Défendre les réseaux

La politique OTAN de cyberdéfense

La politique de cyberdéfense en un coup d'œil

- Prendre en compte les aspects liés à la cyberdéfense dans les structures et les processus de planification de l'OTAN afin de mener à bien les tâches fondamentales que sont la défense collective et la gestion des crises.
- Mettre l'accent sur la prévention, la résilience et la défense des moyens informatiques essentiels aux yeux de l'OTAN et des Alliés.
- Développer des capacités de cyberdéfense robustes et centraliser la protection des réseaux propres à l'OTAN.
- Définir des exigences minimales permettant d'assurer la cyberdéfense des réseaux nationaux essentiels pour l'exécution des tâches fondamentales de l'OTAN.
- Aider les Alliés à atteindre un niveau minimal de cyberdéfense et à réduire les vulnérabilités des infrastructures nationales critiques.
- Établir une coopération avec les Partenaires, les autres organisations internationales, le secteur privé et le monde universitaire.

Contexte

L'environnement de sécurité du XXIe siècle a considérablement évolué. Nos sociétés et nos économies modernes sont interconnectées par des réseaux, des câbles et les adresses IP de nos ordinateurs. L'Alliance, qui dépend de plus en plus de systèmes d'information et de communication (SIC) critiques complexes, doit s'adapter et renforcer ses défenses afin de relever les défis émergents. À cet égard, la nouvelle version de la politique OTAN de cyberdéfense présente clairement la manière dont l'Alliance prévoit d'intensifier ses activités en matière de cyberdéfense.

Le concept stratégique de l'OTAN de 2010 souligne la nécessité de « continuer de développer notre capacité à prévenir et à détecter les cyberattaques, à nous en défendre et à nous en relever… ». La fréquence et la complexité des menaces évoluent rapidement. Les menaces provenant du cyberespace – qu'elles émanent d'États, d'hacktivistes ou encore d'organisations criminelles, pour ne citer que quelques sources possibles – constituent un défi considérable pour l'Alliance, qu'il convient de relever de toute urgence.

Pourquoi une politique OTAN ?

La nouvelle politique OTAN de cyberdéfense constitue une base solide sur laquelle les Alliés peuvent s'appuyer pour faire progresser leurs travaux dans ce domaine. Ce document présente les priorités et les activités de l'OTAN en matière de cyberdéfense – en précisant notamment les réseaux à protéger et la manière de le faire.

Dans ce contexte, au Sommet de Lisbonne en 2010, les chefs d'État et de gouvernement ont chargé le Conseil de l'Atlantique Nord d'élaborer une nouvelle version de la politique OTAN de cyberdéfense. Dans un premier temps, un document conceptuel sur la cyberdéfense de l'OTAN a été soumis aux ministres de la Défense en mars 2011, ce document offrant le fondement conceptuel à la révision de la politique de cyberdéfense. Cette politique a ensuite été élaborée puis approuvée par les ministres de la Défense des pays de l'OTAN le 8 juin 2011. Elle est assortie d'un instrument de mise en œuvre – un plan d'action, qui constitue un document détaillé comportant des tâches et activités spécifiques en rapport avec les structures propres à l'OTAN et les forces de défense des Alliés.

Aperçu de la politique

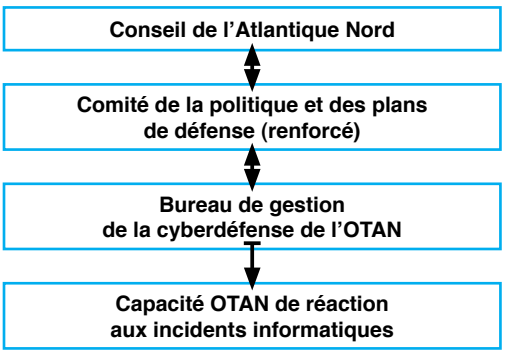
Élément central

Pour mener à bien les tâches fondamentales de l'Alliance que sont la défense collective et la gestion des crises, il faut garantir l'intégrité et la continuité du fonctionnement des systèmes d'information. L'OTAN met donc principalement l'accent sur **la protection de ses propres systèmes d'information et de communication.** Par ailleurs, pour mieux défendre ses systèmes et réseaux d'information, l'Alliance va renforcer ses capacités afin de pouvoir faire face au vaste éventail de cybermenaces auxquelles elle est actuellement confrontée.

Objectifs

L'OTAN va mettre en œuvre une approche coordonnée de la cyberdéfense englobant les aspects liés à la planification et au développement des capacités ainsi que les mécanismes de réaction à activer en cas de cyberattaque. À cette fin, l'OTAN intégrera des mesures de cyberdéfense dans l'ensemble de ses missions. En ce qui concerne le

Gouvernance de la cyberdéfense



développement des capacités de cyberdéfense, **le processus OTAN de planification de défense (NDPP) guidera l'intégration de la cyberdéfense dans les cadres nationaux de défense.** Comme l'Alliance doit pouvoir compter sur une infrastructure sécurisée, les réseaux de l'OTAN, y compris ceux des agences et des missions à l'étranger, seront placés sous un dispositif centralisé de protection. L'OTAN définira par ailleurs **des exigences minimales auxquelles devront répondre les réseaux nationaux qui traitent des informations OTAN ou qui peuvent y accéder.** Pour ce faire, l'Organisation recensera ses points de dépendance critique par rapport aux systèmes et réseaux d'information des Alliés, avec qui elle coopérera pour définir ces exigences minimales. Il est essentiel que l'OTAN dispose d'une infrastructure sécurisée, et il importe donc que les Alliés assurent la protection et la défense des systèmes et réseaux d'information critiques des pays. Si la demande lui en est faite, l'OTAN aidera les Alliés à atteindre un niveau minimal de cyberdéfense.

Principes

Les activités de cyberdéfense de l'OTAN s'inspirent des principes généraux que sont **la prévention et la résilience**, ainsi que la non-duplication. La prévention et la résilience revêtent une importance particulière étant donné que certaines menaces continueront d'exister en dépit de tous les efforts qui seront accomplis pour s'en protéger et s'en défendre. Pour éviter que des attaques ne se produisent, il faudra avant tout améliorer notre état de préparation et réduire les risques en limitant les perturbations et leurs conséquences. La notion de résilience est essentielle car elle permet de se relever plus rapidement après une attaque.

Réaction

Comme indiqué dans le concept stratégique, l'OTAN défendra le territoire et la population de ses pays membres contre toutes les menaces, y compris celles qui concernent les défis de sécurité émergents tels que la cyberdéfense. La politique OTAN de cyberdéfense réaffirme que toute réaction de défense collective est déterminée sur la base d'une décision du Conseil de l'Atlantique Nord. L'OTAN préservera une certaine ambiguïté stratégique et une certaine souplesse quant à la manière de réagir aux différents types de crises comportant un volet cyberdéfense. L'OTAN tiendra par ailleurs compte des aspects liés à la cyberdéfense dans ses procédures de gestion des crises, qui détermineront la réaction à adopter dans le contexte d'une crise ou d'un conflit de grande ampleur.

L'OTAN fournira une assistance coordonnée en cas de cyberattaque contre un ou plusieurs Alliés. Pour ce faire, l'OTAN améliorera les mécanismes de consultation, l'alerte précoce, la connaissance de la situation et le partage de l'information entre les Alliés. Pour faciliter ces activités, l'OTAN a mis en place un cadre permettant la conclusion de mémorandums d'entente sur la cyberdéfense entre les autorités responsables de la cyberdéfense au sein des pays alliés et le Bureau de gestion de la cyberdéfense de l'OTAN.

S'agissant de la réaction aux incidents survenant au sein des infrastructures d'information propres à l'OTAN, la capacité OTAN de réaction aux incidents informatiques (NCIRC) assure la gestion des activités quotidiennes et applique les mesures d'atténuation appropriées.

Quel rôle joue l'OTAN dans le domaine de la cyberdéfense ?

La politique OTAN de cyberdéfense met principalement l'accent sur la protection des réseaux de l'Alliance et sur les exigences en matière de cyberdéfense à appliquer aux réseaux nationaux sur lesquels l'OTAN s'appuie pour mener à bien ses tâches fondamentales que sont la défense collective et la gestion des crises.

Comment l'OTAN réagira-t-elle en cas de cyberattaque dirigée contre elle ou contre les Alliés ?

Toute réaction de défense collective de l'OTAN sera déterminée sur la base d'une décision politique du Conseil de l'Atlantique Nord. L'OTAN ne préjuge pas des réactions possibles et conserve donc une certaine souplesse pour décider d'une éventuelle ligne de conduite à adopter.

En quoi consiste le plan d'action ?

Le plan d'action est un document évolutif, qui sera actualisé en permanence pour faire en sorte que l'OTAN joue un rôle de premier plan dans l'évolution du cyberespace et conserve la souplesse nécessaire pour relever les défis que posent les cybermenaces. Si la politique définit l'objectif de la cyberdéfense de l'OTAN, le plan d'action précise quant à lui la manière de l'atteindre.

Coopération avec la communauté internationale

Les cybermenaces ne connaissent aucune frontière, ni politique ni institutionnelle. Les vulnérabilités et les risques sont les mêmes pour tous. Conscients du caractère véritablement planétaire du cyberespace et des menaces qui s'y rapportent, **l'OTAN et les Alliés coopéreront avec les Partenaires, les autres organisations internationales, le monde universitaire et le secteur privé** pour promouvoir la complémentarité et éviter les doubles emplois. L'OTAN adaptera son engagement international basé sur des valeurs partagées et des approches communes. La coopération dans le domaine de la cyberdéfense pourrait englober des activités en rapport avec la sensibilisation et la mise en commun des meilleures pratiques.

Mesures concrètes

- L'OTAN définira des exigences minimales auxquelles devront répondre les systèmes d'information nationaux essentiels pour l'exécution des tâches fondamentales de l'OTAN.
- L'OTAN aide les Alliés à atteindre un niveau minimal de cyberdéfense afin de réduire les vulnérabilités des infrastructures nationales critiques.
- Les Alliés peuvent en outre venir en aide à l'un des leurs ou à l'Alliance en cas de cyberattaque.
- La cyberdéfense sera entièrement intégrée dans le processus OTAN de planification de défense. Des exigences pertinentes en matière de cyberdéfense seront définies et classées par priorité dans le cadre du NDPP.
- Les autorités militaires de l'OTAN évalueront la manière dont la cyberdéfense contribue à la réalisation des tâches fondamentales de l'Alliance, à la planification des missions militaires et à l'exécution des missions.
- Des exigences en matière de cyberdéfense seront également définies pour les pays non OTAN fournisseurs de troupes.
- Des exigences contraignantes en matière d'authentification seront appliquées. Le processus d'acquisition et les exigences relatives à la gestion des risques pour la chaîne logistique seront rationalisés.
- L'OTAN renforcera ses capacités d'alerte précoce, de connaissance de la situation et d'analyse.
- L'OTAN établira des programmes de sensibilisation et développera plus avant le volet cyberdéfense des exercices OTAN.
- L'OTAN et les Alliés sont encouragés à tirer profit de l'expérience et du soutien du Centre d'excellence pour la cyberdéfense en coopération, situé à Tallinn en Estonie.

1503-11 NATO Graphics & Printing

Division Diplomatie publique de l'OTAN – 1110 Bruxelles, Belgique – www.nato.int – publications@hq.nato.int –