DESCRIPTION DE POSTE
SECRÉTARIAT INTERNATIONAL DE L'OTAN

DIVISION : DIVISION CIVILO-MILITAIRE RENSEIGNEMENT ET SÉCURITÉ (JISD)
BUREAU DE SÉCURITÉ DE L'OTAN (NOS)
BRANCHE SUPERVISION DE LA POLITIQUE ET DE LA SÉCURITÉ (SPOB)
SECTION CYBERSÉCURITÉ

INTITULÉ : Administratrice/administrateur (homologation de sécurité des systèmes d'information et de communication classifiés)

GRADE : G15/G17 (A.2/A.3)

FAMILLE DE POSTES : Activités centrales – Mise en œuvre des politiques et programmes

NIVEAU DE TRAVAIL : V

POSTE N° : JIS0***

CLAUSE CONTRACTUELLE : G

HABILITATION DE SÉCURITÉ : NS

1. RÉSUMÉ

La Division civilo-militaire Renseignement et sécurité (JISD), placée sous l'autorité de la/du secrétaire général(e) adjoint(e) (ASG) pour le renseignement et la sécurité, 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) et directrice/directeur du NOS.

Le NOS est responsable de la coordination générale de la sécurité à l'OTAN entre pays membres et organismes civils et militaires de l'OTAN, ainsi qu'avec les organisations internationales et les pays partenaires avec lesquels l'OTAN coopère. Il est également chargé de la sécurité du siège de l'OTAN et de son personnel à Bruxelles, de la protection de la/du secrétaire général(e), ainsi que de la sécurité et de la sûreté du personnel en mission à l'étranger. Le NOS comprend le Bureau de la directrice/du directeur, la Branche Supervision de la politique et de la sécurité (SPOB), la Branche Sécurité de protection et services de secours (PSESB), l'Équipe Protection rapprochée (CPU) et la Branche Renseignement de sécurité (SIB).

La SPOB veille à ce que la politique de sécurité de l'OTAN soit appliquée dans l'ensemble des organismes et des pays membres de l'Organisation, ainsi que dans les pays non OTAN et les organisations avec lesquels l'OTAN coopère, selon les besoins. Elle élabore la politique et les directives de sécurité, appuie leur mise en application et vérifie leur conformité au travers d'audits de sécurité dans les domaines fonctionnels spécifiques que sont la sécurité concernant le personnel, la sécurité

physique, la sécurité des informations, la sécurité des systèmes d'information et de communication (SIC) – aussi appelée « cybersécurité » –, la sécurité industrielle et la sécurité de protection. La SPOB collabore avec les autres branches de la JISD afin que l'interprétation et l'application de la politique de sécurité se fassent de manière coordonnée et cohérente.

La Section Cybersécurité, qui fait partie de la SPOB, remplit les trois fonctions clés suivantes : (i) homologation de sécurité des SIC de l'OTAN et des services associés, (ii) inspections de sécurité et visites d'examen dans des pays et dans des entités OTAN ou non OTAN, et (iii) élaboration et tenue à jour des politiques et des directives de sécurité concernant les SIC.

Sous la direction de la/du chef de la Section Cybersécurité, la personne titulaire du poste est responsable de l'homologation de sécurité des SIC de l'OTAN et des services associés selon la politique de sécurité de l'Organisation. Elle est le point de contact privilégié des gestionnaires des projets nécessitant une homologation de sécurité et des personnes intervenant dans ces projets, notamment pour ce qui concerne la production et la mise à disposition de supports de formation théorique et pratique sur la cybersécurité et l'homologation de sécurité à l'OTAN. Elle contribue aux visites d'examen dans des entités non OTAN ainsi qu'aux audits de sécurité des SIC de l'OTAN.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La personne titulaire du poste doit :

- posséder un diplôme universitaire – ou une qualification de niveau équivalent – dans le domaine de la cybersécurité ou des systèmes d'information, ou dans un autre domaine scientifique présentant un intérêt pour le poste ;
- avoir trois ans d'expérience dans le domaine de la cybersécurité, acquise de préférence dans le secteur privé, dans une organisation internationale ou au sein d'une autorité nationale de sécurité ou de toute autre administration publique d'un pays de l'OTAN dotée de responsabilités similaires ;
- justifier d'une connaissance et d'une expérience probante de la planification, de l'exécution, de la formulation de conseils et d'orientations, et du suivi en lien avec les dispositions, les programmes, les projets, les procédures d'homologation et les inspections en matière de cybersécurité ;
- avoir une connaissance approfondie des normes internationales de cybersécurité et des bonnes pratiques en la matière ;
- avoir une expérience probante de l'informatique en nuage (*cloud*), de l'informatique en périphérie (*edge*), de l'informatique géodistribuée (*fog*) et de leurs modèles de déploiement ;
- très bien connaître l'un des concepts suivants : DevSecOps, intelligence artificielle, confiance zéro, et sécurité centrée sur la donnée ;
- avoir une expérience probante des appréciations des vulnérabilités et des tests d'intrusion ;
- être capable de rédiger des rapports complets à l'usage des autorités compétentes ;

- justifier d'excellentes aptitudes à la communication écrite et être capable de rédiger des documents en lien avec les SIC ;
- 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 ;
- être disposée à travailler en dehors des heures normales de service.

ACQUIS SOUHAITABLES
Seraient considérées comme autant d'atouts :

- une connaissance de l'OTAN, de sa politique de sécurité et de ses directives complémentaires ;
- une connaissance de *plusieurs* des concepts suivants : DevSecOps, intelligence artificielle, confiance zéro, sécurité centrée sur la donnée, mise en réseau définie par logiciel, architecture orientée services ;
- une ou plusieurs certifications professionnelles dans le domaine de la cybersécurité ;
- une expérience dans le domaine de l'évaluation/la gestion des risques de sécurité (SRA/SRM).

3. RESPONSABILITÉS PRINCIPALES

Développement de l'expertise

Fournit des avis et des orientations en lien avec la cybersécurité aux pays membres et aux organismes civils et militaires de l'OTAN, ainsi qu'à des pays partenaires et à d'autres organisations internationales. Se tient informé(e) des dernières tendances et technologies en matière de cybersécurité. Organise des formations théoriques et pratiques sur l'homologation de sécurité à l'intention des parties prenantes concernées.

Gestion des connaissances

À partir d'exposés, de débats et de recherches, évalue les programmes de sécurité en place dans les pays membres et les organismes civils et militaires de l'OTAN, ainsi que dans des pays non OTAN et d'autres organisations internationales. Crée et tient à jour un référentiel d'information et de connaissance sur les questions de cybersécurité qui doit permettre à la communauté de sécurité d'améliorer sa perception de la situation.

Planification et exécution

Exécute le processus d'homologation de sécurité des SIC de l'OTAN et des services associés. Revoit les documents relatifs à l'homologation de sécurité et, le cas échéant, rédige des rapports sur la décision d'homologation. Organise les procédures de travail liées à l'homologation de sécurité et pilote leur exécution, dans un esprit d'efficacité. Fournit des avis sur ce qui pourrait être fait, dans le respect du règlement de sécurité de l'OTAN, pour améliorer le processus d'homologation de sécurité et son exécution dans les pratiques courantes. Rédige des documents sur le processus et les

procédures de travail relatifs à l'homologation de sécurité et aux questions de cybersécurité, selon les besoins.

Gestion de projet

Organise et exécute le processus d'homologation de sécurité des SIC de l'OTAN, et effectue des inspections dans tous les organismes OTAN afin de vérifier que la politique en vigueur est respectée, selon les instructions de la/du chef de la Section. Assure conseils et coordination dans la planification et la mise en application des dispositions de cybersécurité dans le cadre de projets menés à l'échelle de l'OTAN. Contribue aux inspections de sécurité, aux visites d'examen et aux audits du NOS.

Gestion des parties prenantes

Assure la liaison entre diverses parties prenantes ayant différents intérêts, telles que les autorités opérationnelles des SIC, les autorités de planification et de mise en œuvre des SIC, les prestataires de services SIC et les officiers de sécurité des SIC, selon les demandes, les instructions et les orientations de la/du chef de la Section. Établit des rapports à l'usage des autorités nationales et/ou des autorités de sécurité compétentes.

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

4. STRUCTURE ET LIAISONS

La personne titulaire du poste relève de la/du chef de la Section Cybersécurité de la SPOB. Elle entretient des relations de travail étroites avec les autres membres de la Branche, et plus largement avec les autres membres de la JISD, ainsi qu'avec les parties prenantes d'autres divisions de l'OTAN. Elle entretient des contacts avec de hauts responsables, civils ou militaires, des pays de l'OTAN et des pays partenaires, d'organismes civils et militaires de l'OTAN, ainsi que de pays non OTAN et d'autres organisations.

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

5. COMPÉTENCES

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

- Réflexion analytique : 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.

J.C. Gad Justesen-Jørgensen
Directeur
Ressources humaines de l’OTAN

23/10/2025