NOTIFICATION OF AN "A"GRADE VACANCY
NATO INTERNATIONAL STAFF

OPEN TO NATIONALS OF NATO MEMBER STATES ONLY

LOCATION: NATO Headquarters, Brussels, Belgium

DIVISION: Emerging Security Challenges Division
Cyber Defence Section

TITLE: Officer, Cyber Defence Policy

GRADE: A.4

SECURITY CLEARANCE: COSMIC TOP SECRET

VACANCY N°: 170217

Please note that the competition for this post is provisionally scheduled as follows:

- **Pre-selection testing 4 July 2017;**
- **Final selection on 29 and 30 August 2017, in Brussels, Belgium.**

---

1. SUMMARY

The Emerging Security Challenges Division (ESC) provides a structured approach for NATO to the emerging security challenges of the 21st Century and beyond. These include terrorism, Weapons of Mass Destruction proliferation, cyber threats, as well as risks to energy security. The Division also promotes security cooperation on these challenges through a variety of programmes, in NATO, with Partner nations and with other International Organisations, as appropriate. The Division plays an important role in the implementation of the Wales and Warsaw Summit Declarations on the topics above.

In the Cyber Defence Section, under the direction of the Section Head, the incumbent will be responsible for developing, monitoring, and articulating cyber defence policy and related cyber defence issues. He/she will maintain and develop further updates to NATO's Cyber Defence Policy, as well as coordinate all related activities, including respective committee work.

He/she will be further responsible for coordinating cyber defence activities with Strategic Commands, NATO Agencies, Cooperative Center of Excellence (CCD COE) Tallinn, with members of the Alliance, as well as with other stakeholders on cyber defence related issues, including the cyber defence cooperation with Partner nations. He/she will maintain contacts with other International Organisations active in the field of cyber defence (e.g. EU, UN,

OSCE), as well as with the academic and think tank community and the private sector. He/she will deputise in the absence of the Head of Section.

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL
The incumbent must:

- have a university degree, preferably in the field of cyber defence or in political science, or international relations;
- have at least five years' professional experience in cyber defence and related areas;
- have knowledge and experience in the development, implementation and operations of cyber defence policy, concepts and capabilities;
- be familiar with the strategic issues, security challenges facing the Alliance and NATO's security environment;
- have experience working in a multilateral environment or an environment with a variety of stakeholders from multi-cultural backgrounds;
- possess the following minimum levels in the official languages of NATO (English/French): V ("Advanced") in one and I ("Beginner") in the other;
- be willing to travel and work outside normal office hours.

DESIRABLE
The following would be an advantage:

- having held cyber defence responsibilities at a managerial level in a government of a NATO Nation or in an International Organisation;
- knowledge of International Organisations such as EU, UN, OSCE.

3. MAIN ACCOUNTABILITIES

Policy Development
Develop, review and update NATO's cyber defence policy, concepts and action plans for the approval of appropriate NATO committees. Manage the development and maintenance of cyber defence policy guidance and input to the NATO's defence planning process. Provide policy guidance and support to other stakeholders at the HQ and to cyber defence offices at Strategic Commands, NATO Agencies and relevant Centers of Excellence (e.g. CCD CoE Tallinn).

Project Management
Develop and present strategic and policy-driven cyber defence requirements for NATO-wide capabilities and projects such as the NATO Computer Incident Response Capability (NCIRC) and for the Science for Peace and Security (SPS) Programme.

Expertise Development
Develop and maintain expertise in all matters relating to cyber defence. Maintain expertise to provide direction and guidance to the NATO civil and military bodies on cyber defence capabilities, implementations and procedures. Ensure collaboration with and updates to relevant NATO bodies on issues such as intelligence, counter terrorism, Communication

and Information Systems (CIS) and security committees and communities relevant to cyber defence.

Knowledge Management
Manage the development, review and update of NATO's cyber defence policy, concepts and action plans. Assist in the development and maintenance of Cyber Defence Memorandum of Understanding between Nations and NATO CDMB, and contribute with cyber defence specific knowledge to relevant NATO exercise activity. Manage the development and maintenance of Cyber Threat Assessments relevant to NATO and Allies. Ensure cross-sectional and divisional collaboration. Identify innovations to improve the performance of the section and Division. Share knowledge in a small team of action officers composed of International Staff and NHQC3 Staff.

Representation of the Organization
Make presentations on the subject matter to visitors to NATO HQ, contribute to media briefings by the Division, and represent the Alliance at workshops, conferences and seminars.

Stakeholder Management
Establish and maintain close working relations with national delegations to NATO, including Partner missions, as well as with national officials in capitals, who are responsible for cyber defence. Establish cyber defence liaison with national and International Organisations in support of NATO policy and objectives.

Information Management
Share knowledge on cyber defence and related issues through appropriate channels within the NATO Headquarters as well as with other stakeholders.
Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

The incumbent reports to the Section Head, Cyber Defence and through him/her to the Deputy Assistant Secretary General (DASG) for Emerging Security Challenges. He/she 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, the CCD CoE Estonia and other NATO Agencies. He/she will also maintain good working relations in his/her field of competence with other international organisations (e.g. EU, UN,OSCE) on cyber defence related matters.

Direct reports: N/a
Indirect reports: N/a

5. COMPETENCIES

The incumbent must demonstrate:

- Analytical Thinking;
- Clarity and Accuracy;
- Conceptual Thinking;

- Customer Service Orientation;
- Impact and Influence;
- Initiative;
- Organisational Awareness;
- Teamwork.

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 Regulations.

7. HOW TO APPLY:

Applications **must** be submitted using one of the following links, as applicable:

- For NATO civilian staff members only: please apply via the internal recruitment portal (for more information, please contact your local Civilian HR Manager);
- For all other applications: www.nato.int/recruitment

ADDITIONAL INFORMATION:

NATO as employer values diverse backgrounds and perspectives and is committed to recruiting and retaining a diverse and talented workforce. NATO welcomes applications of nationals from all Member States 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.

Appointment will be subject to receipt of a **security clearance** (provided by the national Authorities of the selected candidate) and approval of the candidate's **medical file** by the NATO Medical Adviser.

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.

Please note that we can only accept applications from nationals of NATO member countries.

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.

NOTIFICATION DE LA VACANCE D'UN POSTE DE GRADE « A »
SECRÉTARIAT INTERNATIONAL DE L'OTAN

POSTE OUVERT AUX SEUL(E)S RESSORTISSANT(E)S DES ÉTATS MEMBRES DE L'OTAN

LIEU D'AFFECTATION : Siège de l'OTAN (Bruxelles – Belgique)

DIVISION : Division Défis de sécurité émergents
Section Cyberdéfense

INTITULÉ : Administrateur/Administratrice (politique de cyberdéfense)

GRADE : A.4

HABILITATION DE SÉCURITÉ : COSMIC TOP SECRET

POSTE VACANT N° : 170217

On voudra bien noter que le concours pour ce poste est actuellement prévu pour les dates suivantes :

- **épreuves de présélection le 4 juillet 2017 ;**
- **sélection finale les 29 et 30 août 2017, à Bruxelles.**

---

1. RÉSUMÉ

La Division Défis de sécurité émergents (ESC) offre à l'OTAN un cadre structuré lui permettant de relever les défis de sécurité émergents du XXI^{e} siècle et au-delà. Parmi ceux-ci figurent le terrorisme, la prolifération des armes de destruction massive, les cybermenaces, ainsi que les risques pesant sur la sécurité énergétique. La Division favorise par ailleurs la coopération en matière de sécurité au travers de toute une série de programmes, à l'OTAN, avec les pays partenaires et avec d'autres organisations internationales, selon les besoins. La Division joue un rôle important dans la mise en œuvre des orientations énoncées dans les déclarations des sommets du pays de Galles et de Varsovie s'agissant des domaines précités.

Sous la direction du/de la chef de la Section Cyberdéfense, le/la titulaire du poste est chargé(e) d'élaborer, de suivre et de coordonner la politique de cyberdéfense et les questions qui y sont liées. Il/elle maintient la politique OTAN de cyberdéfense à jour et élabore des actualisations complémentaires, et coordonne toutes les activités qui y ont trait, y compris les travaux des comités respectifs.

Il/Elle est également chargé(e) de coordonner les activités de cyberdéfense avec les commandements stratégiques, les agences de l'OTAN, le Centre d'excellence pour la cyberdéfense en coopération (CCD COE) de Tallinn, les pays membres de l'Alliance ainsi que d'autres parties prenantes pour ce qui est des questions liées à la cyberdéfense, y compris la coopération en matière de cyberdéfense avec les pays partenaires. Il/Elle entretient des contacts avec d'autres organisations internationales actives dans le domaine de la cyberdéfense (par exemple l'UE, l'ONU et l'OSCE), ainsi qu'avec le monde universitaire, des groupes de réflexion et le secteur privé. Il/Elle supplée le/la chef de la Section en son absence.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS
Le/La titulaire du poste doit :

- avoir un diplôme universitaire, de préférence dans le domaine de la cyberdéfense, des sciences politiques ou des relations internationales ;
- avoir au moins cinq années d'expérience professionnelle dans le domaine de la cyberdéfense et dans des domaines apparentés ;
- avoir une connaissance et une expérience de l'élaboration, de la mise en œuvre et de l'application de la politique et des concepts de cyberdéfense, ainsi que de l'exploitation des capacités dans ce domaine ;
- être familiarisé(e) avec les questions stratégiques, les défis de sécurité auxquels l'Alliance fait face et l'environnement de sécurité de l'OTAN ;
- avoir une expérience professionnelle dans un environnement multilatéral ou un environnement où interviennent de multiples parties prenantes d'origines culturelles diverses ;
- 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 prêt(e) à voyager et à travailler en dehors des heures normales de service.

ACQUIS SOUHAITABLES
Seraient considérés comme autant d'atouts :

- l'exercice de responsabilités de cyberdéfense dans une fonction d'encadrement, au sein du gouvernement d'un pays membre de l'OTAN ou dans une organisation internationale ;
- une connaissance d'organisations internationales telles que l'UE, l'ONU ou l'OSCE.

3. RESPONSABILITÉS PRINCIPALES

Élaboration des politiques
Élabore, examine et actualise la politique, les concepts et les plans d'action de l'OTAN en matière de cyberdéfense, pour approbation par les comités appropriés de l'OTAN. Gère l'élaboration et l'actualisation des orientations générales de cyberdéfense ainsi que les contributions au processus OTAN de planification de défense. Fournit des orientations générales et un soutien aux autres parties prenantes du siège et aux bureaux de

cyberdéfense des commandements stratégiques, des agences de l'OTAN et des centres d'excellence concernés (par exemple le CCD COE de Tallinn).

Gestion de projet
Élabore et présente les besoins de cyberdéfense stratégiques fondés sur les orientations, dans le cadre de capacités et de projets à l'échelle de l'OTAN, tels que la capacité OTAN de réaction aux incidents informatiques (NCIRC) et le programme OTAN pour la science au service de la paix et de la sécurité (SPS).

Développement de l'expertise
Développe et tient à jour son expertise dans toutes les questions ayant trait à la cyberdéfense. Tient à jour son expertise en vue de fournir des orientations et des directives aux organes civils et militaires de l'OTAN sur les capacités de cyberdéfense, la mise en œuvre de ces capacités et les procédures correspondantes. Collabore avec les organismes concernés de l'OTAN et échange des informations actualisées avec eux sur des questions telles que le renseignement, le contreterrorisme, les systèmes d'information et de communication (SIC), ainsi qu'avec les comités et les services travaillant dans le domaine de la cyberdéfense.

Gestion des connaissances
Gère l'élaboration, l'examen et la mise à jour de la politique, des concepts et des plans d'action de l'OTAN en matière de cyberdéfense. Aide à développer et à tenir à jour les mémorandums d'entente sur la cyberdéfense entre les pays et le Bureau de gestion de la cyberdéfense (CDMB) de l'OTAN, et contribue aux activités pertinentes liées aux exercices OTAN en mettant à disposition des connaissances spécifiques en matière de cyberdéfense. Gère la réalisation et la mise à jour des évaluations des cybermenaces concernant l'OTAN et les Alliés. Fait en sorte que les sections et les divisions travaillent en collaboration. Trouve des innovations de nature à améliorer les performances de la Section et de la Division. Partage ses connaissances au sein d'une petite équipe d'administrateurs composés de membres du Secrétariat international et du NHQC3S.

Représentation de l'Organisation
Fait des exposés sur les questions traitées à l'intention des visiteurs présents au siège de l'OTAN, prend part aux séances d'information organisées à l'intention des médias par la Division et représente l'Alliance à des ateliers, conférences et séminaires.

Gestion des parties prenantes
Établit et entretient d'étroites relations de travail avec les délégations des pays auprès de l'OTAN, y compris les missions des partenaires, ainsi qu'avec les fonctionnaires nationaux des capitales chargés de la cyberdéfense. Établit une liaison avec les organisations nationales et internationales dans le domaine de la cyberdéfense, à l'appui de la politique et des objectifs de l'OTAN.

Gestion de l'information
Partage ses connaissances sur la cyberdéfense et sur les questions connexes, par les voies appropriées au siège de l'OTAN, ainsi que par la collaboration avec d'autres parties prenantes.
S'acquitte de toute autre tâche en rapport avec ses fonctions qui pourrait lui être confiée.

4. STRUCTURE ET LIAISONS

Le/La titulaire relève du/de la chef de la Section Cyberdéfense, et, par son intermédiaire, du/de la secrétaire général(e) adjoint(e) délégué(e) (SGAD) de la Division Défis de sécurité émergents. Il/Elle travaille en étroite coordination 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 le CCD COE basé en Estonie et d'autres agences de l'OTAN. Il/Elle entretient également de bonnes relations de travail dans son domaine de compétence avec d'autres organisations internationales (par exemple l'UE, l'ONU et l'OSCE) pour les questions en rapport avec la cyberdéfense.

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

5. COMPÉTENCES

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

- Réflexion analytique
- Clarté et précision
- Réflexion conceptuelle
- Souci du service au client
- Persuasion et influence
- Initiative
- Compréhension organisationnelle
- Travail en équipe

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. COMMENT POSTULER

Les candidatures **doivent** être soumises comme suit :

- pour les seuls agents civils de l'OTAN : via le portail de recrutement interne (pour plus de précisions, veuillez prendre contact avec votre responsable des ressources humaines civiles) ;
- pour toutes les autres candidatures : via le lien www.nato.int/recruitment.

INFORMATIONS COMPLÉMENTAIRES

L'OTAN, en tant qu'employeur, accorde une grande importance à la diversité des parcours et des perspectives, et est déterminée à recruter et à fidéliser des personnes talentueuses issues d'horizons divers. 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.

La nomination se fera sous réserve de la délivrance d'une **habilitation de sécurité** par les autorités du pays dont le/la candidat(e) retenu(e) est ressortissant(e) et de l'approbation de son **dossier médical** par le/la médecin-conseil de l'OTAN.

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.

On notera que seules les candidatures de ressortissant(e)s de pays de l'OTAN pourront être acceptées.

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.