Date: 08.09.2015

L'AGEFI
QUOTIDIEN DE L'AGENCE ÉCONOMIQUE ET FINANCIÈRE À GENÈVE

L'Agefi
1002 Lausanne
021/ 331 41 41
www.agefi.com

Genre de média: Médias imprimés
Type de média: Magazines populaires
Tirage: 9'510
Parution: 5x/semaine

N° de thème: 844.003
N° d'abonnement: 844003
Page: 2
Surface: 30'973 mm²

Pour l'innovation et la sécurité

L'armée suisse n'a-t-elle pas clairement vocation à devenir un futur centre d'excellence de compétences numériques?

FATHI DERDER*

Chaque jour, des entreprises et des citoyens suisses sont victimes de cyber-attaques. La facture se compte en centaines de millions de francs, voire plus. Il est crucial de disposer d'une stratégie nationale de cyber-défense à la hauteur du défi numérique, afin d'assurer la sécurité du pays, tout en dynamisant notre système de recherche, notre économie et notre force d'innovation. La Suisse doit être en mesure d'anticiper les cyber-menaces, de les détecter à temps. Et, en cas d'attaque, de pouvoir assurer la résilience de ses infrastructures et institutions vitales et les défendre. Ainsi l'Etat, et plus précisément l'armée, doit devenir un acteur clé dans ce domaine. Voici quelques pistes de réflexions qui seront formalisées et déposées pendant la prochaine session. Pour l'innovation, et pour notre sécurité. Aujourd'hui, l'armée et le Parlement se rassurent en lisant les rapports de l'administration sur la cyber-sécurité. Où l'on détaille les milliards que nous investirons ces prochaines années pour sécuriser la transmission des données. Mais les rapports ne font que lister les acteurs concernés, de manière statique et ponctuelle, sans développer de réelle stratégie d'action concertée pour notre sécurité. Quant aux milliards dépensés à acquérir des systèmes de sécurité américains ou israéliens, ils ne stimulent pas notre place scientifique: nous nous rendons simplement dépendants de l'étranger dans un domaine extrêmement sensible. La seule vraie solution de sécurité durable, pour la Suisse, consiste à investir dans la recherche, l'innovation, pour développer des solutions propres. Nous en avons les moyens, et les compétences. La Suisse ne peut pas se contenter d'être un client de Tel-Aviv et de la Silicon Valley. A terme, notre souveraineté s'évanouit. Elle disparaît, et avec elle nos compétences.

Pour éviter cet écueil, inspirons-nous, précisément, des modèles américains ou israéliens. Et développons des centres de recherche et des incubateurs au sein de l'armée[1]. Que ce soit sur la base d'une DARPA (Defense Advanced Research Projects Agency) américaine pour les innovations de rupture, ou l'Unité 8200 israélienne pour développer des start-up à la pointe dans domaine de la cyber-sécurité.

Nous proposons ainsi de créer une Darpa suisse[2]. Ou pour être précis, une «mini-Darpa» concentrée sur un seul thème, au cœur de la mission de l'armée: la cyber-sécurité. Avec un budget de 100 millions de francs par année, sans toucher à l'enveloppe totale de l'armée. L'armée consacre 2% de ses ressources à la cyber-sécurité. Sur la base d'une armée à 5 milliards, 100'000 hommes et 9000 employés, nous aurions ainsi une task force conséquente pour la cyber-sécurité. Dotée de 100 millions de francs. Nous pourrions consacrer 30 millions pour le fonctionnement, et 70 millions dans la recherche et développement, avec 2000 militaires (milice active et réserve citoyenne) et près de 200 personnes dans le noyau de base. Ce modèle a de multiples avantages:

Nos problèmes internes et de capacité d'appui subsidiaire seraient réglés.

Comme l'Université Ben Gurion en Israël, ce centre aurait un rôle d'incubateur fédérant les échanges avec des entreprises privées suisses et les hautes écoles (à Ben Gurion, les 5000 postes du centre de compétence génèrent 10.000 postes induits).

On assure une gestion dynamique des talents avec les entreprises, en stimulant recrutement, formation continue, placement...

On dispose d'un puissant observatoire du numérique capable de générer une image globale du domaine, faire des recommandations, des simulations, etc.

Autre piste à creuser: renforcer le rôle de l'armée dans ce domaine numérique, et créer un centre de compétences en la matière. A l'image de ce que nous avons fait pour les menaces ABC (atomique, biologique, chimique), nous devons créer un centre de compétences «D», pour Digital.

En résumé, nous mettons sur pied, au sein de l'armée, une structure pour notre cyber-sécurité couvrant l'ensemble des étapes du transfert de technologies en matière digitale: un centre de compétences, un pôle de recherche appliquée, et un incubateur à start-up. Nous augmentons

Date: 08.09.2015

L'AGEFI
QUOTIDIEN DE L'AGENCE ÉCONOMIQUE ET FINANCIÈRE À GENÈVE

L'Agefi
1002 Lausanne
021/ 331 41 41
www.agefi.com

Genre de média: Médias imprimés
Type de média: Magazines populaires
Tirage: 9'510
Parution: 5x/semaine

N° de thème: 844.003
N° d'abonnement: 844003
Page: 2
Surface: 30'973 mm²

ainsi durablement nos compétences, tout en stimulant nos secteurs militaires, économiques et scientifiques.

Devant l'urgence de la situation, il faut faire vite. C'est possible: le principe fondamental est ancré dans la loi, nous pouvons procéder par une simple modification d'ordonnance. Et tenir des délais serrés: un an pour la mise en œuvre, 5 ans pour être opérationnel, 10 ans pour être une référence. Du moins en théorie. En pratique, ce sera plus compliqué, notamment à cause de la campagne en cours. Nous déposerons un texte pendant cette session. Mais le vrai travail commencera après les élections. Espérons…

———

* *Conseiller national, Le Réseau*

———

[1] *Pour l'instant, seul le Postulat 15.3359 «Pour une armée innovante a été déposé formellement». Sur cette base, une proposition concrète sera déposée dans les jours qui viennent, lors de cette session d'automne..*

[2] *C'est une des 50 actions proposées dans le livre «Le prochain Google sera suisse (à 10 conditions)», paru le 4 septembre chez Slatkine.*