area of digital transformation and cyber, aligned with NATO's goals and objectives. Engage with all stakeholders to enhance the coordinated execution of the Alliance's Digital Transformation Implementation Strategy (DTIS), specifically for operational cyber defence and cyber security elements. Provide advice on what emerging digital technology, such as quantum, Artificial Intelligence (AI), and Next Generation Networks, as well as cyber trends are, and how they can be integrated within the NATO context.

Policy Development

Contribute to the overall strategy development by developing operational procedures and improving digital transformation objectives and cyber defence and security posture. Lead the implementation of policies and plans on service assurance and coherence, CIS accreditation, spectrum management, employment of NATO Cyber Rapid Reaction Teams.

Expertise Development

Provide senior guidance and recommendations on both digital readiness/defence and cyber security capabilities. Deliver a significant change for the Alliance and drive cybersecurity improvements across 41 separate NATO civil and military bodies. Contribute to the assessment of external cybersecurity opportunities and threats, and advice on NATO Enterprise cybersecurity capabilities and services required. Advise on cyber defence operations (DCO), cybersecurity, CIS accreditation, incident management, service assurance, spectrum management and specific digital interoperability issues.

Stakeholder Management

Promote and encourage cooperation and collaboration among all stakeholders (enterprise and Allies), ensuring coherence, integration and alignment with overall NATO goals and objectives in areas related to digital transformation, cyber defence and cyber security for the enterprise. Work with both military and civilian stakeholders, across a diverse set of capabilities in a challenging and dynamic environment. Engage and consult with governance and management authorities on requirements, capital investments, operation, maintenance and disposal of the NATO Enterprise's cybersecurity capabilities and services. Develop and

maintain close relationship with the NATO Communications and Information Agency, in particular with the NATO Cyber Security Centre (NCSC), as well as the military command structure, and other relevant senior policy committees and boards.

Representation of the Organization

Represent and communicate cyber and digital transformation objectives and goals, within NATO, as well and with industry and academia, at public events on behalf of the division and NATO HQ, as instructed.

Organisational Efficiencies

Identify and enable cost-effective and innovative shared-solutions across the NATO Enterprise to address relevant cybersecurity functions. Improve NATO's digital and cybersecurity posture across the whole NATO Enterprise through the uplift of fundamental cybersecurity and digital functions. Address fundamental cybersecurity functions from an Enterprise perspective, measuring and monitoring performance, and adapting to new technological challenges to improve the organisation's resilience. Drive the development of shared solutions and ensure compliance to enterprise technology standards, governance processes and performance metrics.

Project Management

Provide Enterprise oversight on cybersecurity issues, and work towards the continual improvement of the NATO Enterprise cyber security and cyber defence posture. Co-lead cyber defence operations (DCO), incident management or spectrum management and serve as Enterprise coordinator for the NICC.

Planning and Execution

Assist the ASG/CDT in exercising their Cybersecurity Single Point of Authority role and respond with agility to changing NATO priorities and to changes in the cybersecurity landscape. Provide strategic direction and oversight for the design, development, and operation of the NATO Enterprise cybersecurity architecture.

People Management

Manage the directorate by cultivating a motivating, inclusive and effective workplace. Provide mentoring, coaching and training opportunities and be available to offer guidance at critical moments. Promote transparency in decision-making, equal access to opportunities for all staff and an inclusive management culture. Identify possible development and mobility opportunities for individuals.

Financial Management

Plan, supervise and ensure financial accountability of the annual budgets dedicated to the portfolio of digital readiness and associated cybersecurity activities.

Knowledge Management

Support the development of knowledge management systems, dashboards and other processes related further to digital maturity and cybersecurity. Oversee the development and dissemination of operational tactics, techniques and procedures (TTPs). Supervise education, training, and exercises to ensure Alliance and NATO Enterprise readiness.

Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

The incumbent reports to the DASG for Capability Development, Readiness and Operations and through him/her to the ASG/CDT as CIO. The incumbent has delegated authority from the NATO CIO and regularly works with the Office of the Secretary General on cybersecurity matters. The incumbent works closely with Allied Command Operations and Allied Command Transformation for cybersecurity and digital matters and is required to operate and engage with senior government and military personnel in NATO and partner nations, NATO civil and military bodies, and in non-NATO entities. The incumbent also liaises with leadership in relevant international organisations, industry and academia, as required.

Direct reports: 8
Indirect reports: 40

5. COMPETENCIES

The incumbent must demonstrate:

- Achievement: Sets and works to meet challenging goals;
- Change Leadership: Champions change;
- Conceptual Thinking: Creates new concepts;
- Developing Others: Provides in-depth mentoring, coaching and training;
- Impact and Influence: Uses complex influence strategies;
- Initiative: Plans and acts for the long-term;
- Leadership: Communicates a compelling vision;
- Organizational Awareness: Understands underlying issues;
- Self-Control: Stays composed and positive even under extreme pressure.

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.

Contract clause applicable:

This is a senior post of specialised political nature in which turnover is required for political reasons. 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. The maximum period of service in this post is six years.

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.

Serving staff will be offered a contract in accordance with the NATO Civilian Personnel Regulations.

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.

Please note that the competition for this post is provisionally scheduled as follows:
Pre-selection testing: **end of January 2026**;
Final selection: **end of February 2026**, in Brussels, Belgium.

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.

Directrice/Directeur pour la préparation et les operations - 251868
Emplacement principal : Belgique-Bruxelles
Organisation : OTAN SI
Horaire : Temps plein
Date de retrait : 4-Jan-2026
Salaire (Base de paie) : 12,722.61 Euro (EUR) Mensuelle
Grade NATO Grade G23
Niveau de l'habilitation de sécurité CTS

Description

1. RÉSUMÉ
La Division Cyber et transformation numérique (CDT) est, au sein de l'OTAN, le principal moteur des travaux relatifs à la cyberdéfense, à la transformation numérique et à la résilience face aux pratiques hybrides. Elle est dirigée par un(e) secrétaire général(e) adjoint(e) (ASG), secondé(e) par deux secrétaires général(e)s adjoint(e)s délégué(e)s (DASG), dont l'un(e) est civil et l'autre est militaire (officier général), suivant un modèle d'encadrement conjoint. En tant qu'entité civilo-militaire intégrée, la division combine l'acuité stratégique du Secrétariat international (SI) et l'expertise opérationnelle de l'État-major militaire international (EMI), ce qui lui permet de formuler des avis cohérents, crédibles et exploitables à l'intention des organes décisionnels de haut niveau de l'OTAN. Exerçant les fonctions d'un directeur des systèmes d'information (CIO) au sein de l'OTAN, la division assure la cohérence des technologies de l'information et de la communication (TIC) au sein des organismes civils et militaires de l'entreprise OTAN. À ce titre, l'ASG/CDT est chargé(e) de concrétiser la vision des Alliés pour l'entreprise OTAN : elle/il rend compte à la/au secrétaire général(e) et est responsable, à l'échelle de l'entreprise OTAN, de l'élaboration des directives et de la formulation des avis concernant l'acquisition et l'utilisation des technologies de l'information et des services informatiques.

Dans ce contexte, la Direction Préparation et opérations a pour rôle de veiller à ce que les capacités numériques et cyber de l'OTAN soient viables sur le plan opérationnel, qu'elles fassent l'objet d'exercices et que leur état de disponibilité opérationnelle soit maintenu. Elle assure une mission essentielle pour ce qui est de traduire les capacités développées en résultats opérationnels et en services durables, et de soutenir en temps réel les efforts touchant à la cyberdéfense, à la connaissance de la situation dans le domaine numérique et à la continuité de service sur l'ensemble des missions de l'OTAN. Elle coordonne les entraînements, les exercices et la préparation opérationnelle, et sert d'interface principale avec le Centre OTAN intégré pour la cyberdéfense (NICC). Elle analyse les expériences passées et les enseignements identifiés dans le cadre d'opérations antérieures et les intègre dans les stratégies, les politiques, les plans, le processus de développement capacitaire et les activités liées à la disponibilité opérationnelle, permettant ainsi une amélioration continue et renforçant la résilience et la réactivité de l'OTAN dans les domaines de l'information et du cyber.

La directrice/Le directeur pour la préparation et les opérations conseille l'équipe dirigeante de la CDT sur les questions cyber et numériques, pilote l'exécution des fonctions opérationnelles, assure la coordination avec le NICC, élabore les politiques et plans appropriés, et veille à leur mise en œuvre. La directrice/Le directeur fait en sorte que les nouvelles capacités numériques soient pleinement intégrées dans les opérations, inscrites dans la durée et en adéquation avec les besoins de la mission. La personne titulaire du poste supervise également l'élaboration de directives opérationnelles, ainsi que l'entraînement et les exercices visant à maintenir la disponibilité opérationnelle à l'échelle de l'Alliance. Elle supplée également la/le DASG, selon les instructions reçues.

Dans les trois prochaines années, la personne retenue pour le poste sera amenée à relever les **grands défis** suivants :

1. elle devra veiller au respect et à la mise en œuvre des étapes qui font suite à la fondation du NICC, laquelle marque une étape importante dans l'adoption d'une approche civilo-militaire intégrée dans la réponse aux cyberincidents et dans la planification et la conduite de cyberopérations défensives ;

2. elle devra poursuivre l'opérationnalisation du milieu cyber, qui occupe une place importante dans les opérations multimilieux (MDO), afin que ces dernières soient exécutées de manière adéquate, renforçant ainsi la contribution du cyber à la dissuasion et à la défense ;

3. elle devra veiller à ce que son équipe aide à synchroniser les efforts déployés pour protéger les réseaux de l'entreprise OTAN et ceux des opérations et missions de l'Alliance, enjeu crucial sur le moyen/long terme.

Outre le formulaire de candidature à remplir (y compris le questionnaire de filtrage), il est demandé aux candidat(e)s de résumer leur point de vue sur ces défis clés (et éventuellement sur d'autres) ainsi que l'approche qu'elles/ils adopteraient pour les relever si le poste leur était attribué. Ce texte sera évalué dans le cadre de la procédure de sélection (voir les instructions complètes sur la manière de postuler à la fin de l'avis de vacance de poste).

2. QUALIFICATIONS ET EXPÉRIENCE ACQUIS ESSENTIELS

La personne titulaire du poste doit :

- posséder un diplôme universitaire ou une qualification équivalente dans le domaine des TIC ou dans un domaine lié à la cybersécurité, ou encore dans une discipline STEM ;
- avoir quinze ans d'expérience pertinente, à des niveaux de responsabilité croissants, dont au moins huit ans dans des postes liés à la cybersécurité, à la tête de grandes équipes au sein d'organisations publiques ou privées de taille importante ;
- avoir au moins cinq ans d'expérience dans la direction, le pilotage et le développement d'une équipe composée de professionnels de la cybersécurité et des technologies de l'information ayant des profils variés (incluant à la fois des gestionnaires et des techniciens) au sein d'une organisation multiculturelle de grande envergure ;
- avoir une expérience approfondie de la gestion de programmes ou d'initiatives impliquant de multiples parties prenantes et un changement organisationnel ;

- avoir de bonnes aptitudes en matière de recherche de consensus, une grande capacité d'influence auprès de parties prenantes de haut niveau, et être capable de travailler dans des environnements complexes ;
- avoir déjà supervisé des opérations de cybersécurité, notamment en matière de réponse aux incidents, de menaces cyber et de gestion du risque :
- être au fait des vecteurs de menace actuels en matière de cybersécurité, des mesures de protection contre ces vecteurs et des technologies de référence sur le marché ;
- 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 considérés comme autant d'atouts :

- un diplôme de master ou de doctorat dans un domaine présentant un intérêt pour le poste ;
- une expérience à un poste de haut responsable dans le domaine de la cybersécurité (par exemple en tant que responsable de la sécurité des systèmes d'information (RSSI)) ;
- une expérience probante de l'élaboration et de la mise en œuvre de mesures de sécurité, ainsi que du suivi d'opérations relatives à la sécurité des informations ;
- une compréhension approfondie des technologies actuelles et émergentes dans le domaine du numérique et de la cybersécurité, ainsi que de la manière dont les entreprises les emploient pour protéger l'activité numérique ;
- des certifications pertinentes pour le poste et en lien avec la cybersécurité (CISSP, CISM, CCSP, etc.), la gestion de programmes/projets (PMP ou PRINCE2, etc.) et les technologies de l'information (ITIL, COBIT, CGEIT, etc.).

3. RESPONSABILITÉS PRINCIPALES

Vision et direction

Aide l'équipe de direction de la CDT à définir les buts et objectifs stratégiques dans le domaine du cyber et de la transformation numérique, conformément aux buts et objectifs de l'OTAN. Interagit avec toutes les parties prenantes afin de favoriser une exécution coordonnée de la stratégie de mise en œuvre de la transformation numérique de l'OTAN (DTIS), en particulier pour ce qui touche à la cyberdéfense opérationnelle et aux aspects relatifs à la cybersécurité. Donne des avis sur les technologies numériques émergentes (telles que les technologies quantiques, l'intelligence artificielle (IA) et les réseaux de communication de nouvelle génération), sur les tendances émergentes dans le domaine cyber, et sur la manière dont elles peuvent être intégrées dans le contexte de l'OTAN.

Élaboration des politiques

Contribue au processus global d'élaboration des stratégies en établissant des procédures opérationnelles, en affinant les objectifs de transformation numérique et en améliorant la posture de cyberdéfense et de sécurité. Pilote la mise en œuvre des politiques et des plans portant sur la fourniture d'un service continu et cohérent, sur l'homologation des systèmes d'information et de communication (SIC), sur la gestion du spectre et sur l'utilisation des équipes de réaction rapide pour la cyberdéfense de l'OTAN.

Développement de l'expertise

Fournit des orientations et des recommandations de haut niveau concernant la maturité et la défense numériques ainsi que les capacités de cybersécurité. Mène à bien un changement important au sein de l'Alliance et améliore les moyens de cybersécurité des 41 organismes civils et militaires de l'OTAN. Contribue à l'évaluation des opportunités et des menaces numériques extérieures, et fournit des avis sur les capacités et les services dont l'entreprise OTAN a besoin en matière de cybersécurité. Fournit des avis portant sur les cyberopérations défensives, la cybersécurité, l'homologation des SIC, la gestion des incidents, la continuité de service, la gestion du spectre ainsi que sur des questions spécifiques relatives à l'interopérabilité numérique.

Gestion des parties prenantes

Promeut et encourage la coopération et la collaboration entre toutes les parties prenantes (qu'il s'agisse d'Alliés ou du secteur privé) afin d'assurer la cohérence et l'intégration des travaux, ainsi que leur alignement avec les buts et objectifs de l'OTAN dans les domaines relatifs à la transformation numérique, à la cyberdéfense, et à la cybersécurité à l'échelle de l'entreprise OTAN. Travaille avec des parties prenantes militaires et civiles sur un ensemble varié de capacités, dans un environnement stimulant et dynamique. Interagit et procède à des consultations avec les autorités de gouvernance et de gestion concernant les besoins, les dépenses d'investissement et l'exploitation, la maintenance et le retrait des capacités et services relatifs à la cybersécurité de l'entreprise OTAN. Établit et maintient des relations étroites avec l'Agence OTAN d'information et de communication – et en particulier avec les Centres des services de cybersécurité de l'OTAN –, avec la structure de commandement militaire ainsi qu'avec d'autres comités et bureaux d'orientation.

Représentation de l'Organisation

Au nom de la division et de l'Organisation, présente et fait connaître les objectifs et les buts en matière de cyber et de transformation numérique, aussi bien au sein de l'OTAN qu'auprès d'acteurs de l'industrie et des milieux universitaires lors d'activités publiques, selon les instructions reçues.

Efficacité organisationnelle

Identifie des solutions partagées innovantes remplissant les fonctions de cybersécurité souhaitées et présentant un bon rapport coût/efficacité, et facilite leur mise en place dans toute l'entreprise OTAN. Améliore la posture de l'OTAN en matière de numérique et de cybersécurité en renforçant les fonctions numériques et de cybersécurité fondamentales dans toute l'entreprise. Examine les fonctions de cybersécurité fondamentales à l'échelle de l'entreprise OTAN, mesure et surveille leurs performances, et conduit l'adaptation aux nouveaux défis technologiques afin d'accroître la résilience de l'Organisation. Encourage le développement de solutions partagées et s'assure de leur conformité avec les normes techniques, les processus de gouvernance et les indicateurs de performance de l'entreprise.

Gestion de projet

Assure la supervision des questions de cybersécurité à l'échelle de l'entreprise OTAN et s'emploie à améliorer constamment la posture de cybersécurité et de cyberdéfense de l'entreprise. Aide à piloter des cyberopérations défensives, des activités de gestion des incidents et de gestion du spectre, et assure, côté entreprise OTAN, la coordination avec le NICC.

Planification et exécution

Aide l'ASG/CDT à exercer son rôle d'autorité unique pour la cybersécurité et s'adapte parfaitement à l'évolution des priorités de l'Organisation et de l'environnement de cybersécurité. Assure la direction stratégique et la supervision de la conception, du développement et de l'exploitation de l'architecture de cybersécurité de l'entreprise OTAN.

Gestion des personnes

Gère la direction en faisant en sorte que le cadre de travail soit motivant, inclusif et propice à l'efficacité. Encadre et accompagne ses collaborateurs, leur propose des formations et se tient à leur disposition pour les conseiller dans les moments décisifs. Promeut la transparence dans le processus décisionnel, l'égalité des chances pour tous les membres du personnel et un encadrement inclusif. Réfléchit aux possibilités de développement professionnel et de mobilité pouvant être offertes à chacun(e).

Gestion financière

Planifie et supervise les budgets annuels dédiés au portefeuille d'activités pour la maturité numérique et aux activités de cybersécurité qui y sont associées, et veille au respect de l'obligation de rendre compte en la matière.

Gestion des connaissances

Contribue à l'élaboration de systèmes de gestion des connaissances, de tableaux de bord et d'autres processus liés à la maturité numérique et à la cybersécurité. Supervise l'élaboration et la diffusion de tactiques, de techniques et de procédures opérationnelles (TTP). Supervise la conduite de formations, d'entraînements et d'exercices pour assurer le niveau de préparation de l'Alliance et de l'entreprise OTAN.

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 l'ASG/CDT, en sa qualité de CIO, par l'intermédiaire de la/du DASG pour le développement des capacités, la préparation et les opérations. Elle a une délégation de pouvoirs du CIO de l'OTAN et elle collabore régulièrement avec le Bureau de la/du secrétaire général(e) pour ce qui touche aux questions de cybersécurité. Elle travaille en étroite collaboration avec le Commandement allié Opérations et avec le Commandement allié Transformation sur les questions liées au numérique et à la cybersécurité, et elle doit travailler et interagir avec de hauts responsables civils et militaires de l'OTAN, des pays membres, des organismes civils et militaires de l'Organisation et d'entités non OTAN. Elle assure la liaison avec les organisations internationales compétentes, avec l'industrie et avec les milieux universitaires, selon les besoins.

Nombre de subordonné(e)s direct(e)s : 8
Nombre de subordonné(e)s indirect(e)s : 40

5. COMPÉTENCES

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

- Recherche de l'excellence : se fixe et s'efforce d'atteindre des objectifs ambitieux.
- Promotion du changement prend fait et cause pour le changement.
- Réflexion conceptuelle crée de nouveaux concepts.
- Valorisation du personnel : assure un mentorat, un accompagnement professionnel et une formation approfondis.
- Persuasion et influence : a recours à des stratégies d'influence complexes.
- Initiative : planifie et agit sur le long terme.
- Aptitude à diriger : communique une vision convaincante.
- Compréhension organisationnelle cerne les enjeux profonds.
- Maîtrise de soi reste calme et positive, même en cas de pression extrême.

6. CONTRAT

Contrat proposé (hors détachement) : contrat d'une durée déterminée de trois ans ; renouvelable pour une période de trois ans maximum.

Clause contractuelle applicable :

Il s'agit d'un poste de haut niveau ayant un caractère politique spécialisé, qui exige une rotation pour des raisons politiques. 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. La durée de service à ce poste n'excède pas six ans.

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.

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 voudra bien noter que le concours pour ce poste est programmé provisoirement comme suit :

Épreuve pré-sélective **fin javier 2026** ;

Epreuves sélectives fin **février 2026**, à Bruxelles (Belgique).

On trouvera de plus amples informations concernant le processus de recrutement et les conditions d'emploi sur le site web de l'OTAN (http://www.nato.int/cps/fr/natolive/recruit-hq-e.htm).

La nomination se fera après vérification des diplômes et des antécédents professionnels de la/du candidat(e) retenu(e) et sous réserve de la délivrance d'une **habilitation de sécurité** par les autorités du pays dont la/le candidat(e) retenu(e) est ressortissant(e), de l'approbation de son **dossier médical** par la/le médecin-conseil de l'OTAN et de l'achèvement du processus d'**accréditation** et de notification par les autorités compétentes.

Dans le cadre de ses procédures de recrutement et de sélection, l'OTAN n'acceptera aucune réponse qui aura été produite, en tout ou en partie, au moyen d'un outil d'intelligence artificielle (IA) générative, notamment d'un modèle conversationnel comme ChatGPT (Chat Generative Pre-trained Transformer) ou de tout autre générateur de texte. L'Organisation se réserve le droit de vérifier si la/le candidat(e) a eu recours à de tels outils. Tout dossier de candidature élaboré, en tout ou en partie, à l'aide d'une application d'IA générative ou créative pourra être rejeté sans autre examen, à la seule discrétion de l'OTAN. Cette dernière se réserve également le droit de prendre toute autre mesure qu'elle jugerait nécessaire.

8. INFORMATIONS COMPLÉMENTAIRES

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

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

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

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

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

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

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

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

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

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

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