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

YPP, Cyber Policy and Threat Intelligence - 241418

Primary Location Belgium-Brussels
Other Locations Italy-Naples, Belgium-Mons
NATO Body NATO International Staff (NATO IS)
Schedule Full-time
Application Deadline 27-October-2024, 11:59:00 PM
Salary (Pay Basis) 4,771.04Euro (EUR) Monthly
Grade NATO Grade G11

Description

The Young Professionals Programme (YPP)

Through times of crisis and peace, NATO has safeguarded our freedom and security for 75 years and counting. Threats evolve every day and NATO is continuing to adapt to keep us safe. Together we will make sure our Alliance remains ready today to face the challenges of tomorrow.

We are launching an accelerator for your international career – the third cycle of our Young Professionals Programme (YPP). Through this global three-year programme, you will experience the frontline of a political and military alliance and start a journey of personal and professional development in a diverse and inclusive work environment. Together, we will enable NATO to:

- Address existing and emerging global challenges with security implications;
- Facilitate political consultation and dialogue between Nations;
- Leverage innovation, science and technology to support peace and security;
- Stay ahead in cutting-edge domains such as cyber defence and aerospace;
- Support multiple operations on land, at sea and in the air around the world;
- Fight terrorism, piracy and human trafficking at a global level; and,
- Run crisis management exercises that mobilize thousands of people and items of equipment.

Do you want to make a difference and help protect close to one billion people across 32 NATO member states, including your own? If you are ready to take on this challenge, and are a national of a NATO member state, hold a Master's degree and have at least one year of work experience, then apply for the YPP.

With you, we are stronger.
#WeAreNATO

Your role

During the three years of the programme, you will be assigned to three different NATO bodies:

Year	Year 1	Year 2	Year 3
NATO body	NATO International Military Staff (IMS) – NATO HQ - NATO Digital Staff (NDS)	Allied Command Operations (ACO) – NATO Communications & Information Systems Group (NCISG)	Allied Command Operations (ACO) – JFC Naples
Work area	**Cyber Defence & Emerging Technologies**	**Cyber Defence & Emerging Technologies**	**Cyber Defence & Emerging Technologies**
Placement	**Brussels, Belgium**	**Mons, Belgium**	**Naples, Italy**

For more information, please see the path narrative here. You can also find more information about the NATO bodies here & the NATO Young Professionals Programme here.

This is an opportunity for you to apply your knowledge and skills in the broader area of **Cyber Policy and Threat Intelligence.** As you gain experience, you will be given increasing responsibilities, such as:

- Supporting NATO's efforts in systematically introducing innovation in defence planning and capability development processes and activities;
- Supporting a secure conduct of the Alliance's operations and business through the provision of scientific, technical, acquisition, operations, maintenance, and/or sustainment support in the cyber & EDTs domains;
- Contributing to elements of the entire lifecycle of cyber defence capabilities development, from definition of requirements to planning, delivery and retirement;
- Staying abreast on the current cyber threats from internal and publicly available external sources and assessing risk to NATO and its Member States;
- Applying data and insights from operational incidents to strengthen existing, as well as develop new cyber defence capabilities, policies, products and processes;
- Providing IT security SME knowledge and support during applicable IT security incidents;
- Contributing to conducting cyber security operations, participating in incident management and associated coordination and support activities;
- Providing actionable intelligence to Cyberspace Situation Awareness (CySA) security analysts, Threat and Vulnerability Management, Global Physical Security, global business units, and industry partners on cyber security-related matters;
- Collaborating with SOC Analysts, Security Engineering, and Security Architecture, Threat and providing documentation to maintain, develop and create runbooks and SOPs for CTI and CySA;
- Analysing malicious traffic and IOCs hits for attributing to threat actors;
- Researching and providing reports on attacker campaigns as required. Analysing and developing documents, and presenting general & technical presentations on security threats to business units and Information Security Risk Management personnel;
- Informing the Strategic Level about military implications of technological innovation; and,
- Reviewing weekly, monthly and on-demand threat intelligence reports. Contributing to the measurement of the effectiveness of the cyber threat intelligence within NATO;
- Contributing to the integration of cyber threat intelligence in NATO's cyber defence mechanisms and controls; and
- Researching new trends within the areas of responsibilities of cyber defence & EDTs.

Who we are looking for

The changing pace of the world demands that NATO and its people remain flexible, eager to learn and able to work effectively with a variety of stakeholders from diverse backgrounds. For an YPP position, we are looking for candidates **with at least one year of professional experience**.

For the **YPP, Cyber Policy and Threat Intelligence** path, we are generally interested in the following educational backgrounds:

- Master's degree in the field of cyber studies, international security, engineering, information and communication technology, computer science;
- Any other degree that you believe can be useful to the area of **Cyber Policy and Threat Intelligence** – let us know how your knowledge and skills can be applied!

Any of the following experience or skills would be considered as an asset:

- Experience in the area of cyber operations or analysis, or in relevant position for the path;
- Knowledge of security software and familiarity with cyber security regulations;
- Comprehensive understanding of the principles of computer and communication security, networking, and the vulnerabilities of modern operating systems and applications;
- Experience in development and implementation of computer security or EDTs policies;
- Interest in hacking and activities that derive intelligence on cyber threats (capabilities and intent of cyber threat actors) and cyber vulnerabilities;
- Experience in malware protection technologies, malicious code techniques and associated countermeasures;
- Strong passion for information technology & EDTs with a strong commitment to maintaining and improving oversight on technology evolution;
- Interest in business, information, application, technology and system architecture and integration;
- Knowledge of cyber threat intelligence lifecycle, levels, sources, and products;
- Experience in using and managing threat intelligence platforms;
- Knowledge of intrusion detection systems, and security information and event management (SIEM) systems;
- Experience with qualitative and quantitative analytical methodologies and technologies;
- Any additional training/certification(s) related to cyber defence & emerging technologies (such CEH, CompTIA, SANS etc) and project or programme management certification;
- Strong analytical & drafting skills;
- Proactivity, can-do attitude & willingness to learn and share information; and,
- Teamwork, excellent communication, facilitation and interpersonal skills.

What we offer

NATO will offer the Young Professionals:

- An experience of a lifetime at the forefront of an international organization where you'll have the opportunity to develop your skills and expand your professional network;
- A diverse and stimulating work and personal experience where you will be assigned to three different NATO bodies around the globe, one each year; and,
- A competitive salary and other benefits, including excellent health insurance and a generous annual leave package of 30 days

Are you interested in being part of NATO and the YPP? **Apply by 27 October 2024 [23:59 – Brussels time]**

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)

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.

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.

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.

Programme pour les jeunes talents – Politique cyber et renseignement sur les cybermenaces - 241418

Emplacement principal Belgique-Bruxelles
Autres emplacements Italie-Naples, Belgique-Mons
Organisation OTAN SI
Horaire Temps plein
Date de retrait 27-Octobre-2024, 23:59:00
Salaire (Base de paie) 4 771,04Euro (EUR) Mensuelle
Grade NATO Grade G11

Description

Programme pour les jeunes talents (YPP)

Depuis plus de 75 ans, l'OTAN préserve la liberté et la sécurité des citoyens de ses pays membres, en temps de crise comme en temps de paix. Face à des menaces qui évoluent sans cesse, elle s'adapte en permanence pour demeurer à même d'assurer notre sécurité. Ensemble, faisons-en sorte que l'Alliance reste prête à relever les défis qui l'attendent !

L'OTAN lance le troisième appel à candidatures dans le cadre du programme pour les jeunes talents, véritable tremplin vers une carrière à l'international. En participant à ce programme, d'une durée de trois ans, vous serez immergé(e) au cœur d'une alliance politico-militaire et vous développerez vos compétences personnelles et professionnelles d'un bout à l'autre de votre parcours, dans un environnement de travail inclusif qui valorise la diversité. Ensemble, nous aiderons l'OTAN :

- à faire face, aujourd'hui comme demain, aux défis mondiaux ayant des incidences en matière de sécurité ;
- à favoriser la concertation et le dialogue politiques entre pays ;
- à mettre l'innovation, la science et la technologie au service de la paix et de la sécurité ;
- à conserver une longueur d'avance dans des domaines de pointe tels que la cyberdéfense et l'aéronautique ;
- à soutenir de multiples opérations terrestres, maritimes et aériennes aux quatre coins du globe ;
- à lutter contre le terrorisme, la piraterie et la traite des êtres humains au niveau mondial ;
- à mener des exercices de gestion de crise mobilisant des milliers de personnes et toute une panoplie d'équipements.

Vous souhaitez aider l'OTAN à protéger ses 32 pays membres, dont le vôtre, et ainsi mettre vos compétences au service d'un milliard de personnes ? Vous êtes ressortissant(e) d'un pays de l'OTAN, vous possédez un diplôme de master et vous avez une expérience professionnelle d'au moins un an ? Alors posez votre candidature au programme pour les jeunes talents !

Ensemble, nous serons plus forts.
#WeAreNATO

Vos fonctions

Dans le cadre du programme, vous serez affecté(e) successivement à trois organismes OTAN, pour une durée d'un an à chaque fois :

Année	1	2	3
Organisme OTAN	État-major militaire international (EMI) – Siège de l'OTAN – Secrétariat numérique de l'OTAN (NDS)	Commandement allié Opérations (ACO) – Groupe Systèmes d'information et de communication de l'OTAN (NCISG)	Commandement allié Opérations (ACO) – JFCNP
Domaine d'activité	**Cyberdéfense et technologies émergentes**	**Cyberdéfense et technologies émergentes**	**Cyberdéfense et technologies émergentes**
Lieu d'affectation	**Bruxelles (Belgique)**	**Mons (Belgique)**	**Naples (Italie)**

Pour plus d'informations, consultez le descriptif de la filière Politique cyber et renseignement sur les cybermenaces. Vous pouvez aussi cliquer ici pour en apprendre plus sur les organismes participants, et là pour en savoir plus sur le programme lui-même.

Vous serez amené(e) à mettre en pratique vos connaissances et vos compétences dans les domaines de la **politique cyber et du renseignement sur les cybermenaces**. À mesure que vous acquerrez de l'expérience, vous vous verrez confier des responsabilités de plus en plus grandes. Il pourra notamment vous être demandé :

- de contribuer à l'action de l'OTAN en veillant à ce que l'innovation fasse partie intégrante des processus et activités de planification de défense et de développement des capacités ;
- de contribuer à la sécurité des opérations et des activités de l'Alliance en fournissant, dans le domaine cyber et dans celui des TE/TR, une aide scientifique et/ou technique ainsi qu'un soutien pour l'acquisition, l'exploitation, la maintenance et/ou le maintien en condition des capacités ;
- de participer à différents stades du cycle de vie des capacités de cyberdéfense (définition des besoins, planification, mise à disposition, retrait de service) ;
- de suivre l'évolution des cybermenaces, en consultant des sources d'information internes ainsi que des sources d'information externes accessibles au public, et d'évaluer les risques qui pèsent sur l'OTAN et ses pays membres ;
- de mettre à profit les données recueillies et les enseignements tirés suite à des incidents opérationnels pour renforcer les capacités, politiques, produits et processus existants en matière de cyberdéfense et pour en mettre au point de nouveaux ;
- de fournir une expertise et un soutien en sécurité informatique chaque fois qu'un incident de sécurité informatique le nécessitera ;
- de contribuer à la conduite d'opérations de cybersécurité et de participer à la gestion des incidents ainsi qu'aux activités de coordination et de soutien s'y rapportant ;
- de fournir du renseignement exploitable pour les questions de cybersécurité aux analystes des domaines « connaissance de la situation cyber », « gestion des menaces et des vulnérabilités » et « sécurité physique globale », aux unités opérationnelles déployées dans le monde et aux partenaires industriels ;
- de collaborer avec les analystes du Centre d'opérations de sécurité (SOC) chargés des questions d'ingénierie de sécurité, d'architecture de sécurité et d'analyse de la menace, et de fournir de la documentation pour élaborer, améliorer et tenir à jour des manuels de réponse aux incidents (« runbooks ») et des instructions permanentes pour les besoins du renseignement sur les cybermenaces et de la connaissance de la situation cyber ;

- d’analyser le trafic malveillant et les indicateurs de compromission aux fins de l'identification des auteurs d'actes de cybermalveillance ;
- d’effectuer des recherches et de fournir des rapports sur des campagnes de cybermalveillance, lorsqu’il y a lieu ; d’effectuer des analyses, d'élaborer des documents et de présenter des exposés à caractère général ou technique sur les menaces de sécurité aux unités opérationnelles et aux personnels chargés de la gestion des risques liés à la sécurité des informations ;
- de faire connaître au niveau stratégique les incidences des innovations technologiques sur le plan militaire ;
- d’examiner des comptes rendus de renseignement sur les cybermenaces (hebdomadaires, mensuels et établis à la demande) ; de contribuer à la mesure de l’efficacité du renseignement sur les cybermenaces à l’OTAN ;
- de contribuer à l’intégration du renseignement sur les cybermenaces dans les procédures de contrôle et mécanismes de l’OTAN relatifs à la cyberdéfense ;
- de vous tenir au courant des dernières nouveautés dans les domaines de la cyberdéfense et des TE/TR.

Profil recherché

Dans un monde en pleine évolution, il est indispensable que l’OTAN reste capable de s’adapter et que ses employés sachent se montrer toujours flexibles, désireux d’apprendre et aptes à travailler efficacement avec de multiples parties prenantes aux profils divers. Dans le cadre du programme pour les jeunes talents, nous recherchons des candidat(e)s ayant **au moins un an d’expérience professionnelle**.

Pour la filière **Politique cyber et renseignement sur les cybermenaces**, nous sommes à la recherche de personnes ayant obtenu :

- un master en études cyber, en sécurité internationale, en ingénierie, en technologies de l'information et de la communication ou en informatique ;
- tout autre diplôme qui pourrait être utile dans les domaines **de la politique cyber et du renseignement sur les cybermenaces** ; dites-nous comment nous pourrions tirer parti de vos connaissances et de vos compétences !

Seraient considérés comme autant d’atouts :

- une expérience dans le domaine des cyberopérations ou de l’analyse cyber, ou une expérience acquise dans des fonctions en rapport avec la filière ;
- une connaissance des logiciels de sécurité et une bonne connaissance de la réglementation applicable en matière de cybersécurité ;
- une bonne compréhension des principes sous-tendant la sécurité informatique et la sécurité des communications et une connaissance approfondie des réseaux ainsi que des vulnérabilités des systèmes d'exploitation et applications modernes ;
- une expérience de l’élaboration et de l’application de politiques de sécurité informatique ou de politiques TE/TR ;
- un intérêt pour le hacking et les activités de production de renseignement sur les cybermenaces (capacités et intentions des acteurs malveillants) et sur les cybervulnérabilités ;
- une expérience des technologies de protection contre les logiciels malveillants ainsi que des techniques faisant appel à du code malveillant et des contre-mesures possibles ;
- une passion pour l’informatique et les TE/TR, et la volonté de se tenir informé(e) de l’évolution des technologies ;
- un intérêt pour l’architecture et l’intégration des processus métier, des informations, des applications, des technologies et des systèmes ;
- une connaissance du cycle de vie du renseignement sur les cybermenaces, des niveaux de menace, des produits de renseignement et des sources dont ils sont issus ;
- une expérience de l’utilisation et de la gestion des plateformes d’analyse du renseignement sur les cybermenaces ;
- une connaissance des systèmes de détection des intrusions et des systèmes de gestion des événements et des informations de sécurité (SIEM) ;
- une expérience des technologies et méthodes d’analyse qualitative et quantitative ;

- le fait d'avoir suivi une formation complémentaire ou obtenu une certification en rapport avec la cyberdéfense et les technologies émergentes (p. ex. CEH, CompTIA, SANS, etc.) et/ou d'être titulaire d'une certification dans le domaine de la gestion de projet et de programme ;
- de grandes compétences analytiques et rédactionnelles ;
- une attitude proactive et déterminée et la volonté d'apprendre et de partager l'information ;
- un bon esprit d'équipe, de solides compétences de communication et de facilitation des échanges et de grandes aptitudes relationnelles.

Ce que nous proposons

Participer au programme sera l'occasion pour les jeunes talents :

- d'acquérir une expérience à nulle autre pareille au cœur d'une organisation internationale où ils pourront étendre le champ de leurs compétences et développer leur réseau professionnel ;
- de vivre une expérience riche et stimulante sur les plans professionnel et personnel en étant affectés successivement à trois organismes OTAN, dans différents pays, pour une durée d'un an à chaque fois ;
- de bénéficier d'un salaire compétitif et d'autres avantages, notamment d'une excellente couverture maladie et de 30 jours de congé annuel.

Vous souhaitez travailler pour l'OTAN et participer au programme pour les jeunes talents ? **Vous avez jusqu'au 27 octobre 2024 à 23h59 (heure de Bruxelles) pour poser votre candidature**.

PROCESSUS 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 via l'un des liens suivants :

- Pour les membres du personnel civil de l'OTAN seulement : veuillez postuler via le portail interne de recrutement;
- Pour tous les autres candidats : www.nato.int/recruitment

Veuillez noter : Au moment des entretiens, les candidat(e)s seront invité(e)s à présenter des justificatifs de leur formation et de leur expérience professionnelle pertinentes pour ce poste.
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.

Pour plus d'informations concernant le processus de recrutement et les conditions d'emploi, veuillez vous référer au site suivant. http://www.nato.int/cps/en/natolive/recruit-hq-e.htm.

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.

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.

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.

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.