

	NATO	NORTH ATLANTIC TREATY ORGANIZATION INTERNATIONAL STAFF
	OTAN	ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD SECRÉTARIAT INTERNATIONAL

VACANCY NOTIFICATION/ NOTIFICATION DE LA VACANCE DU POSTE

Officer, Security Architecture and Cyber Capabilities - 261192

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 27-Sep-2026
Salary (Pay Basis): 8,273.12 (EUR) Monthly
Grade NATO Grade G17
Clearance Level NS

Description

1. SUMMARY

The Cyber and Digital Transformation Division (CDT) leads NATO's digital transformation, cybersecurity and cyber defence efforts, translating NATO priorities into coherent strategies and coordinated delivery across the Alliance to strengthen interoperability, resilience, cybersecurity and operational effectiveness.

The incumbent leads and coordinates the activities related to Capability Architecture within the Cyber Plans and Capabilities Section. They support the Section Head in establishing, maintaining and exploiting security by design in the development of relevant Capability and Solution Architectures. In addition, the incumbent will interact with Industry and academia in order to keep abreast of latest developments in cybersecurity.

2. QUALIFICATIONS AND EXPERIENCE

The incumbent must:

- hold a university degree from an institute of a recognised standing in computer science, cybersecurity, or a similar related field;
- have a minimum of 4 years' experience in information technology, IT application, technology and system architecture, and integration;
- have substantial experience with security architecture projects, designing and/or implementing Communications and Information Services (CIS) security;
- be able to prepare and present complex information technology issues in simple terms to non-technical audiences; and

- have the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; I ("Beginner") in the other.

The following are considered an advantage:

- have experience with IT risks, cybersecurity, services security techniques and auditing, open system architectures and technology evaluation (related security protocols, standards and technologies);
- relevant certifications in Enterprise Architecture, IT service management and regulatory security standards & compliance frameworks (such as CISSP, Zero Trust, TOGAF, ITIL, ISO27001, NIST, CIS, OWASP, etc.); and
- experience in operating within both, on-premise and cloud-based, environments.

3. MAIN ACCOUNTABILITIES

Planning and Execution: Lead the development of Capability Architecture products and artefacts to follow strategic goals and other guidance set by NATO senior governance committees. Develop and maintain cyber capability architectures, including CIS-Security and cryptography. Provide security architecture support for the assessment of Capability Programmes and Plans for Cyber Defence, CIS Security and cryptography. Draft background briefs, progress reports, prepare presentations, and other items, as tasked, including for high-level meetings and management.

Project Management: Provide architecture and interoperability assessments for cyber standalone projects and urgent requirement requests. Maintain control of project and program plans, identify and monitor project implementation risks, provide expertise and leadership in the resolution of exceptions and issues. Assess the security perspective of capability programs in place in NATO nations, as well as NATO civil and military bodies.

Stakeholder Management: Ensure close collaboration with Allied Command Transformation (ACT) and NATO Communications and Information Agency (NCIA) during the development of Capability Architectures and the development of Solution Architectures. Engage with national cyber engineers and industry cyber engineers to ensure capability architectures are technically sound and interoperability is built in by design. Closely coordinate with staff working on the IT security and cybersecurity issues across the NATO enterprise. Represent and speak on behalf of the division, as appropriate, in committees, panels or working groups with industry and academia on matters pertaining to the domain of expertise.

Knowledge Management: Provide support and recommendations, be the point of reference for the NATO Enterprise architectural approach. Ensure relevant architectures conform with all relevant NATO Reference Architectures and applicable regulatory documents. Keep abreast with the latest technology developments in the area of responsibilities and expertise and provide appropriate advice.

Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

Reporting line: The incumbent reports to the Head, Cyber Plans and Capabilities Section.

Interactions: The incumbent works in close cooperation with other team members in the cyber cluster, across the division and HQ, as well as experts in the same field, across the NATO enterprise.

Direct reports: N/A

Indirect reports: N/A

5. COMPETENCIES

The incumbent must demonstrate:

- Analytical Thinking: sees multiple relationships.
- Flexibility: adapts to unforeseen situations.
- Impact and Influence: takes multiple actions to persuade.
- Initiative: is decisive in a time-sensitive situation.
- Organizational Awareness: understands organisational climate and culture.
- Teamwork: cooperates.

6. CONTRACT

Contract to be offered to the successful applicant (if non-seconded): Definite duration contract of three years; possibility of renewal for up to three years, during which the incumbent may apply for conversion to an indefinite duration contract.

Contract clause applicable:

In accordance with the contract policy, this is a post in which turnover is desirable for political reasons in order to be able to accommodate the Organisation's need to carry out its tasks as mandated by the Nations in a changing environment, for example by maintaining the flexibility necessary to shape the Organisation's skills profile, and to ensure appropriate international diversity.

The maximum period of service foreseen in this post is 6 years. The successful applicant will be offered a 3-year definite duration contract, which may be renewed for a further period of up to 3 years. However, according to the procedure described in the contract policy the incumbent may apply for conversion to an indefinite contract during the period of renewal and no later than one year before the end of contract.

If the successful applicant is seconded from the national administration of one of NATO's member States, a 3-year definite duration contract will be offered, which may be renewed for a further period of up to 3 years subject also to the agreement of the national authority concerned. The maximum period of service in the post as a seconded staff member is six years.

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

7. USEFUL INFORMATION REGARDING APPLICATION AND RECRUITMENT PROCESS

Please note that we can only accept applications from nationals of NATO member countries. Applications must be submitted using e-recruitment system, as applicable:

- For NATO civilian staff members only: please apply via the internal recruitment portal ([link](#));
- For all other applications: www.nato.int/recruitment

Before you apply to any position, we encourage you to [click here](#) and watch our video providing 6 tips to prepare you for your application and recruitment process.

Do you have questions on the application process in the system and not sure how to proceed? [Click here](#) for a video containing the information you need to successfully submit your application on time.

When submitting your application, please ensure that your Taleo Candidate Profile is updated and that your CV is correctly uploaded in the Taleo attachments section.

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 reference documents without proper quotes (plagiarism), or any tools available on internet, including but not limited to translation facilities, or generative artificial-intelligence (AI) 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 tools will be rejected without further consideration, and NATO reserves the right to take further steps in such cases as appropriate.

8. ADDITIONAL INFORMATION

NATO is committed to diversity and inclusion, and strives to provide equal access to employment, advancement and retention, independent of gender, age, nationality, ethnic origin, religion or belief, cultural background, sexual orientation, and disability. NATO welcomes applications of nationals from all member Nations, and strongly encourages women to apply.

NATO is committed to fostering an inclusive and accessible working environment, where all candidates living with disabilities can fully participate in the recruitment and selection process. If you require reasonable accommodation, please inform us during your selection process.

Candidates will be required to provide documented medical evidence to support their request for accommodation.

Building Integrity is a key element of NATO's core tasks. As an employer, NATO values commitment to the principles of integrity, transparency and accountability in accordance with international norms and practices established for the defence and related security sector. Selected candidates are expected to be role models of integrity, and to promote good governance through ongoing efforts in their work.

Due to the broad interest in NATO and the large number of potential candidates, telephone or e-mail enquiries cannot be dealt with.

Applicants who are not successful in this competition may be offered an appointment to another post of a similar nature, albeit at the same or a lower grade, provided they meet the necessary requirements.

The nature of this position may require the staff member at times to be called upon to travel for work and/or to work outside normal office hours.

The organization offers several work-life policies including Teleworking and Flexible Working arrangements (Flexitime) subject to business requirements.

Please note that the International Staff at NATO Headquarters in Brussels, Belgium is a non-smoking environment.

For information about the NATO Single Salary Scale (Grading, Allowances, etc.) please visit our [website](#). Detailed data is available under the Salary and Benefits tab.

NATO does not charge any application, processing, training, interviewing, testing or other fee in connection with the application or recruitment process. For more info please [click here](#).

Administratrice/Administrateur (Architecture de sécurité et cybercapacités- 261192

Emplacement principal : Belgique-Bruxelles

Organisation : OTAN SI

Horaire : Temps plein

Date de retrait : 27-sep-2026

Salaire (Base de paie) : 8,273.12 Euro (EUR) Mensuelle

Grade NATO Grade G17

Niveau de l'habilitation de sécurité NS

Description :

1. RÉSUMÉ

La Division Cyber et transformation numérique (CDT) pilote les travaux de l'OTAN en matière de transformation numérique, de cybersécurité et de cyberdéfense, traduisant les priorités de l'Organisation en stratégies cohérentes et en réalisations coordonnées à l'échelle de l'Alliance afin de renforcer l'interopérabilité, la résilience, la cybersécurité et l'efficacité opérationnelle.

Au sein de la Section Planification et développement des capacités cyber, la personne titulaire du poste dirige et coordonne les activités relatives à l'architecture des capacités. Elle aide la/le chef de section à établir, à maintenir et à mettre en œuvre les principes de sécurité dès la conception dans le cadre du développement des architectures liées aux capacités et aux solutions. En outre, elle interagit avec l'industrie et les milieux universitaires afin de se tenir au fait des développements les plus récents en matière de cybersécurité.

2. QUALIFICATIONS ET EXPÉRIENCE

La personne titulaire du poste doit :

- posséder un diplôme de niveau universitaire délivré par un établissement de valeur reconnue dans le domaine de l'informatique, de la cybersécurité ou dans une discipline apparentée ;
- avoir au moins quatre ans d'expérience dans les domaines des technologies de l'information, des applications informatiques, des architectures technologies et systèmes, et de l'intégration ;
- avoir une solide expérience des projets d'architecture de sécurité, ainsi que de la conception et/ou de la mise en œuvre de la sécurité des systèmes d'information et de communication (SIC) ;
- être capable de préparer des sujets complexes relatifs aux technologies de l'information et de les présenter en termes simples à un public non spécialisé ;
- 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.

Seraient considérés comme autant d'atouts :

- une expérience en ce qui concerne les risques informatiques, la cybersécurité, les techniques et les moyens d'audit en matière de sécurité des services, les architectures

de systèmes ouverts et l'évaluation des technologies (protocoles de sécurité, normes et technologies) ;

- des certifications pertinentes en architecture d'entreprise, en gestion de services informatiques et en normes de sécurité et cadres de conformité réglementaires (tels que CISSP, Zero Trust, TOGAF, ITIL, ISO27001, NIST, SIC et OWASP) ;
- le fait d'avoir déjà travaillé à la fois sur site et dans un environnement cloud.

3. RESPONSABILITÉS PRINCIPALES

Planification et exécution – Dirige l'élaboration des produits et des éléments de l'architecture des capacités, suivant les objectifs stratégiques et autres orientations fixés par les hauts comités de gouvernance de l'OTAN. S'emploie à développer et à maintenir des architectures de cybercapacités, notamment pour la sécurité des SIC et la cryptographie. En tant que spécialiste en architecture de sécurité, aide à évaluer les programmes et plans capacitaires pour la cyberdéfense, la sécurité des SIC et la cryptographie. Rédige des notes d'information et des rapports d'activité, et prépare des présentations et d'autres documents, selon ce qui est demandé, notamment pour des réunions et des responsables de haut niveau.

Gestion de projet – Réalise des analyses d'architecture et d'interopérabilité dans le cadre de projets indépendants et de demandes urgentes. Se tient parfaitement au fait des plans de projets et de programmes, identifie les risques pesant sur la mise en œuvre des projets et en assure le suivi, met son expertise et son leadership au service de la gestion des exceptions et de la résolution des problèmes. Évalue, sous l'angle de la sécurité, les programmes capacitaires en place dans les pays de l'OTAN ainsi qu'au sein des organismes civils et militaires de l'Organisation.

Gestion des parties prenantes – Assure une étroite collaboration avec le Commandement allié Transformation (ACT) et l'Agence OTAN d'information et de communication (NCIA) dans le cadre du développement des architectures des capacités et des architectures des solutions. Interagit avec des ingénieurs cyber nationaux et des ingénieurs cyber du secteur industriel afin que les architectures des capacités soient techniquement viables et que l'interopérabilité soit intégrée dès la conception. Collabore étroitement avec les services travaillant sur les questions relatives à la sécurité informatique et à la cybersécurité dans l'ensemble de l'entreprise OTAN. Représente la Division et s'exprime en son nom, lorsqu'il y a lieu, au sein de comités, de commissions ou de groupes de travail ainsi qu'auprès de l'industrie et des milieux universitaires pour les questions relevant de son domaine d'expertise.

Gestion des connaissances – Apporte un soutien, formule des recommandations, et sert de référent(e) s'agissant de l'approche retenue pour l'architecture de l'entreprise OTAN. Veille à ce que les architectures concernées soient conformes à toutes les architectures de référence OTAN pertinentes et aux documents réglementaires applicables. Se tient au fait des développements technologiques les plus récents dans son domaine de compétence et d'expertise, et formule des avis appropriés.

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

4. STRUCTURE ET LIAISONS

Hiérarchie – La personne titulaire du poste relève de la/du chef de la Section Planification et développement des capacités cyber.

Relations de travail – La personne titulaire du poste travaille en étroite coopération avec d'autres membres du pôle cyber, de la Division et du siège, ainsi qu'avec divers experts du même domaine répartis dans toute l'entreprise OTAN.

Nombre de subordonné(e)s direct(e)s : s.o.

Nombre de subordonné(e)s indirect(e)s : s.o.

5. COMPÉTENCES

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

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

6. CONTRAT

Contrat proposé (hors détachement) : contrat d'une durée déterminée de trois ans ; renouvelable pour une période de trois ans maximum, au cours de laquelle le/la titulaire pourra demander qu'il soit transformé en contrat de durée indéterminée.

Clause contractuelle applicable :

Conformément à la politique des contrats, il s'agit d'un poste auquel il est souhaitable, pour des raisons politiques, d'assurer une rotation de manière à pouvoir répondre au besoin qu'a l'Organisation d'exécuter les tâches qui lui sont confiées par les pays dans un environnement en constante évolution, notamment en préservant la souplesse nécessaire à l'adaptation de son profil de compétences, et de veiller au degré de diversité approprié à son caractère international.

La durée de service maximale prévue à ce poste est de six ans. La personne retenue se verra offrir un contrat d'une durée déterminée de trois ans, qui pourra être reconduit pour une période de trois ans maximum. Toutefois, conformément à la procédure décrite dans la politique des contrats, elle pourra demander, au plus tard un an avant l'expiration de la deuxième période, que son contrat soit transformé en contrat de durée indéterminée.

Si la personne retenue est détachée de l'administration d'un État membre de l'OTAN, elle se verra offrir un contrat d'une durée déterminée de trois ans, qui, sous réserve de l'accord des autorités nationales concernées, pourra être reconduit pour une période de trois ans maximum. À ce poste, la durée de service d'un agent détaché n'excède pas six ans.

Les agents en fonction se verront offrir un contrat conforme aux dispositions du Règlement du personnel civil de l'OTAN.

7. INFORMATIONS UTILES CONCERNANT LA PROCÉDURE DE CANDIDATURE ET DE RECRUTEMENT

On notera que seules les candidatures de ressortissant(e)s de pays de l'OTAN pourront être acceptées. Les candidatures doivent être soumises comme suit :

- pour les seuls agents civils de l'OTAN : via le portail de recrutement interne ([lien](#)) ;
- pour toutes les autres candidatures : via le lien www.nato.int/recruitment.

Il est recommandé de commencer par regarder [ici](#) une vidéo proposant six conseils destinés à aider les candidat(e)s à préparer leur dossier.

En outre, on trouvera [ici](#) une vidéo expliquant la marche à suivre sur le portail pour introduire son dossier de candidature et s'assurer de sa réception par l'OTAN dans les délais fixés.

Lors de la soumission de votre candidature, veuillez vous assurer que votre profil de candidat Taleo est à jour et que votre CV est correctement téléchargé dans la section des pièces jointes de Taleo.

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, sur la base de documents de référence non explicitement cités (plagiat) ou au moyen d'outils disponibles sur Internet, y compris, entre autres, d'outils de traduction ou d'outils d'intelligence artificielle (IA) générative. Elle se réserve le droit de vérifier si la personne candidate a eu recours à de tels outils. L'OTAN pourra rejeter sans autre examen tout dossier de candidature élaboré, en tout ou en partie, à l'aide de ces outils. Elle 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](#).