La note du CESA
N°57
03 / 2016

Stagiaire Caroline Pélissier

La coopération des acteurs publics/privés dans la politique de cyberdéfense française

En 2013, le Livre blanc sur la défense et la sécurité nationale établit la cybersécurité comme une priorité nationale. Si de nombreux efforts ont été prévus pour améliorer les différentes structures publiques, la coopération civilo-militaire reste une composante majeure de la protection contre les nouvelles formes de cyberattaque. Réfléchir à de nouvelles collaborations qui pourraient lutter contre une menace en constante évolution est un enjeu majeur.

Volonté de l'État de rester souverain de sa politique de cyberdéfense

Dans la définition de ses objectifs de défense, la France a décidé de renforcer ses infrastructures et de développer son industrie de cybersécurité. Pour y parvenir, elle doit s'appuyer sur des accords avec le secteur privé.

Dès 2008, le Livre blanc prévoit la création d'une nouvelle institution publique chargée de la protection des données numériques : *l'Agence nationale de la sécurité des systèmes d'information* (ANSSI). Elle apporte donc son expertise et son assistance technique aussi bien de manière préventive que dans le traitement des cyberattaques. Son activité se concentre sur les cas affectant les réseaux publics et ceux des *opérateurs d'importance vitale* (OIV).

En outre, la préférence nationale en termes de cybersécurité est désormais inscrite dans la loi. Ainsi, l'article 22 de la Loi de programmation militaire (LPM) prévoit que la priorité soit donnée aux prestataires nationaux, labellisés par l'ANSSI pour ce qui est de la mise en place des équipements de détections d'attaques informatiques et de leur exploitation. Les administrations sont également soumises à cette obligation depuis la publication de la circulaire du 17 juillet 2014 (*politique de sécurité des systèmes d'information de l'État*).

Une coopération au cœur du pôle cyberdéfense français

Toujours dans la continuité de la nouvelle stratégie de cybersécurité nationale, le pacte de défense cyber 2014-2019 prévoit la création d'un pôle d'excellence en Bretagne à même de former les futurs cadres dans ce domaine. Les établissements de l'enseignement supérieur de la région détiennent évidemment une place centrale au sein de ce pôle. On y retrouve l'université *Rennes 1, Supélec, Telecom Bretagne, INSA de Rennes, ENSIBS, IUT de Bretagne* ou encore *l'ENSSAT*. La présence du secteur privé est également indispensable à la réussite de ce projet. Ils apportent un soutien technologique et financier nécessaire à la R&D française. On dénombre ainsi 13 entreprises qui se sont associées au pôle : *Airbus D&S, Atos-Bull, Safran, Thalès, DCNS, Défense Conseil International (DCI), EDF, La Poste, Orange, Alcatel Lucent, Bertin, Cap Gemini Sogeti et Sopra-Steria.* Un partenariat a également été conclu avec le monde militaire, qui est représenté par l'École navale, par l'École de l'air, par l'École spéciale Saint-Cyr Coëtquidant et par la direction générale de l'armement via son service de maîtrise de l'information. Ce pôle a donc pour mission de pallier l'insuffisance d'effectifs spécialisés au sein des institutions publiques.

Développer une communauté nationale de cyberdéfense

Pour le moment, la collaboration entre le public et le privé ne profite réellement qu'aux entreprises historiques du secteur de la défense. Afin de remédier à cette problématique, investir dans les PME semble être une solution appropriée. Des incubateurs de *start-up*[1], comme celui récemment ouvert sur le site de l'ancien hôpital Boucicaut pourraient aussi apporter de nouvelles perspectives à l'innovation française en matière de cybersécurité. Une grande variété de secteur sont concernés, tels que la e-médecine, *les smart cities*, l'aéronautique ou encore l'énergie. Néanmoins, les *start-up* n'ont pas les moyens financiers et humains pour suivre un contrat avec l'Etat sur le long terme, de sorte qu'elles sont toujours dépendantes des grands groupes industriels.

Toutefois, ce sont les industriels américains de la cyberdéfense qui bénéficient des fonds les plus importants pour investir dans les *start-up* françaises, au détriment de nos entreprises, incapables de les concurrencer sur le plan financier. La souveraineté nationale en matière de cyberdéfense pourrait être menacée par ce phénomène.

Si la coopération civilo-militaire permet à la France de se consacrer à la R&D et de mettre en place un contingent significatif de ressources humaines spécialisées, elle a encore du chemin à accomplir avant de devenir un acteur important de la cyberdéfense. Les entreprises françaises doivent notamment accroître leurs investissements dans les nouvelles techniques de pointe afin de se positionner réellement comme des concurrents sérieux aux leaders actuels de la cyberdéfense.

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

1. Ici, tout entreprise de moins de cinq ans.