Association des Anciens de l'ENSI de Bourges
88 boulevard Lahitolle
18020 Bourges cedex
http://www.ada-ensib.com - ada@ensi-bourges.fr

CYBERMENACES :

NOUVELLES PERSPECTIVES POUR L'ENSI DE BOURGES, ÉCOLE DE LA MAÎTRISE DES RISQUES ?

1/ Un changement de paradigme

Les cyberattaques du type Stuxnet ou Flame ont établi dans les faits un changement de la cybermenace : un passage de l'ère de l'artisanat de la cybercriminalité (hackers, script kiddies...) vers une industrialisation des attaques (ciblées, se développant dans la durée, bénéficiant d'importants financements étatiques ou criminels et de structures de développement organisées et structurées).

Dans ce domaine, la réponse doit suivre une même évolution. Une solution passive suffisamment robuste pour garantir un niveau de sécurité déterminé n'est plus possible. Les institutions et les entreprises doivent trouver une réponse adaptative, dans la profondeur à une menace dynamique.

2/ Des besoins nouveaux

Le secteur de la cybersécurité connaît un réel déficit en recrutement, acté par le rapport d'information sur la cyberdéfense du sénateur Jean-Marie Bockel[1] : « Il y aurait dans ce domaine quatre à cinq fois plus d'offres d'emplois disponibles que d'ingénieurs spécialement formés ».

Ce rapport apporte ainsi les recommandations suivantes :

- n°6 : « Instaurer une politique des ressources humaines au sein des services de l'État concernant les spécialistes de la sécurité informatique en encourageant le recrutement, la formation, les mobilités et le déroulement des carrières au sein et entre les services de l'État » ;
- n°27 :« encourager la formation d'ingénieurs spécialisés dans la protection des systèmes d'information et prévoir un module consacré à la protection des systèmes d'information dans toutes les formations d'ingénieurs, dans les grandes écoles d'ingénieurs, les universités et l'enseignement technique ».

[1] *http://www.senat.fr/rap/r11-681/r11-6811.pdf*

Ces besoins de lutte contre les cybermenaces ont été à nouveaux rappelés et mis en exergue dans le Livre blanc 2013 de la défense et de la sécurité nationale[2] : « Il importe également d'accroître le volume d'experts formés en France et de veiller à ce que la sécurité informatique soit intégrée à toutes les formations supérieures en informatique. »

Ce constat est également partagé par les industriels qui l'ont précisé lors du colloque « La Cyberdéfense : Quelles perspectives après le Livre blanc ? » organisé le 16 mai 2013 au Sénat[3] :

- JM Nasr (Président Cassidian France, EADS) : « Nous embauchons les mêmes profils […] sollicités par tout le monde, […] les prix sont élevés » ;
- Y Le Floch (VP Sogeti, Cap Gemini) : « Il nous faudrait aujourd'hui deux à trois fois plus de spécialistes en sortie des écoles […], le vivier dans lequel nous puisons est composé à 90% d'étrangers » ;
- J. Notin (PDG Nov'IT) : « Une des grosses difficulté que l'on a au quotidien c'est de trouver des ressources de nationalité française en nombre».

3/ Des industriels impliqués, des partenariats en développements

Pour faire face à cette situation, des initiatives de l'État et des industries ont déjà vu le jour :

- Thalès finance une chaire de cybersécurité à l'École spéciale militaire de St Cyr[4] ;
- La fondation EADS finance la chaire de cyberstratégie de l'Institut des hautes études de défense nationale (IHEDN)[5] ;
- Alcatel Lucent est partenaire de la première promotion en cybersécurité de l'École nationale supérieure d'ingénieurs de Bretagne Sud (ENSIBS)[6], qui a été habilité par la CTI le 13 février 2013.

Ainsi l'ENSIBS estime que « les besoins en recrutement d'ingénieurs [en cyberdéfense] sont estimés actuellement par ces entreprises à plus de 1000 ingénieurs par an (800 pour le privé et 200 pour le public) ».

Cela démontre à la fois la réalité du besoin et la volonté des industriels de s'investir pour le satisfaire.

---

[2] *http://www.gouvernement.fr/gouvernement/livre-blanc-2013-de-la-defense-et-de-la-securite-nationale#*

[3] *http://www.senat.fr/colloques/colloque_cyberdefense_quelles_perspectives_apres_le_livre_blanc.html*

[4] *http://www.st-cyr.terre.defense.gouv.fr/index.php/Les-ecoles-de-Saint-Cyr-Coetquidan/Actualites/Inauguration-de-la-chaire-de-cyberdefense-et-cybersecurite-Saint-Cyr-Sogeti-Thales*

[5] *http://partenaires-ihedn.fr/activite/chaire-castex-de-cyberstrategie*

[6] *http://www-ensibs.univ-ubs.fr/nouvelle-formation-en-cyberdefense-356660.kjsp?RH=ENSIBSPROFIL1_FR&RF=1351525136274*
http://www.letelegramme.fr/ig/generales/regions/morbihan/ubs-cyberdefense-une-formation-d-avenir-14-02-2013-2004630.php

4/ Un champ légitime pour l'ENSI de Bourges

L'ENSI de Bourges, reconnue comme l'École de la maîtrise des risques, forme depuis sa création des professionnels de la sécurité informatique, aujourd'hui en poste dans différentes entreprises du secteur.
La problématique de la cyberdéfense ne s'arrête cependant pas uniquement aux réseaux informatiques : JM Nasr (Président Cassidian France, EADS) : « Pour EADS, la cybersécurité c'est protéger un groupe de 860 entités légales dans 168 pays […] et son infrastructure informatique, les outils de production […] impliquant un bon millier de sous-traitants critiques […] et les produits (7 adresses IP actives dans un avion) ».

La cyberdéfense n'est donc pas le champ unique des spécialistes réseaux, mais une thématique s'interfaçant en profondeur dans le champ des professionnels du risque que forme l'ENSI de Bourges.

5/ Des opportunités à saisir par l'ENSI de Bourges

Les partenariats évoqués plus hauts fragilisent l'ENSI de Bourges en tant qu'École de la maîtrise des risques en légitimant d'autres institutions sur cette thématique et en captant des financements.

Néanmoins, des opportunités de partenariats restent à saisir :

- avec les industriels spécialistes du secteur ;
- dans le domaine de la recherche (rapport sénatorial : « Notre pays manque cruellement de laboratoires travaillant sur [ces] sujets clés » ; G.POUPARD responsable du pôle sécurité des systèmes d'information à la Direction Générale de l'Armement « On a des relations fortes avec plusieurs laboratoires français […], on travaille très concrètement en finançant des thèses, en suivant des doctorants, en finançant des travaux de recherche »...) ;
- avec les opérateurs d'importance vitale menacés (réseaux de télécommunication, d'énergie, de transport, d'eau...) ;
- en soutien du développement de la notion de Maintien en Condition de Sécurité, à l'image du Maintien en Condition Opérationnelle ;
- en soutenant les acteurs du domaine concernant leurs besoins prioritaires: capacité de détection de la menace, normalisation et certification des briques de sécurité, analyse des risques, audits et contrôles.

Ainsi lors du colloque « La cybersécurité : un enjeu mondial, une priorité nationale, des réponses régionales » organisé le 3 juin 2013 à Rennes[7], le ministre de la Défense a esquissé la création d'un pôle d'excellence en matière de cyberdéfense dans le domaine de la formation : « J'ai d'ailleurs, dans cette perspective, missionné l'inspecteur général

[7] *http://www.etrs.terre.defense.gouv.fr/2012-10-11-11-08-08/colloque-cybersecurite*

des armées-armement Jean-Bernard Pène, pour montrer la faisabilité académique et la viabilité économique de ce projet et, du même coup, engager un dialogue avec tous les acteurs intéressés – les écoles, la DGA, les laboratoires, les entreprises… La constitution d'un club de partenaires me semble à cet égard une perspective intéressante. »[8]

L'ENSI de Bourges (ou son successeur l'INSA CVL) a toute la légitimité et la reconnaissance de ses formations pour s'investir dans ce domaine.
Il pourrait ainsi être particulièrement pertinent pour relancer l'attractivité de l'École de créer un mastère spécialisé en cybermenace ou une option au sein de la filière STI et de s'inscrire au sein d'un probable pôle d'excellence en cyberdéfense.

Fabien Ravetto (*Promo 2002*)
Coordinateur du réseau « Aéronautique, Espace & Défense » de l'AdA ENSIB
ada.fabien@gmail.com

[8] *http://lignesdedefense.blogs.ouest-france.fr/archive/2013/06/03/cyberdefense-l-iga-jean-bernard-pene-va-plancher-sur-un-cent.html*