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

Strategic Cyber Threat Analyst (230121)

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 19-Mar-2023
Salary (Pay Basis): 6,211.72Euro (EUR) Monthly
Grade: NATO Grade G15-G17
Clearance Level: CTS
Description

1. SUMMARY

The Joint Intelligence and Security Division (JISD), under the leadership of the Assistant Secretary General for Intelligence and Security (ASG I&S), comprises two principal pillars: Intelligence – headed by the Deputy ASG for Intelligence; and the NATO Office of Security (NOS) – headed by the Deputy ASG for Security.

Intelligence is responsible for ensuring the situational awareness of the North Atlantic Council and the Military Committee, for the analysis of the indications and warnings in support of the NATO Crisis Response System and for the development of intelligence policies and capabilities for NATO. Its functional areas address: intelligence analysis and production, intelligence policy and capability development.

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

The Cyber Threat Analysis Branch (CTAB) is responsible for providing evidence-based assessments of the cyber threat landscape to empower NATO stakeholders to make risk-informed decisions. The multidisciplinary team combines all-source data with cutting edge technologies to support and enhance the Alliance leaderships' understanding on the nature of cyber competition and conflict. CTAB systematically identifies strategic patterns and trends in cyber space and generates tailored insights to support network defence and mission assurance with predictive analysis, cyber threat intelligence, and threat hunting. The Cyber Threat Analyst is assigned to the CTAB.

S/he will be responsible for a wide range of cyber-related tasks, including the production of cyber threat reporting and will be primarily responsible for:

- Cyber threat intelligence analysis – track, pivot, and enrich threat actor tradecraft
- Investigation of raw telemetry to inform decisions about detection and response, and provide a comprehensive understanding of cyber threat actors' activities. Maintain campaign history to prioritise security detection on high impact threats.
- Geopolitical intelligence analysis – research, analyse, and produce intelligence assessments, including threat estimates and briefs related to region-specific international and domestic military, economic, trade, technology priorities, developments and perspectives with a nexus to cyberspace.
- Production and briefings – generate written (and oral) strategic reports for various stakeholders. Communicate actionable insights based on finished intelligence analysis, including in support of senior-level decision-making.
- Provide advice on operational and defence policy planning matters in support of NATO's cyber defence initiatives;
- Contribute to scenario development and the execution of cyber defence exercises;
- Contribute to the development and presentation of strategic and policy-driven cyber threat projects for JISD capabilities and projects;
- Support engagement with partners, with a focus on industry and academia;

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- possess a university degree, preferably in the field of cyber security, information technology, or in political science, international security or related studies;
- have at least 3 years in-depth experience in the area of cyber operations or analysis;
- have at least 2 years related experience to the tasks described for the post;
- have a solid knowledge of current international security developments, and an understanding of the Alliance's political-military decision-making process;
- have excellent drafting oral communications skills, and have experience preparing threat assessments, intelligence reports, and speaking notes for senior officials;
- possess the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; II ("Elementary") in the other.

DESIRABLE

The following would be considered an advantage:

- having held cyber security responsibilities in a government of a NATO Nation or in an International Organisation such as EU, UN, OSCE or NATO;
- knowledge of the civil and military structure of the Alliance, particularly regarding the functioning of NATO HQ and the NATO committee structure;
- have professional experience in policy development, coordination, and implementation;
- have experience working with industry and developing public-private partnerships dealing with cyber defence at both strategic and technical levels;
- recent experience in activities that derive intelligence on cyber threats (capabilities and intent of cyber threat actors) and cyber vulnerabilities to assist in developing cyber situational awareness;
- experience in project management.
- working knowledge of another language.

3. MAIN ACCOUNTABILITIES

Planning and Execution

Using all means available, investigate cyber threats to NATO and its Allies. Share knowledge on cyber threats and related issues via briefings and reports in order to support decision making by the appropriate authorities. Collaborate with appropriate channels within the NATO HQ as well as with other stakeholders, such as the Office of the CIO, NCIA, Allied Command Operations and counterparts in NATO nations.

Policy Development

Contribute to the development of policies, directives and guidance documents on cyber threats and related issues. Support the development of concepts and policies on technical and operational aspects and provide advice as appropriate.

Knowledge Management

Support the development, review and update of NATO's cyber threat playbooks and other analytical products related to cyber security. Draft background briefs, presentations and geopolitical intelligence assessments related to cyberspace for a variety of NATO and partner stakeholders. Contribute with specific cyber defence knowledge to relevant NATO exercise, training and education activities. Collaborate with appropriate channels within the NATO HQ as well as with other stakeholders, such as the NATO communications and Information Agency, Allied Command Operations and counterparts in NATO Allies.

Stakeholder Management

Establish and maintain close working relationships with national Delegations to NATO, as well as with national officials and experts who are responsible for cyber defence. Build and work effectively through communities of interest with other NATO stakeholders to achieve cyber defence policy objectives. Maintain cyber defence liaison with national and International Organisations in support of NATO policy and objectives. Participate in internal working groups and task forces, as required.

Project Management

Define priorities for and contribute to the development and presentation of technical and operational cyber defence requirements for NATO-wide capabilities and projects, including on aspects related to governance, finance, and delivery. Assist in development and presentation of technical and operational cyber defence requirements for NATO-wide capabilities and projects.

Expertise Development

Develop and maintain expertise in all matters related to cyber defence. Develop and maintain expertise to provide direction and guidance to NATO civil and military bodies on cyber defence policy issues, including operational and technical aspects. Monitor and ensure collaboration with and updates/briefings to NATO bodies and communities relevant to cyber defence. Keep abreast of on-going issues in relevant areas that affect the work of the Section, and maintain broad general knowledge of the Organization and its structure.
Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

The incumbent reports to the Head, Cyber Threat Assessment Branch. S/he will work in close coordination with other sections within the division, as well as with other divisions in the International Staff, with the NATO Military Authorities, with national delegations as well as Alliance capitals, and other NATO Agencies. S/he will also maintain good working relations in her/his field of competence with partner countries, other International Organisations and industry on cyber security related matters.

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

5. COMPETENCIES

The incumbent must demonstrate:

- Analytical Thinking: Sees multiple relationships;
- Clarity and Accuracy: Checks own work.
- Conceptual Thinking: Applies learned concepts.
- Flexibility: Adapts to unforeseen situations;
- Impact and Influence: Takes multiple actions to persuade;
- Initiative: Is decisive in a time-sensitive situation;
- Organisational Awareness: Understands organisational climate and culture;
- Teamwork: Solicits inputs and encourages others.

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.

NOTE: Irrespective of previous qualifications and experience, candidates for twin-graded posts will be appointed at the lower grade. Advancement to the higher grade is not automatic, and will not normally take place during the first three years of service in the post.
Under specific circumstances, serving staff members may be appointed directly to the higher grade, and a period of three years might be reduced by up to twenty four months for external candidates. These circumstances are described in the IS directive on twin-graded posts.

7. 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

Please note that at the time of the interviews, candidates will be asked to provide evidence of their education and professional experience as relevant for this vacancy.
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.
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).

8. ADDITIONAL INFORMATION

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

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

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

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

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

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

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

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

Analyste stratégique des menaces cyber, Branche Analyse des menaces cyber (CTAB) (230121)

Emplacement principal : Belgique-Bruxelles
Organisation : OTAN SI
Horaire : Temps plein
Date de retrait : 19-mars-2023
Salaire (Base de paie) : 6 211,72Euro (EUR) Mensuelle
Grade : NATO Grade G15-G17
Niveau de l'habilitation de sécurité : CTS
Description

1. RÉSUMÉ

La Division civilo-militaire Renseignement et sécurité (JISD), placée sous l'autorité de la/du secrétaire général(e) adjoint(e) pour le renseignement et la sécurité (ASG/I&S), se compose de deux grands piliers : le pilier « renseignement », dirigé par la/le secrétaire général(e) adjoint(e) délégué(e) pour le renseignement (DASG/I), et le pilier « sécurité », à savoir le Bureau de sécurité de l'OTAN (NOS), dirigé par la/le secrétaire général(e) adjoint(e) délégué(e) pour la sécurité (DASG/S).

Le pilier « renseignement » est chargé de faire en sorte que le Conseil de l'Atlantique Nord et le Comité militaire aient une bonne connaissance de la situation, d'analyser les indices et les critères d'alerte à l'appui du système OTAN de réponse aux crises, et de mettre en place pour l'OTAN des politiques et des capacités en matière de renseignement. Ses domaines de compétence sont l'analyse et la production du renseignement, ainsi que l'élaboration des politiques et le développement des capacités en matière de renseignement.

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

La Branche Analyse des menaces cyber (CTAB) est chargée d'établir des évaluations du panorama des menaces cyber fondées sur des données probantes afin que les acteurs OTAN soient en capacité de prendre des décisions éclairées en tenant compte des risques. Cette équipe pluridisciplinaire agrège ainsi des données de toutes sources en utilisant des technologies de pointe pour aider les dirigeants de l'Alliance à comprendre plus finement la nature de la compétition et de l'affrontement dans l'espace cyber. La CTAB s'emploie par ailleurs à repérer de manière systématique les *patterns* et tendances d'ordre stratégique dans le cyberespace et produit des avis éclairés venant alimenter l'analyse prédictive, le renseignement sur les menaces cyber et la chasse aux menaces au profit de l'assurance de la mission et de la défense des réseaux. L'analyste des menaces cyber est affecté(e) à la CTAB.

Elle/Il est chargé(e) de toute une séries de tâches cyber, notamment de la production de rapports sur les menaces cyber, et principalement des tâches suivantes :

- Analyse du renseignement sur les menaces cyber – suivre les activités des acteurs malveillants, « pivoter » sur des événements et enrichir les connaissances relatives aux modes opératoires des attaquants.
- Étudier des données brutes dans le but d'éclairer les décisions touchant à la détection des menaces et aux réponses à y apporter, et offrir une grille d'interprétation complète des activités malveillantes dans le cyberespace. Tenir un historique des campagnes pour cibler les menaces à haut pouvoir destructeur à traiter en priorité.
- Analyse du renseignement géopolitique – rechercher, analyser et produire des évaluations de renseignement, notamment des estimations de la menace et des synthèses concernant les priorités, les évolutions et les perspectives technologiques, commerciales, économiques et militaires propres à des régions données, au niveau national et international, le tout en lien avec le cyberespace.
- Livrables et exposés – préparer des rapports stratégiques écrits (et oraux) à l'intention de diverses parties prenantes. Fournir des avis actionnables, basés sur des analyses de renseignement abouties, pour des décideurs de haut niveau.
- Établir des avis sur des questions de planification opérationnelle et de planification des politiques de défense à l'appui d'initiatives en matière de cyberdéfense de l'OTAN.
- Contribuer à l'élaboration des scénarios et à l'exécution des exercices de cyberdéfense.
- Contribuer à l'élaboration et à la présentation de projets liés aux cybermenaces, qu'ils soient d'ordre stratégique ou politique, pour des capacités et des projets JISD.
- Soutenir les interactions avec les partenaires, et plus particulièrement avec l'industrie et le monde universitaire.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La/Le titulaire du poste doit :

- avoir un diplôme universitaire, de préférence dans le domaine de la cybersécurité, des technologies de l'information, des sciences politiques, de la sécurité internationale ou dans un domaine apparenté ;
- avoir au moins trois ans d'expérience approfondie dans le domaine des opérations ou de l'analyse cyber ;
- avoir au moins deux ans d'expérience dans les tâches figurant dans la présente description de poste ;
- avoir de solides connaissances lui permettant de suivre les développements dans le domaine de la sécurité au niveau international et avoir une bonne connaissance du processus décisionnel politico-militaire de l'Alliance ;
- avoir d'excellentes compétences de rédaction et de communication orale, et avoir une expérience de la préparation d'évaluations de la menace, de comptes rendus de renseignement et de notes d'orateur pour de hauts responsables ;
- avoir au minimum le niveau de compétence V (« avancé ») dans l'une des deux langues officielles de l'OTAN (anglais/français), et le niveau II (« élémentaire ») dans l'autre.

ACQUIS SOUHAITABLES

Seraient considérées comme autant d'atouts :

- une expérience à un poste à responsabilités dans le domaine de la cybersécurité au sein de l'administration publique d'un pays membre de l'OTAN ou d'une organisation internationale telle que l'UE, l'ONU, l'OSCE ou l'OTAN ;

- une connaissance de la structure civile et militaire de l'Alliance, et en particulier du fonctionnement du siège et de la structure des comités de l'OTAN ;
- une expérience professionnelle de l'élaboration, de la coordination et de la mise en œuvre de politiques ;
- une expérience des relations avec l'industrie et de la mise en place de partenariats public-privé pour la cyberdéfense, tant au niveau stratégique que technique ;
- une expérience récente dans des activités de production de renseignement sur les menaces cyber (capacités et intentions des acteurs malveillants) et sur les cybervulnérabilités pour aider à développer la connaissance de la situation cyber ;
- une expérience de la gestion de projet.
- une connaissance pratique d'une autre langue.

3. RESPONSABILITÉS PRINCIPALES

Planification et exécution

Analyse, en utilisant tous les moyens disponibles, les menaces cyber qui pèsent sur l'OTAN et les Alliés. Partage ses connaissances sur les menaces cyber et les questions s'y rattachant dans des exposés et des rapports, afin d'éclairer les autorités compétentes dans leur prise de décision. Collabore avec les interlocuteurs appropriés au siège de l'OTAN, ainsi qu'avec d'autres parties prenantes telles que le Bureau du directeur des systèmes d'information (OCIO), l'Agence OTAN d'information et de communication (NCIA), le Commandement allié Opérations (ACO) et ses homologues dans les pays de l'OTAN.

Élaboration des politiques

Contribue à l'élaboration des politiques, des directives et des documents d'orientation sur les menaces cyber et les questions s'y rattachant. Soutient l'élaboration de concepts et de politiques touchant à des aspects techniques et opérationnels, et formule des avis en tant que de besoin.

Gestion des connaissances

Contribue à l'élaboration, à l'examen et à la mise à jour des manuels d'instructions sur les menaces cyber et d'autres produits analytiques en matière de cybersécurité. Prépare des notes d'information, des présentations et des évaluations de renseignement géopolitiques sur le cyberespace à l'intention de différentes parties prenantes (OTAN et partenaires). Contribue, grâce à ses connaissances particulières de la cyberdéfense, aux exercices, entraînements et formations de l'OTAN en la matière. Collabore avec les interlocuteurs appropriés au sein du siège de l'OTAN, ainsi qu'avec d'autres acteurs tels que l'Agence OTAN d'information et de communication, le commandement allié Opérations ou ses homologues dans les pays de l'OTAN.

Gestion des parties prenantes

Établit et entretient d'étroites relations de travail avec les délégations des pays auprès de l'OTAN, ainsi qu'avec les responsables et experts chargés de la cyberdéfense dans les pays. Met en place des communautés d'intérêt avec d'autres parties prenantes de l'OTAN et travaille efficacement avec celles-ci, le but étant d'atteindre les objectifs de la politique de cyberdéfense. Se tient en 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.

Prend part aux travaux des groupes de travail et des équipes spéciales internes, le cas échéant.

Gestion de projet

Définit les priorités concernant les besoins techniques et opérationnels en matière de cyberdéfense pour des capacités et des projets à l'échelle de l'OTAN, y compris sur des aspects liés à la gouvernance, aux moyens financiers et à leur concrétisation, et contribue à leur élaboration et à leur présentation. Aide à définir et à présenter les besoins en matière de cyberdéfense, qu'ils soient d'ordre technique ou opérationnel, pour des capacités et des projets à l'échelle de l'OTAN.

Développement de l'expertise

Développe et actualise son expertise pour toutes les questions ayant trait à la cyberdéfense. Approfondit et entretient ses connaissances en vue de fournir des orientations et des directives aux organes civils et militaires de l'OTAN sur les questions de politique de cyberdéfense, notamment les volets techniques et opérationnels. Vérifie et fait en sorte qu'il y ait collaboration avec les organes et communautés OTAN présentant un intérêt pour la cyberdéfense, et assure des points de situation et exposés à ces acteurs. Se tient informé(e) des problèmes se posant dans des domaines connexes et affectant les travaux de la Section, et cultive ses connaissances générales de l'Organisation et de ses structures.
S'acquitte de toute autre tâche en rapport avec ses fonctions qui pourrait lui être confiée.

4. STRUCTURE ET LIAISONS

La/Le titulaire du poste relève de la/du chef de la Branche Analyse des menaces cyber. Elle/Il 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 d'autres agences de l'OTAN. Elle/Il entretient également de bonnes relations de travail avec les pays partenaires, d'autres organisations internationales et le secteur privé pour les questions de cybersécurité ayant trait à son domaine de compétence.

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

5. COMPÉTENCES

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

- Réflexion analytique : discerne les relations multiples.
- Clarté et précision : vérifie son travail.
- Réflexion conceptuelle : applique les concepts acquis.
- 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 : sollicite des contributions et encourage les autres.

6. CONTRAT
Voir la version anglaise.

7. PROCESSUS DE RECRUTEMENT
Voir la version anglaise.

8. INFORMATIONS COMPLÉMENTAIRES
Voir la version anglaise.