Décembre 2016

# La cyberdéfense à l'OTAN

Les cybermenaces et les cyberattaques se font de plus en plus fréquentes, sophistiquées et dommageables. L'Alliance est confrontée à un environnement de menaces complexes en pleine évolution. Des acteurs étatiques et non étatiques peuvent utiliser les cyberattaques dans le contexte d'opérations militaires. L'OTAN et les Alliés s'appuient sur des moyens de cyberdéfense forts et résilients pour remplir les tâches fondamentales de l'Alliance que sont la défense collective, la gestion de crise et la sécurité coopérative. L'Alliance doit être préparée à défendre ses réseaux et ses opérations contre la complexité grandissante des cybermenaces et des cyberattaques auxquelles elle est confrontée.

## Politique OTAN de cyberdéfense

Afin de suivre le rythme de l'évolution rapide du panorama des menaces, l'OTAN a adopté une politique renforcée, puis entériné le plan d'action correspondant en septembre 2014, au sommet du pays de Galles. Cette politique pose comme principe que la cyberdéfense fait partie de la tâche fondamentale de l'Alliance qu'est la défense collective ; elle confirme que le droit international s'applique au cyberespace, et elle intensifie la coopération de l'OTAN avec l'industrie. La priorité absolue est de protéger les systèmes d'information et de communication que possède l'Alliance et ceux qu'elle exploite.

La politique prévoit également une gouvernance rationalisée de la cyberdéfense, des procédures pour l'assistance aux pays de l'Alliance en réponse à des cyberattaques, et l'intégration de la cyberdéfense dans la planification au niveau opératif (y compris les plans civils d'urgence). De plus, la politique définit des modalités permettant de poursuivre les activités de sensibilisation, de formation, d'entraînement et d'exercice, et elle appelle à de nouveaux progrès dans diverses initiatives de coopération, y compris celles menées avec les pays partenaires et les organisations internationales. Elle prévoit également un renforcement de la coopération de l'OTAN avec l'industrie, notamment pour ce qui est du partage des informations, de l'échange des meilleures pratiques et de l'exploration de technologies novatrices pour l'amélioration de la cyberdéfense.

À Varsovie, les chefs d'État et de gouvernement des pays de l'OTAN ont aussi reconnu le cyberespace en tant que domaine opérationnel, au même titre que les domaines aérien, terrestre et maritime. Considérer le cyberespace comme un domaine opérationnel permettra à l'Alliance de mieux protéger ses missions et ses opérations, en mettant davantage l'accent sur l'entraînement et la planification militaire. Cela dotera également l'OTAN d'un meilleur cadre pour gérer les ressources, les compétences et les capacités, et pour coordonner les décisions. Cela ne modifiera pas la mission ou le mandat de l'OTAN, qui a un caractère défensif. Comme dans tous les domaines opérationnels, les actions de l'OTAN dans le cyberespace sont défensives, proportionnées et conformes au droit international.

L'Alliance salue par ailleurs les efforts entrepris au sein d'autres instances internationales pour développer des normes de comportement responsable des États, ainsi que des mesures de confiance, en vue de favoriser l'instauration d'un cyberespace plus transparent et plus stable pour la communauté internationale.

## Développer les capacités de cyberdéfense de l'OTAN

La capacité OTAN de réaction aux incidents informatiques (NCIRC) protège les réseaux appartenant à l'OTAN en assurant un soutien centralisé et permanent en matière de cyberdéfense pour les différents sites de l'OTAN. Elle gère et signale les incidents, et elle communique les informations cruciales sur ceux-ci aux responsables de la gestion des systèmes et de la sécurité ainsi qu'aux utilisateurs. La NCIRC possède également des équipes de réaction rapide, qui peuvent être déployées pour aider à protéger les réseaux de l'OTAN ou des Alliés.

L'OTAN aide les Alliés dans leurs efforts visant à protéger leurs propres réseaux et infrastructures critiques en partageant des informations et des meilleures pratiques. Un mémorandum d'entente sur la cyberdéfense entre l'OTAN et les autorités nationales de cyberdéfense de chacun des 28 pays membres de l'Alliance fixe des modalités pour l'échange de tout un éventail d'informations relatives à la cyberdéfense et pour la fourniture d'une assistance afin d'améliorer les capacités de prévention, de résilience et de réponse face aux cyberattaques et aux cyberincidents.

Pour favoriser une approche commune, à l'échelle de l'Alliance, du développement des capacités de cyberdéfense, l'OTAN fixe également des objectifs pour la mise en œuvre, par les pays membres, de capacités nationales de cyberdéfense dans le cadre du processus OTAN de planification de défense (NDPP). En 2017, d'autres objectifs capacitaires en matière de cyberdéfense seront agréés.

L'OTAN conduit régulièrement des exercices – notamment l'exercice annuel Cyber Coalition – et s'efforce d'intégrer des éléments et des considérations de cyberdéfense dans toute la gamme de ses exercices. L'OTAN renforce également ses capacités en matière de formation, d'entraînement et d'exercices, notamment le cyberpolygone OTAN.

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, de consultation, de retour d'expérience, de recherche et de développement en matière de cyberdéfense. Ce Centre ne fait pas partie de la structure de commandement de l'OTAN, mais il possède néanmoins une expertise et une expérience reconnues en matière de cyberdéfense.

L'**École des systèmes d'information et de communication** de l'OTAN, située à Latina (Italie), propose aux personnels des pays membres (et non membres) de l'Alliance des formations à l'exploitation et à la maintenance de certains systèmes d'information et de communication de l'OTAN. L'École déménagera bientôt à Oeiras (Portugal), où elle mettra davantage l'accent sur l'entraînement et la formation en matière de cyberdéfense.

L'École de l'OTAN à Oberammergau (Allemagne) propose également des formations et des entraînements liés à la cyberdéfense 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

Comme les cybermenaces ne connaissent aucune frontière, ni étatique ni organisationnelle, l'OTAN collabore avec les organisations et les pays concernés ainsi qu'avec le secteur privé pour renforcer la sécurité internationale.

L'OTAN travaille, entre autres, avec l'Union européenne (UE), l'Organisation des Nations Unies (ONU), le Conseil de l'Europe et l'Organisation pour la sécurité et la coopération en Europe (OSCE). En février 2016, l'OTAN et l'Union européenne ont conclu un arrangement technique sur la cyberdéfense afin d'aider les deux organisations à mieux prévenir les cyberattaques et à y répondre. Cet arrangement technique fixe un cadre pour l'échange d'informations et le partage de meilleures pratiques entre les équipes d'intervention d'urgence.

## Coopération avec l'industrie

Le secteur privé est un acteur clé du cyberespace. Les innovations et les connaissances technologiques du secteur privé sont indispensables pour que l'OTAN et les Alliés puissent mettre sur pied une cyberdéfense efficace. Au travers du cyberpartenariat OTAN-industrie (NICP), l'OTAN et ses pays membres s'emploient à renforcer leurs relations avec l'industrie et le secteur universitaire. Ce partenariat, qui s'appuie sur les structures existantes, réunit des entités OTAN, des centres nationaux d'alerte et de réaction aux attaques informatiques (CERT) ainsi que des représentants d'industries des pays membres de l'OTAN. Les activités de partage de l'information, les exercices, la formation et l'entraînement 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 5041**
**E-mail : moc@hq.nato.int**
**Suivez-nous sur @NATOpress**

**www.nato.int**

1642-16 NATO Graphics & Printing