

L'organisation de la cyberdéfense au sein de l'OTAN

BRENNUS 4.0

le capitaine Frédéric Segonne, officier stagiaire à l'EMSST (cycle académique 2018-2019)

publié le 29/03/2020

Sciences & technologies

Si la cyberdéfense est, aujourd'hui, au coeur des préoccupations tant au niveau étatique qu'au sein d'organisations internationales, la prise de conscience de l'importance des menaces cybernétiques est relativement récente. À l'image de la majorité de ses nations, l'OTAN a dû développer une politique de cyberdéfense et se doter des moyens de la mettre en oeuvre. Son objectif initial étant d'assurer la défense de ses systèmes d'informations, la finalité de cette politique est de permettre à l'Alliance de riposter de manière proportionnée ou de mener des attaques préventives dans le cyberspace.

La cyberdéfense a fait son apparition dans les sujets d'attention de l'OTAN à compter du sommet de Prague en 2002, préconisant alors un renforcement des capacités de l'Alliance contre les attaques informatiques. Dans un premier temps, c'est la protection de ses propres systèmes d'information et de communication qui a mobilisé l'Alliance, avec notamment la mise en place de la capacité OTAN d'intervention en cas d'incident informatique – NATO Computer Incident Response Capability (NCIRC), au Grand Quartier général des puissances alliées en Europe (SHAPE) à Mons en Belgique.

Cyberattaque contre l'Estonie :

Cette attaque survient à la suite d'un conflit diplomatique avec la Russie, généré par le projet du gouvernement estonien de déplacer le Soldat de Bronze de Tallinn, monument à la gloire de l'armée soviétique.

Au-delà des émeutes menées par une minorité russophone implantée dans le pays, entre le 26 avril et le 18 mai 2007, l'Estonie fut la cible d'une cyberattaque visant une structure étatique. Prenant la forme d'un déni de service, cette attaque a successivement saturé les serveurs des institutions publiques puis privées estoniennes (ministères, banques,

médias) les rendant ainsi inaccessibles pendant plusieurs heures voire plusieurs jours.

Si aucune preuve n'a permis d'incriminer directement les autorités russes, le gouvernement estonien a rapidement désigné le Kremlin comme responsable de cette attaque, la considérant comme un acte de guerre au même titre qu'une frappe de missiles sur les structures visées. Toutefois, la jurisprudence de l'OTAN ne prenait alors pas en compte ce genre d'attaques.

La cyber-attaque dont a été victime l'Estonie en avril 2007 a conduit l'OTAN à réévaluer son niveau de cybersécurité, mais également à s'interroger sur son rôle, en tant qu'alliance défensive, en cas d'attaque de l'un de ses membres, et donc à élaborer une politique de cyberdéfense pour l'Alliance. En effet, cette attaque, attribuée à la Russie, était la première visant une structure étatique, saturant pendant près de trois semaines les sites gouvernementaux puis bancaires, désorganisant profondément les infrastructures du pays. Des attaques similaires, contre la Géorgie (2008), puis l'Ukraine (2017), ont confirmé l'importance de cette menace dans un contexte de conflit hybride.

Le sommet de Bucarest, début 2008, a permis l'approbation du concept de cyberdéfense de l'OTAN, menant à l'élaboration de sa politique en la matière. Une des conséquences immédiates, et réponse la plus visible de l'Alliance à l'attaque qui avait ciblé l'Estonie, fut la création, à l'initiative de huit pays membres, du centre d'excellence de cyberdéfense coopérative – Coopérative Cyber Defence Center of Excellence (CCD COE), le 14 mai 2008 à Tallinn, en Estonie. Ce centre a pour mission l'amélioration des capacités, la coopération et le partage d'informations entre les pays membres et partenaires de l'OTAN. Il contribue également chaque année à l'organisation et à la conduite de l'exercice Cyber Coalition. La France est devenue membre à part entière du CCD COE en juin 2014. Aujourd'hui, le centre regroupe 18 membres ainsi que 3 partenaires de l'Alliance (voir encadré ci-dessous).

La politique de cyberdéfense, et le plan d'action qui en découle, ont été adoptés en 2011, mais c'est lors du sommet du Pays de Galles, en septembre 2014, qu'est prise la décision la plus lourde de conséquences pour l'Alliance. En effet, au sein d'une version renforcée de cette politique, la cyberdéfense est reconnue comme relevant de la tâche fondamentale de l'OTAN qu'est la défense collective, ce qui ouvre la possibilité d'une invocation de l'article 5 du traité de Washington. Il reviendrait alors au Conseil de l'Atlantique Nord de décider, au cas par cas, si les circonstances d'une telle invocation seraient réunies à la suite d'une cyberattaque.

Cette politique renforcée de cyberdéfense affirme également que, pour l'OTAN, le droit international s'applique dans le cyberspace, mais également que la tâche principale de l'Alliance est la défense de ses réseaux et qu'il revient à chaque pays membre de développer et d'améliorer ses moyens nationaux de cyberdéfense, engagement pris lors du sommet de 2016. Ainsi, à travers ses capacités de formation, d'entraînement mais également en améliorant et renforçant le partage d'informations et l'assistance mutuelle, notamment lors de l'exercice annuel Locked Shields, l'OTAN contribue au renforcement de la résilience générale de l'Alliance. La politique ainsi mise en oeuvre met aussi l'accent

sur la nécessité pour l'Alliance de développer sa coopération en matière de cyberdéfense, tant avec les organisations internationales (ONU, UE, OSCE...) qu'avec le monde industriel. Ce dernier volet coopératif a été formalisé au travers du cyberpartenariat OTAN-industrie – NATO Industry Cyber Partnership (NICP), partenariat par lequel les pays membres s'engagent à resserrer leurs liens avec l'industrie en s'appuyant sur les structures existantes, otaniennes, étatiques et industrielles. Ce partenariat favorise notamment les activités de partage de l'information, les exercices, l'entraînement et la formation, ainsi que les projets multinationaux de défense intelligente.

Lors du sommet de Varsovie, en 2016, une autre étape historique a été franchie avec la reconnaissance du cyberspace comme domaine d'opérations dans lequel l'OTAN doit être en mesure de se défendre aussi efficacement qu'elle le fait dans les milieux aérien, terrestre et maritime. Historique, car pour la première fois de son histoire, l'OTAN ajoutait un domaine opérationnel aux trois domaines traditionnels. La cyberdéfense est donc pleinement intégrée dans la planification opérationnelle et dans la conduite des opérations et missions de l'Alliance. La conséquence la plus notable de cette reconnaissance a été l'annonce, en octobre 2018, de la création du Centre des cyberopérations, ou CyOC. Installé au SHAPE, à Mons, ce centre a pour objectif principal de fournir les informations nécessaires à la connaissance de la situation dans le cyberspace. Il a aussi pour mission de coordonner les efforts des nombreux éléments existants et bien établis, tant au niveau de la structure de commandement de l'OTAN, que dans chacun des pays membres, pour exécuter les opérations et missions de l'Alliance dans le cyberspace. L'OTAN ne possédant pas suffisamment de moyens de cyberdéfense en propre, les Alliés ont convenu que les capacités souveraines seraient mises à la disposition de l'Alliance, à titre volontaire, pour la conduite des cyberopérations, comme cela se fait avec les moyens traditionnels relevant des trois autres domaines.

Concernant la défense de ses propres réseaux, l'OTAN se repose sur la NCIRC. Rattachée à l'agence OTAN d'information et de communication – NATO Communications and Information Agency (NCIA), elle protège les réseaux de l'OTAN en assurant un soutien centralisé et permanent, en matière de cyberdéfense, pour l'ensemble des sites de l'Alliance, par l'intermédiaire de son centre technique. Toutefois, le rôle de la NCIRC ne se limite pas à réagir aux cyberincidents. Son centre de coordination est effectivement responsable de la coordination des activités de cyberdéfense au sein de l'OTAN et avec les pays membres.

Depuis ses premiers pas dans la cyberdéfense en 2002, l'OTAN a su se doter d'une politique de cyberdéfense ambitieuse. Les moyens physiques de sa mise en oeuvre existent et prennent de l'ampleur pour les plus récents d'entre eux. Il reste maintenant à l'Alliance à se doter de l'arsenal juridique et diplomatique qui lui permettra de légitimer son action dans le cyberspace, mais aussi, d'un point de vue militaire, d'une doctrine pour les opérations dans le cyberspace qui sera un document d'orientation précieux pour les commandants de l'OTAN. Sous réserve d'approbation par les Alliés, cette doctrine devrait voir le jour au cours de cette année 2019.

L'aspect juridique s'avère plus complexe à traiter. En effet, le but recherché par l'Alliance est de parvenir à définir ce que serait un état de cyberguerre, ce qui lui permettrait de mener, si nécessaire, des opérations préventives dans le cyberspace.

Toutefois, il est pour cela capital de définir le seuil au-delà duquel un acte malveillant relève du conflit armé et, dans le même temps, la réponse que pourra apporter l'OTAN à des actes qui relèveraient alors de la cybercriminalité. En ce sens, l'Alliance étudie la façon dont elle pourrait réagir de manière systématique aux actes malveillants, sans pour autant déclencher un conflit disproportionné. L'objectif des Alliés est donc de se doter d'un éventail de réponses aussi large que possible, afin de pouvoir élaborer des mesures leur permettant de contrer, toujours dans le respect du droit international et des principes de retenue et de proportionnalité, toute attaque dirigée contre eux et ainsi de dissuader toute autre forme d'acte cyber-malveillant ultérieure.

L'OTAN dispose aujourd'hui des capacités lui permettant d'assurer sa résilience face aux cyberattaques qui la visent. L'Alliance continue à les améliorer et à en développer de nouvelles. Cette construction doit se poursuivre tout en faisant face aux nouvelles menaces du cyberspace. La résolution de l'Alliance est, en effet, aussi forte dans le cyberspace que dans chaque milieu où elle a des intérêts. L'OTAN doit maintenant montrer que sa détermination à dissuader toute agression contre ses membres demeure et ne fait finalement que s'étendre à un quatrième domaine opérationnel.

Exercices cyber de l'OTAN :

Chaque année, l'OTAN organise différents exercices qui intègrent dorénavant systématiquement un aspect cyber. Il existe toutefois certains exercices dédiés à la cyberdéfense, le plus notable d'entre eux étant Cyber Coalition qui fêtera ses 12 ans en 2019. Cet exercice vise à améliorer la coordination et la collaboration entre l'OTAN et les Alliés et à renforcer leurs capacités à protéger le cyberspace de l'Alliance.

Sur une base annuelle également, se tient depuis 2010, au CCD COE, Locked Shields, exercice de cyberdéfense en temps réel au cours duquel la France s'est classée première pour son édition 2019.

Sources

Communiqués officiels des sommets de l'OTAN de Bucarest, Lisbonne, Norfolk, Varsovie, Bruxelles ;

Rapports d'information du Sénat n°449 du 8 juillet 2008 ;

Fiche d'information de l'OTAN de février 2018 et 2019 ;

« What is NATO really doing in Cyberspace ? », Don Lewis, 4 février 2019 ;

https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=fr ;

<https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/FR/index.htm> ;

<https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019/>.

Titre : le capitaine Frédéric Segonne, officier stagiaire à l'EMSST (cycle académique 2018-2019)

Auteur(s) : le capitaine Frédéric Segonne, officier stagiaire à l'EMSST (cycle académique 2018-2019)

Date de parution 18/03/2020

EN SAVOIR PLUS
