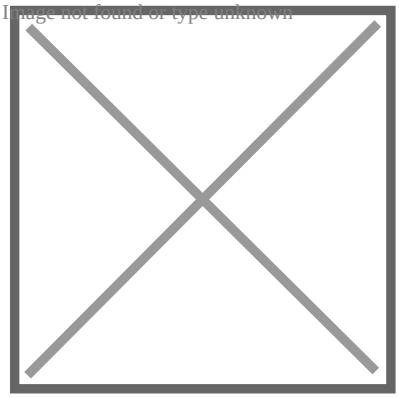
# Les centres d’excellence baltes, avant-garde expérimentale de l’Otan

## Description

**Depuis leur adhésion à l’Otan en 2004, les États baltes reçoivent une aide militaire soutenue de leurs alliés occidentaux. Elle s’est accrue à la suite du déclenchement de la guerre en Ukraine. Toutefois, loin d’être de simples consommateurs de sécurité collective, l’Estonie, la Lettonie et la Lituanie tentent également d’être considérées comme des contributeurs entreprenants.**




Pour se démarquer au sein de l’Otan, les États baltes ont, dès leur intégration, suivi une logique de spécialisation et développé des compétences de niche grâce auxquelles ils peuvent prétendre, malgré leurs faibles moyens, être ponctuellement à la pointe de l’innovation technologique et doctrinale. Ces domaines de spécialisation se rattachent, dans les trois pays, à une conception post-moderne de la guerre. Il s’agit de sphères militaires pour le moment périphériques mais que l’Otan considère comme des formes de conflit amenées à se développer dans les prochaines décennies. C’est pourquoi les États baltes apparaissent à certains égards comme une sorte d’institut d’études avancées de l’Otan. En guise de laboratoires, ils disposent d’infrastructures dédiées à leurs recherches: les centres d’excellence.

Il s’agit d’organismes internationaux homologués par l’Otan qui leur reconnaît une expertise dans un domaine opérationnel précis, mais qui n’appartiennent pas à sa structure de commandement. Créés dans un but de mutualisation des moyens, ces centres sont à l’origine de productions innovantes dont l’Otan peut par la suite librement s’inspirer. On en dénombre aujourd’hui vingt-trois, dont trois se situent dans les États baltes. Pour eux, ce sont de véritables vitrines, des *think-tanks* qui leur permettent d’acquérir une visibilité internationale[1].

### L’Estonie et la cybersécurité

Le premier centre d’excellence à avoir été créé dans les pays baltes est celui de Tallinn. Le Cooperative Cyber Defence Centre of Excellence (CCD COE) est aujourd’hui l’un des centres les plus reconnus de l’Alliance. Son implantation à Tallinn découle d’abord des compétences estoniennes en matière de nouvelles technologies de l’information et de la communication. Ce sont néanmoins les cyberattaques de 2007 qui en ont concrètement accéléré la création. Le centre a été homologué en octobre 2008.

Aujourd’hui, il compte un effectif d’environ cinquante personnes. Il est avant tout chargé de réfléchir à l’aspect doctrinal des cyberconflits. En 2012, après trois ans de recherches, un petit groupe d’experts internationaux réunis au centre ont publié un document intitulé *Manuel de Tallinn* qui répertorie les différents types de cyberattaques et énonce de possibles contre-mesures à adopter pour y faire face.

Le gouvernement russe a reproché à ce texte de se référer presque exclusivement à la conception américaine des cyberconflits. Il est vrai que ce sont majoritairement des spécialistes anglo-saxons, comme Michael N. Schmitt, directeur du centre Stockton à l'United States Naval War College, qui ont présidé à sa rédaction. Une deuxième édition du manuel, *Tallinn 2.0*, sera publiée d'ici la fin de 2016.

Outre cette première étude qui a fait la réputation internationale du centre, celui-ci organise un événement annuel incontournable en matière de cyberdéfense, la CyCon. Chaque année, ce colloque rassemble environ 300 spécialistes internationaux triés sur le volet.

Un autre rendez-vous annuel d'envergure, l'exercice Locked Shield[2], est encadré par le centre. Plusieurs équipes de cybersoldats s'affrontent alors, les uns tentant de protéger leurs systèmes informatiques, tandis que les autres s'efforcent de les infiltrer pour y récupérer des informations ou pour les mettre hors service. L'organisation de cet événement permet, en amont, d'instaurer des standards informatiques communs. Le réalisme de tels exercices peut toutefois être interrogé, sachant qu'ils se déroulent sur un réseau fermé et qu'ils reproduisent des cyberattaques d'assez petite envergure. Par ailleurs, les vraies cyberattaques sont souvent découvertes au moins un an après leur déclenchement.

Le centre s'est trouvé impliqué à plusieurs reprises dans le conflit qui se déroule en Ukraine. En effet, en mars 2014, il a été rapporté que certains de ses employés avaient été détachés en Ukraine pour lui fournir un soutien en matière de cyberdéfense. À cette occasion, des activistes pro-russes ont tenté de mettre hors service les infrastructures numériques du centre. Par la suite, en avril 2015, le centre a été accusé par le média *Russia Today*, sans que celui-ci n'avance cependant aucune preuve tangible, d'apporter un soutien logistique à un site internet ukrainien nationaliste, Mirotvorets, sur lequel sont publiées des informations personnelles concernant des personnalités pro-russes désignées comme des «ennemis de l'État» ukrainien à abattre.

**La Lettonie et la communication stratégique**

Le centre d'excellence de Riga, en Lettonie, n'a pas encore acquis la même envergure que celui de Tallinn, d'autant que son homologation par l'Otan ne date que de septembre 2014. Néanmoins, sa création a été fortement accélérée par la guerre en Ukraine et les autorités lettones encouragent vivement son développement[3].

Dans un monde caractérisé par l'abondance des sources d'information et où, à chaque niveau de commandement de l'Otan, on trouve un bureau ou une équipe de communicants, le centre d'excellence sur la communication stratégique (Strategic Communications Centre of Excellence, StratCom COE) se veut un pôle de recherches et de débats au carrefour de différentes disciplines (la diplomatie publique, les affaires publiques, les affaires militaires, les opérations d'information et les opérations psychologiques). Pour ce faire, il est chargé d'encadrer des exercices et des formations, et de produire des analyses stratégiques. Le premier document majeur à avoir été publié par le centre tente d'analyser ce qui a fait la réussite de la communication russe durant la crise ukrainienne. Actuellement, les travaux du centre portent majoritairement sur les stratégies de guerre hybride.

Globalement, l'objectif du centre est de s'assurer que l'Alliance dispose d'un outil de communication de qualité afin qu'elle puisse, selon qu'elle évolue dans un environnement amical ou hostile, diffuser son influence et faire valoir ses perceptions géopolitiques. La création du centre n'a pas été justifiée par l'excellence de l'expertise lettone mais par les problèmes que le pays pouvait lui-même rencontrer du fait de la présence, sur son territoire, d'une importante communauté russophone. Le gouvernement

letton craint en effet qu'à terme les offensives médiatiques initiées par la Russie puissent contribuer à déstabiliser la région.

**La Lituanie et la sécurité énergétique**

Le centre d'excellence de Vilnius, spécialisé dans la sécurité énergétique (Energy Security Centre of Excellence, ENSEC COE), a été homologué en octobre 2012. La Lituanie n'avait alors pas, elle non plus, de compétences particulières à faire valoir dans ce domaine, mais elle avait en revanche un problème à résoudre: la quasi-totalité de ses besoins en électricité, pétrole et gaz étaient alors assurés par la Russie. C'est donc une volonté d'indépendance énergétique et de mise à distance du fournisseur russe qui est à l'origine de la création du centre.

Le centre propose des études en matière de protection des infrastructures énergétiques. Il s'intéresse également à la logistique militaire en recherchant des solutions pour faciliter le ravitaillement énergétique des troupes, principalement en carburant. Ces propositions permettent non seulement de diminuer les coûts mais aussi de réduire le nombre d'escortes protégeant les moyens de ravitaillement militaires. Conséquence heureuse mais non prioritaire, cela réduirait également l'empreinte carbone des armées. Le centre accompagne en outre la mise en place d'exercices importants. En octobre 2014, en coopération avec les pays nordiques et les pays membres de l'Initiative de coopération d'Istanbul[4], il a organisé un exercice visant à prévenir les dégâts que pourraient occasionner des attaques sur des terminaux d'exportation et d'importation d'énergie, ainsi que sur des bateaux convoyeurs. En mai 2016, un autre exercice a tenté de minimiser l'impact d'une offensive simulée sur un réseau électrique lituanien.

Aujourd'hui, l'Estonie, la France, l'Italie, la Lettonie et la Turquie sont contributeurs à part entière du centre. Le Canada a par ailleurs fourni un million d'euros pour lui permettre de développer un projet de mini-base énergétique militaire composée de panneaux solaires et d'une éolienne. Voilà donc une structure qui semble être en pleine expansion[5], un succès en partie dû à la nouvelle image écoresponsable dont a dernièrement voulu se parer l'Otan et qui a été particulièrement mise en avant par son ancien secrétaire général, Anders Fogh Rasmussen, lors de l'inauguration du centre.

**Notes :**
[1] Hélène Mazeran, Aude de Chavagnac, Général Paul Kuntz, «Défense: les think tanks des États baltes», *Cercle K2*, 11 janvier 2016.
[2] En 2015, seize nations, ainsi que la Nato Computer Incident Response Capability (organe responsable de la coordination cyberdéfensive au sein de l'Otan), y ont participé.
[3] La Lettonie tente d'y attirer des spécialistes étrangers et y investit chaque année trois millions d'euros, budget conséquent pour le pays.
[4] Ce partenariat a été créé en 2004 entre Bahreïn, le Koweït, le Qatar, les Émirats arabes unis et l'Otan pour œuvrer à la stabilité du Moyen-Orient.
[5] «Discussion en France sur le développement du Centre d'excellence OTAN pour la sécurité énergétique», *Ministère lituanien des Affaires étrangères*, 20 avril 2016.

**Vignette :** Logo du centre d'excellence sur la communication stratégique (Stratcom COE).

* Étudiant en Master 2 à l'Institut français de géopolitique (IFG), jeune chercheur s'intéressant à la place géostratégique des États baltes au sein de l'Otan.

**date créée**
15/07/2016

**Champs de Méta**
**Auteur-article :** Louis VAILHEN*