Février 2019

La cyberdéfense à l'OTAN

La cybermenace continue d'évoluer. Les cyberattaques majeures récemment lancées contre des Alliés démontrent que le développement de nos moyens de cyberdéfense et l'amélioration de notre cyberrésilience doivent être des priorités absolues.

Approche OTAN de la cyberdéfense

Les Alliés estiment que l'impact d'une cyberattaque sur nos sociétés peut être tout aussi néfaste que celui d'une attaque conventionnelle. C'est pourquoi la cyberdéfense fait partie de cette tâche fondamentale de l'OTAN qu'est la défense collective.

Au sommet de Varsovie, en 2016, l'OTAN a 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'Organisation de mieux prendre en compte les cybermenaces dans les missions et les opérations.

Grâce à des initiatives telles que l'engagement en faveur de la cyberdéfense, pris en 2016, les Alliés renforcent également les moyens de cyberdéfense des infrastructures et des réseaux nationaux, point capital pour l'amélioration de la cyberrésilience.

Si chaque Allié reste responsable de ses propres moyens de cyberdéfense, l'OTAN contribue au renforcement de ces moyens, et cette aide prend notamment 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.

L'OTAN a également mis en place des politiques qui lui permettront de s'appuyer sur les cybercapacités nationales des Alliés au cours de ses opérations et missions, sous contrôle politique et conformément à son mandat défensif. Plusieurs Alliés ont ainsi mis leurs effets cyber souverains à la disposition de ces opérations et missions, tout en restant cependant pleinement propriétaires de ces capacités comme ils restent propriétaires de leurs blindés, navires et aéronefs lorsque ceux-ci sont utilisés dans le cadre 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.

Cyberattaques contre l'OTAN

L'infrastructure informatique de l'OTAN est répartie sur plus de 60 sites, depuis le siège des instances politiques à Bruxelles jusqu'aux sites des opérations de l'OTAN, en passant par les commandements militaires. Plus de 100 000 personnes utilisent les réseaux de l'OTAN, qui depuis une décennie sont de plus en plus souvent la cible de cyberattaques.

Les systèmes de cyberdéfense de l'OTAN détectent chaque jour des événements suspects, de la tentative peu sophistiquée à l'attaque de réseaux de l'OTAN à l'aide de technologies de pointe. La plupart de ces événements sont traités automatiquement, mais certains nécessitent une analyse et une intervention de nos experts. Ces derniers protègent en permanence les réseaux de l'OTAN des intrusions, recueillent, analysent et partagent les informations sur les logiciels malveillants, préviennent la perte de données et mènent des travaux de cybercriminalistique, d'analyse de vulnérabilité et d'évaluation post-incident.

Structures de cyberdéfense de l'OTAN

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. La NCIRC fait partie de l'**Agence OTAN d'information et de**

communication (NCIA), qui 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.

Pour renforcer ses moyens de cyberdéfense, l'OTAN met en place à Mons (Belgique) un nouveau **Centre des cyberopérations (CyOC)**, qui sera opérationnel en 2023. Ce centre permettra à nos commandants militaires d'avoir une meilleure connaissance de la situation, à l'appui de nos opérations et missions. Il coordonnera également l'activité opérationnelle de l'OTAN dans le cyberespace et y garantira notre liberté d'action en rendant nos opérations plus résilientes aux cyberattaques.

En tant qu'organisation, l'OTAN ne prévoit pas de se doter de ses propres capacités de cyber offensives. De leur côté, les Alliés peuvent proposer leurs **effets cyber souverains** à l'appui des opérations et missions de l'OTAN, sachant que dans un tel cas leurs capacités cyber nationales resteront à tout moment sous leur contrôle. Plusieurs Alliés ont ainsi déjà offert leurs effets cyber nationaux à l'OTAN. Grâce à ce mécanisme, les moyens de défense de l'OTAN peuvent évoluer aussi rapidement que la cybermenace.

Des exercices et des formations OTAN se déroulent en Estonie, sur le **cyberpolygone de l'OTAN** qui facilite chaque année l'exercice phare de cyberdéfense de l'Organisation, « Cyber Coalition ».

Le **Centre d'excellence pour la cyberdéfense en coopération de l'OTAN**, installé à Tallinn (Estonie) et accrédité par l'OTAN, s'occupe de formation et d'entraînement ainsi que de recherche et développement en matière de cyberdéfense. Son expertise est appréciée, et il organise des exercices auxquels participent tant les Alliés que des partenaires de l'OTAN.

L'École de l'OTAN à Oberammergau (Allemagne) propose des formations liées au domaine cyber, à l'appui des opérations, de la stratégie, de la politique, de la doctrine et des procédures de l'Alliance. L'**Académie de la NCIA**, en construction à Oeiras (Portugal), organisera la formation du personnel de l'OTAN. Enfin, 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 partagent des informations par l'intermédiaire de leurs équipes de réponse aux cyberincidents, et procèdent à des échanges de meilleures pratiques.

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 par exemple consacré à la cyberdéfense. De même, dans le cadre de son aide au renforcement des capacités de défense, l'OTAN apporte son concours à la Jordanie en matière de cyberdéfense.

L'OTAN resserre ses liens avec l'industrie et le monde universitaire au travers du cyberpartenariat OTAN-industrie. Cela va dans le sens des efforts déployés par l'Alliance 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 5041
Email: moc@hq.nato.int
Suivez-nous sur Twitter (@NATOpress)

www.nato.int

0177-19 NATO Graphics & Printing