Young Professionals Programme

PATH 7 – Cyber Defence & Emerging Technologies

Path Narrative

Year 1: Defence Innovation Accelerator for the North Atlantic (DIANA), London, United Kingdom

Work area: Cyber Defence & Emerging Technologies

In Year 1, the incumbent will work in the Safety, Security and Resilience (SSR) Team. The SSR Team within the DIANA Executive (DX) is responsible for managing, coordinating and supervising all aspects related to security across the DIANA regional offices and regional hub, including personnel security, physical security, security of classified information, Communication and Information System (CIS) Security, and industrial security in accordance with NATO's Security Policy. The role will focus on Cyber Security elements across DIANA.

The projects, products, and deliverables to which the Young Professional will contribute include:

- Support the continued security governance of DIANA digital environment;
- Undertaking security risk assessments;
- Develop technical security expertise in O365, Azure, and DIANA own Operating System;
- Build cyber incident response skills in partnership with our commercial Security Operations Centre; and
- Gain an understanding of how a cross-security domain approach reduces organizational risk.

Year 2: International Military Staff (IMS), Brussels, Belgium

Work area: Cyber Defence & Emerging Technologies

In Year 2, the incumbent will work in the Cyber Readiness Section of the Cyber and Digital Transformation Division (CDT). CDT is a joint division, composed of members of the International Military Staff (IMS) and International Staff (IS). CDT staff provide a coordinated approach to NATO's cyber and digital transformation, positioning it to best address security and defence challenges of the 21st century. CDT serves as the NATO Headquarters' focal point for cyber defence strategy and policy, cybersecurity evaluation, digital transformation, and hybrid policy, including NATO's energy security agenda.

The Cyber Readiness Section leads and coordinates the implementation of NATO's cyber strategy, policy, and governance by ensuring operational readiness, resilience, and responsiveness.The effectiveness measurement and reporting function, which the candidate will be a part of, ensures continuous monitoring, assessment, and reporting on NATO's cyber risk exposure, governance effectiveness, and overall defence posture. Metrics are measured for both the 32 Allies of NATO, and the NATO entities which support the Alliance.

The projects, products, deliverables to which the young professional will contribute to include:

- Play an active role in support of the 'Effectiveness measurement and reporting' function of the Cyber Readiness Section;
- Be part of the team responsible for the coordination and oversight of the NATO Cybersecurity Scorecard, a comprehensive annual assessment programme that evaluates and reports on the cybersecurity posture and performance of civil and military entities across the NATO Enterprise;
- Support the primary coordination officer while acting as a working level point of contact for the Cybersecurity Scorecard;
- Participate in annual progress assessments, in collaboration with internal and external stakeholders who will support the evaluation efforts from technical and operational perspectives;
- Benchmark our tools and processes and contribute to the adoption of industry best practice cyber frameworks;
- Gain a unique exposure to the entire Organisation at the highest political and strategic level as the outcomes are annually tracked by multiple Senior Policy Committees as tasked by the North Atlantic Council (NAC);
- Assist on the collection of metrics for related cyber projects.

Year 3: NATO Communications and Information Systems Group (NCISG), Mons, Belgium

Work area: Cyber Defence & Emerging Technologies

In Year 3, the incumbent will work in the Defensive Cyberspace Operations (DCO) section of NCISG J2/6. The Information Assurance and Cyber Defense branch plans, prepares and executes all cyber defense lifecycle management activities within the NATO Deployable Communication Information Systems (DCIS) ecosystem. Cyber Threat Intelligence has an increasing impact on the way that DCOs are planned, prepared, and executed. In the context of the NATO DCIS ecosystem, the cyber threat intelligence function has a twofold purpose: to contribute to DCO planning and execution led by the CYOC and to provide actionable threat intelligence to the Cyber Defense processes of NATO DCIS. The integration of cyber threat intelligence in DCIS enhances the protective capabilities of the Cyber Defense systems and prepositions the response resources

against prioritized potential threats. To this purpose, using edge technologies like machine learning and big data analysis is critical for leveraging cyber threat intelligence from NCISG.

The projects, products, and deliverables to which the young professional will contribute to include:

- Applying innovative technologies to assess open and closed-source intelligence data sources and to identify actionable cyber threat intelligence for the DCIS cyber defense capabilities.
- Dealing with the effective application of threat intelligence within isolated, air-gapped environments.
- Integrating cyber defense mechanisms' actionable data (e.g., signatures, behavior patterns) into the cyber defense mechanisms of DCIS.
- Integrating intelligence platforms (e.g., OpenCTI, MISP) into the DCIS ecosystem.
- Developing DCIS-specific cyber operations indicators.

1re année : Accélérateur d'innovation de défense pour l'Atlantique Nord (DIANA) – Londres (Royaume-Uni)

Domaine d'activité : Cyberdéfense et technologies émergentes

Au cours de la première année, la/le participant(e) travaillera au sein de l'équipe chargée de la sûreté, de la sécurité et de la résilience. Cette équipe, qui est rattachée au Comité exécutif du DIANA, est chargée de la gestion, de la coordination et de la supervision de tout ce qui a trait à la sécurité des bureaux régionaux et de l'antenne régionale du DIANA, notamment la sécurité concernant le personnel, la sécurité physique, la sécurité des informations classifiées, la sécurité des systèmes d'information et de communication (SIC) et la sécurité industrielle, en se conformant à la politique de sécurité de l'OTAN. La/Le participant(e) sera ainsi chargé(e) de tâches liées à la cybersécurité au sein du DIANA.

La/Le participant(e) sera amené(e) :

- à contribuer à la gouvernance de la sécurité dans l'environnement numérique du DIANA ;
- à procéder à des analyses de risques ;
- à développer une expertise technique en matière de sécurité, dans Office 365, Azure et le système d'exploitation du DIANA ;
- à développer le savoir-faire concernant la réponse à apporter aux cyberincidents, en collaboration avec le Centre d'opérations de sécurité ;
- à découvrir comment l'adoption d'une approche interdomaines de la sécurité permet de réduire les risques organisationnels.

2e année : État-major militaire international (EMI) – Bruxelles (Belgique)

Domaine d'activité : Cyberdéfense et technologies émergentes

Au cours de la deuxième année, la/le participant(e) sera affecté(e) à la Section Préparation cyber de la Division Cyber et transformation numérique (Division CDT). Cette division, composée de personnels de l'État-major militaire international (EMI) et du Secrétariat international (SI), est le pôle de référence, au siège de l'OTAN, pour tout ce qui concerne la stratégie de cyberdéfense, la cybersécurité, la transformation numérique et la lutte contre les menaces hybrides, y compris l'action en matière de sécurité

énergétique. Elle assure la cohérence de la transformation cyber et numérique de l'OTAN et aide ainsi l'Organisation à faire face aux défis de sécurité et de défense du XXI^{e} siècle.

La Section Préparation cyber pilote et coordonne la mise en œuvre de la stratégie, de la politique et du cadre de gouvernance établis par l'OTAN dans le domaine cyber, et ce selon trois axes : la disponibilité opérationnelle, la résilience et la réactivité. L'équipe à laquelle la/le participant(e) sera associé(e) est chargée du suivi et de l'évaluation des vulnérabilités cyber, de l'efficacité du cadre de gouvernance et de la posture de défense globale de l'OTAN, ainsi que du travail de *reporting* sur ces questions. Des données sont récoltées pour les 32 Alliés ainsi que pour les entités OTAN concernées.

La/Le participant(e) sera amené(e) :

- à contribuer activement au travail d'évaluation de l'efficacité et de *reporting* de la Section Préparation cyber ;
- à épauler l'équipe chargée de gérer et superviser le Cybersecurity Scorecard de l'OTAN, un vaste programme annuel qui permet d'évaluer la posture en matière de cybersécurité et la performance des entités civiles et militaires de l'entreprise OTAN et d'en rendre compte ;
- à aider l'administrateur principal chargé de la coordination tout en servant de point de contact pour le programme susmentionné ;
- à participer à l'élaboration de bilans annuels, en collaboration avec les parties prenantes internes et externes qui apportent leur contribution sur les plans technique et opérationnel ;
- à comparer nos outils et processus avec ce qui se fait ailleurs et à contribuer à l'adoption de cadres de référence (bonnes pratiques) du secteur privé dans le domaine du cyber ;
- à découvrir les rouages politiques et stratégiques de l'OTAN, au niveau le plus élevé, dans le contexte du suivi annuel effectué par les comités politiques de haut niveau, qui reçoivent leurs instructions du Conseil de l'Atlantique Nord ;
- à participer à la collecte de données dans le cadre de projets cyber.

3^{e} année : Groupe Systèmes d'information et de communication de l'OTAN (NCISG) – Mons (Belgique)

Domaine d'activité : Cyberdéfense et technologies émergentes

Au cours de la troisième année, la/le participant(e) travaillera à la Division J2/6 du NCISG, plus précisément dans la Section Opérations défensives dans le cyberespace (DCO) de la Branche Assurance de l'information et cyberdéfense (IA/CD). Cette branche planifie, prépare et exécute toutes les activités de gestion du cycle de vie dans le domaine de la cyberdéfense au sein de l'écosystème des systèmes d'information et de communication déployables (SIC déployables) de l'OTAN. Le renseignement sur les cybermenaces influe de plus en plus sur la manière dont les DCO sont planifiées, préparées et exécutées.

S’agissant de l’écosystème des SIC déployables de l’OTAN, la fonction de ce renseignement a un double objectif : contribuer à la planification et à l’exécution des DCO conduites par le Centre des cyberopérations et fournir du renseignement qui soit exploitable dans le cadre des processus de cyberdéfense des SIC déployables de l’OTAN. L’intégration du renseignement sur les cybermenaces dans les SIC déployables permet de renforcer les capacités de protection des systèmes de cyberdéfense et de prépositionner les ressources à mobiliser face aux menaces potentielles jugées prioritaires. À cette fin, le recours à des technologies de pointe comme les systèmes d’apprentissage automatique ou d’analyse du big data est fondamental pour une bonne exploitation du renseignement sur les cybermenaces fourni par le NCISG.

La/Le participant(e) sera amené(e) :

- à utiliser des technologies innovantes pour évaluer du renseignement de sources ouvertes ou fermées et recenser les éléments sur les cybermenaces à exploiter dans le cadre des capacités de cyberdéfense des SIC déployables ;
- à veiller à l’exploitation efficace du renseignement sur les cybermenaces dans des environnements sans connexion isolés physiquement ;
- à intégrer les données exploitables des mécanismes de cyberdéfense (p. ex. signatures, modèles de comportement) dans les mécanismes de cyberdéfense des SIC déployables ;
- à intégrer des plateformes d’analyse du renseignement (p. ex. OpenCTI, MISP) dans l’écosystème des SIC déployables ;
- à définir des indicateurs pour les cyberopérations concernant spécifiquement les SIC déployables.