La note du CESA
N°53
03 / 2016

Stagiaire Caroline Pélissier

Estonie : une stratégie de cyberdéfense ambitieuse

En 2007, l'Estonie est victime d'une cyberattaque de grande ampleur. La vigueur de cette dernière est telle que seul un État peut en être à l'origine. Le voisin russe est alors fortement soupçonné. Depuis, de nombreuses mesures ont été prises pour éviter ce genre de crise. Grâce à sa population hyper-connectée et à une coopération renforcée avec les organisations internationales (OI), l'Estonie est devenue un acteur majeur de la cyberdéfense.

Nécessité de renforcer un système déjà victime d'une cyberattaque de grande ampleur

L'action de 2007 a pris la forme de dénis de service[1] visant les sites gouvernementaux, les banques, et également les partis politiques. En conséquence, le pays est resté paralysé pendant plusieurs semaines.

Cette attaque est d'autant plus sérieuse que l'économie de l'État balte repose majoritairement sur le numérique. En effet, après la chute de l'URSS, les Estoniens étaient dans l'obligation de reconstruire leur société. Plutôt que de reprendre le modèle administratif russe, très lourd, ils se sont lancés dans l'administration numérique, ce qui leur a permis peu à peu de rattraper leur retard. Ainsi, en 2007, 98% des transactions bancaires du pays s'effectuaient par Internet, tout comme 82% des déclarations fiscales[2]. De plus, les écoles ont complètement incorporé l'e-environment dans l'éducation des jeunes, habitués à maîtriser les nouvelles technologies. Le fait de s'en prendre aux systèmes d'informations du pays est donc un moyen de déstabilisation efficace.

Les stratégies d'amélioration de la cyberdéfense nationale

Dans un premier temps, la sécurisation du cyberespace se concentre sur le renforcement des infrastructures d'Internet, sur la restriction de manière automatique de l'accès aux serveurs à des utilisateurs jugés malveillants et sur l'augmentation du recours à des moyens d'authentification. L'État prévoit également de perfectionner ses connaissances des différents modes opératoires de cyberattaques, de manière à mieux appréhender la menace.

En outre, par le lancement de sa stratégie de cyberdéfense, l'Estonie souhaitait renforcer ses compétences en développant son offre de formation. Ainsi, dès 2008, sont mis en place des cours de cybersécurité dans les universités, à la suite des efforts conjoints de la *Tallin technical university,* de l'*Estonian national defence college* et du *training and development centre in communication and information systems* des forces de défense estoniennes. L'objectif est de mieux prévoir et de mieux gérer une crise liée à une cyberattaque. Enfin, l'accent est mis sur la nécessité de sensibiliser la population sur les dangers numériques.

Intensifier la coopération internationale

L'Estonie représente une source d'inspiration pour la communauté internationale s'agissant de cyberdéfense. Plusieurs OI ont profité que ce pays était particulièrement avancé en matière de cyberdéfense pour y installer leurs infrastructures. Ainsi, Tallin accueille le *Cooperative cyber defence centre of excellence* de l'OTAN qui est un centre de recherche et de formation. De nombreux pays y envoient des ressortissants dans le but d'améliorer leurs compétences dans ce domaine. C'est le cas notamment de la France qui est officiellement membre du centre depuis 2014. La formation dispensée sur place peut prendre la forme d'une simulation où deux groupes d'informaticiens s'affrontent. L'un joue le rôle de pirates, et doit *hacker* les systèmes d'information de l'autre.

La stratégie de cyberdéfense mise en place à la suite de l'offensive de 2007 peut servir de modèle aux autres États désireux de renforcer leur système de protection contre les cyber menaces. Toutefois, des améliorations sont encore nécessaires afin de mieux se prémunir contre ce genre de crise. L'Estonie souhaite renforcer le cadre légal international de la cyberdéfense. Afin de mieux défendre ses intérêts nationaux et de se protéger de la menace russe, ce rôle de législateur pourrait lui permettre de faire entendre sa voix sur la scène internationale.

Ces propos ne reflètent que l'opinion de l'auteur.

1 Dans ce cas précis, les serveurs ont été saturés afin d'empêcher l'accès à certains sites internet.
2 À titre de comparaison, en 2014 en France, 41% des déclarations fiscales étaient faites en ligne.