Février 2018

Cyberdéfense de l'OTAN

Les cybermenaces continuent d'évoluer. Les cyberattaques majeures récemment lancées contre des Alliés démontrent que cyberdéfense et cyberrésilience doivent être des priorités absolues.

Approche OTAN de la cyberdéfense

Au sommet du pays de Galles, en 2014, les Alliés ont déclaré que le droit international s'appliquait au cyberespace et que l'impact d'une cyberattaque sur nos sociétés pouvait être tout aussi néfaste que celui d'une attaque conventionnelle. En conséquence, ils ont estimé que la cyberdéfense faisait partie de cette tâche fondamentale de l'OTAN qu'est la défense collective.

Au sommet de Varsovie, en 2016, ils ont reconnu le cyberespace en tant que domaine d'opérations – au même titre que les airs, la terre et la mer. Cela permet aux commandants militaires de l'OTAN de mieux prendre en compte les cybermenaces dans les missions et les opérations.

Pour autant, cela ne modifie pas le mandat de l'OTAN : comme dans tous les domaines opérationnels, les actions de l'OTAN dans le cyberespace sont défensives, proportionnées et conformes au droit international.

Au sommet de Varsovie, les Alliés ont également adopté l'engagement en faveur de la cyberdéfense, afin de renforcer les moyens de défense cyber des infrastructures et des réseaux nationaux. Chacun des Alliés est responsable de sa propre cyberdéfense, mais l'OTAN apporte son aide sous bien des formes.

Cyberattaques contre l'OTAN

Depuis dix ans, l'OTAN est de plus en plus souvent la cible de cyberattaques. La majorité des attaques visant ses réseaux émanent d'acteurs étatiques.

Chaque jour, des événements suspects sont détectés. La plupart d'entre eux sont traités automatiquement, mais certains nécessitent une analyse et une intervention des experts en cyberdéfense de l'OTAN.

En 2016, l'OTAN a traité en moyenne 500 incidents par mois, soit une augmentation d'environ 60 % par rapport à 2015. Au cours de l'année 2017, les experts en cybersécurité de l'OTAN ont noté une évolution des cyberattaques et un ciblage croissant des systèmes les plus vulnérables, tels que les appareils personnels et les réseaux liés à l'OTAN mais non protégés par elle.

Capacités de cyberdéfense de l'OTAN

En 2017, pour renforcer les moyens de cyberdéfense de l'OTAN, les Alliés ont décidé de créer un **Centre des cyberopérations (CyOC)**, qui est actuellement en cours d'installation.

La **capacité OTAN de réaction aux incidents informatiques** (NCIRC), située au SHAPE à Mons, protège les réseaux appartenant à l'OTAN en assurant, 24 heures sur 24, leur soutien en matière de cyberdéfense. Son équipe de 200 experts gère les incidents et fournit à l'OTAN et aux Alliés une analyse actualisée des défis à relever.

L'aide que l'OTAN apporte aux Alliés dans le cadre du renforcement de leurs propres moyens de cyberdéfense prend les formes suivantes :

- partage d'informations en temps réel sur les menaces (au moyen d'une plateforme d'échange d'informations sur les logiciels malveillants) et partage des meilleures pratiques en matière de traitement des cybermenaces ;
- équipes de réaction rapide « cyberdéfense », pouvant être mises à la disposition des Alliés confrontés à des défis ;
- élaboration d'objectifs à atteindre par les Alliés, afin de faciliter une approche commune de leurs capacités de cyberdéfense ;
- investissement dans la formation, l'entraînement, et les exercices tels que Cyber Coalition, l'un des plus grands exercices de cyberdéfense au monde.

Plusieurs entités aident également l'Alliance et ses pays membres à améliorer leurs moyens de cyberdéfense.

L'**Agence OTAN d'information et de communication (NCIA)**, dont les sites principaux se trouvent en Belgique (Bruxelles et Mons) et aux Pays-Bas (La Haye), apporte son soutien aux opérations de l'OTAN et assure tant la connexion des systèmes d'information et de communication que la défense des réseaux de l'Organisation.

Les experts en cyberdéfense utilisent le **cyberpolygone de l'OTAN** à Tartu (Estonie) pour renforcer leurs compétences, au travers d'exercices réalistes. Le cyberpolygone facilite chaque année l'exercice phare de cyberdéfense de l'OTAN, Cyber Coalition.

Le **Centre d'excellence pour la cyberdéfense en coopération de l'OTAN**, installé à Tallinn (Estonie), est un centre de recherche et d'entraînement accrédité par l'OTAN s'occupant de formation ainsi que de recherche et développement en matière de cyberdéfense. Son expertise est reconnue.

L'**Académie de la NCIA** est en construction à Oeiras (Portugal). Elle apportera une contribution majeure aux capacités de cyberdéfense de l'OTAN en assurant chaque année, à partir de son ouverture en 2019, la formation de milliers de civils et de militaires.

L'**École de l'OTAN** à Oberammergau (Allemagne) propose également des formations et des entraînements liés au domaine cyber à l'appui des opérations, de la stratégie, de la politique, de la doctrine et des procédures de l'Alliance.

Le **Collège de défense de l'OTAN**, à Rome (Italie), favorise la réflexion stratégique sur les questions politico-militaires, y compris les questions de cyberdéfense.

Coopération avec les partenaires

Les partenariats jouent un rôle essentiel s'agissant de faire face efficacement aux défis dans le cyberespace. L'OTAN coopère avec un large éventail de partenaires, y compris des organisations internationales, l'industrie et le monde universitaire.

La cyberdéfense est l'un des domaines de coopération renforcée entre l'OTAN et l'Union européenne, et ce au titre de la lutte contre les menaces hybrides, qui fait l'objet d'une coordination accrue entre les deux organisations. L'OTAN et l'UE échangent leurs meilleures pratiques, et leurs équipes de réponse aux cybercrises partagent l'information.

L'OTAN aide également les pays partenaires à lutter contre les défis cyber. L'un des fonds d'affectation spéciale de l'OTAN pour l'Ukraine est d'ailleurs consacré à la cyberdéfense.

Coopération avec l'industrie

Le secteur privé est un acteur clé du cyberespace, et son expertise est capitale pour la cyberdéfense. L'OTAN resserre ses liens avec l'industrie au travers du cyberpartenariat OTAN-industrie. Cela va dans le sens des efforts déployés par l'OTAN pour protéger ses propres réseaux, améliorer sa résilience et aider les Alliés à développer leurs capacités.

Le partage de l'information, les exercices, l'entraînement et la formation ne sont que quelques exemples de domaines dans lesquels l'OTAN et l'industrie collaborent.

Division Diplomatie Publique (PDD) – Section Presse et médias
Tél.: +32(0)2 707 9867
Email: moc@hq.nato.int
Suivez-nous sur Twitter (@NATOpress)

www.nato.int

0233-18 NATO Graphics & Printing