Young Professionals Programme

PATH 6 – Cyber Operations and Threat Intelligence

Path Narrative

Year 1 & Year 2: NATO Communications and Information Systems Group (NCISG), Mons, Belgium

Work area: Cyber Defence & Emerging Technologies

In Year 1 & 2, 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.

Year 3: International Military Staff (IMS), Brussels, Belgium

Work area: Cyber Defence & Emerging Technologies

In Year 3, the incumbent will work in the Cyber Ops Section of the Cyber and Digital Transformation Division (CDTD). CDTC is composed of members of the International Military Staff (IMS) and International Staff (IS) at the heart of NATO's cyber & digital transformation. The Cyber and Digital Transformation Division (CDTD) provides a coordinated approach for NATO to the security and defence challenges of the 21st century. It serves as the NATO Headquarters' focal point for cyber defence strategy, cyber security, digital transformation and hybrid policy, including NATO's energy security agenda.

The Cyber Ops section leads and coordinates two distinct but complementary functions across NATO's Enterprise-wide cyber landscape: the strategic Cybersecurity and Decision-Making function and the operational Enterprise Cyber Operations function. The former ensures risk management and enables risk-informed decision-making. The latter ensures the planning, coordination, and execution of Enterprise Cyber Operations, including the activities of the NATO Integrated Cyber Defence Centre (NICC), which brings together military and civilian assets from NATO Enterprise and Allies for more coordinated and efficient cyber operations.

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

- Assist with propose planning, overseeing, assessing and following up on cyber defence activities in close coordination with the relevant NATO Enterprise stakeholders, including within the context of the NICC;
- Contribute to the development of policies, directives, guidance and administrative documents;
- Engage with a network of relations with key civilian and military experts in the NICC, across SHAPE and NATO HQ;
- Draft background briefs, progress reports, prepare presentations, and other items for high- level meetings. Contribute to effective information sharing with the relevant NATO bodies and stakeholders;
- Depending on the exact team within the section, the incumbent would contribute to Enterprise risk-management deliverables (audit, risk analysis reports, etc.). incident management strategic deliverables, or documents for the planning and coordination of defensive cyberspace operations to include the implementation activities of the NICC.

1re et 2e années : Groupe Systèmes d'information et de communication de l'OTAN (NCISG) – Mons (Belgique)

Domaine d'activité : Cyberdéfense et technologies émergentes

Au cours des première et deuxième années, 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.

3e année : État-major militaire international (EMI) – Bruxelles (Belgique)

Domaine d'activité : Cyberdéfense et technologies émergentes

Au cours de la troisième année, la/le participant(e) travaillera au sein de la Section Opérations 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 XXIe siècle.

La Section Opérations cyber pilote et coordonne deux fonctions distinctes mais complémentaires à l'échelle de l'entreprise OTAN : sur le plan stratégique, elle permet la gestion des risques cyber et la prise de décision fondée sur les risques connus ; sur le plan opérationnel, elle assure la planification, la coordination et l'exécution des opérations cyber, y compris les activités du Centre OTAN intégré pour la cyberdéfense (NICC), qui réunit des civils et des militaires venant de toute l'entreprise OTAN et des pays de l'Alliance pour permettre de renforcer la coordination et l'efficacité de ces opérations.

La/Le participant(e) sera amené(e) :

- à contribuer à la planification, à la supervision, à l'évaluation et au suivi d'activités en matière de cyberdéfense, en étroite collaboration avec les parties prenantes de l'OTAN concernées, notamment dans le cadre du NICC ;
- à contribuer à l'élaboration de politiques, directives, orientations et documents administratifs ;
- à entretenir des contacts avec les principaux experts civils et militaires du NICC, et à faire le lien entre le SHAPE et le siège de l'OTAN ;
- à rédiger des notes d'information et des rapports d'activité, et à préparer des présentations et d'autres documents pour des réunions de haut niveau ; à contribuer au partage efficace de l'information avec les organismes concernés et les autres parties prenantes de l'OTAN ;
- en fonction de l'équipe qu'elle ou il rejoindra, à contribuer à l'élaboration de livrables en matière de gestion des risques (audits, analyse des risques, etc.) et de gestion des incidents au niveau stratégique, ou de documents relatifs à la planification et à la coordination d'opérations défensives dans le cyberespace dans le cadre de la mise en œuvre des activités du NICC.