Les partenariats
public-privé en Cybersécurité

Par Cyril Bras

Note du rédacteur en chef : Cet article est un focus sur les travaux de la 2e session nationale « Souveraineté numérique & Cybersécurité de l'IHEDN et l'INHESJ » sur les intérêts et les limites du partenariat public-privé. Les membres du groupe de travail sont dans l'ordre alphabétique : Cyril Bras, Rémi de Gouvion Saint-Cyr, Ludovic Haye, Brunon Le Jossec & Dominique Lestrade. Son intérêt a retenu notre attention. Rapporteur de ces travaux, Cyril Bras a bien voulu en retracer les problématiques essentielles qu'ils soulèvent en répondant à nos questions.

CYRIL BRAS

Responsable RSSI Grenoble-Alpes Métropole. Ville de Grenoble et CCAS

Comment définir le partenariat public/privé en Cybersécurité ?

Le contrat de partenariat public privé (PPP) est un contrat administratif par lequel l'État ou une autorité publique confie à un prestataire privé la gestion et le financement d'équipements, d'ouvrages permettant d'assurer un service public.
Au-delà de cette définition générale, nous pouvons remarquer que des partenariats existent déjà dans le domaine de la Cybersécurité ; le FIC en est quelque part une illustration concrète.
C'est d'ailleurs au cours du FIC 2020 que Guillaume Poupard, directeur général de l'ANSSI, donnait sa perception de l'impérieuse nécessité d'une collaboration « L'idée, c'est que le privé seul n'a pas la solution, le public non plus. On croit donc que la solution se trouve dans l'alliance des deux[1] ».

(1) L. Adm, « FIC 2020 : « Le privé seul n'a pas la solution, le public non plus », 29 Janvier 2020. [En ligne]. Available: https://www.zdnet.fr/actualites/fic-2020-le-prive-seul-n-a-pas-la-solution-le-public-non-plus-39898215.htm . [Accès le 25 Février 2020].

Ce partenariat permet la combinaison des forces et spécificités de ces deux

entités. L'État assure des missions de service public, la justice et la défense entre dans ses prérogatives régaliennes. Le secteur privé pour assurer sa survie face à la concurrence est une source continue d'innovations.

D'une certaine façon notre groupe de travail en est aussi une illustration puisque nous sommes issus des sphères publiques et privées.

Outre le FIC, avez-vous des exemples de partenariats déjà en place ?

Le projet « No More Ransom », initié en juillet 2016, associe les acteurs publics de lutte contre la cybercriminalité et ceux du privé afin de détecter les attaques et d'apporter des solutions aux victimes[2].

Nous pouvons également mentionner le démantèlement du Botnet Retadup, en août 2019, par la Gendarmerie Nationale en lien avec le fabriquant d'Antivirus Avast[3], ce dernier fournissant les éléments techniques pour conduire l'enquête.

Comme évoqué précédemment, certaines activités relèvent de la sphère étatique exclusive comme par exemple le « hack back »[4]. Cependant, il convient d'y associer les acteurs privés de la résilience cyber. Pour ce faire, les visas attribués par l'ANSSI[5] permettent notamment de garantir un niveau de confiance pour les utilisateurs publics de solutions de sécurité développées par des acteurs privés. Le privé apporte alors une partie de la solution au public.

Enfin nous pouvons encore citer une expérience menée à Bruxelles entre des entreprises privées et le ministère de l'emploi afin d'aider à la reconversion et à la réinsertion professionnelle vers le secteur de la Cybersécurité[6].

(2) T. de Coatpont, « La collaboration public-privé, nouvelle arme de la cybersécurité ?» 22 Mars 2019. [En ligne]. Available: https://business.lesechos.fr/directions-numeriques/ [Accès le 25 Février 2020].

(3) UnderNews Actu, « La gendarmerie (C3N) met fin au botnet Retadup – 800 000 machines zombies, » 28 Août 2019. [En ligne]. Available: https://www.undernews.fr/malwares-virus-antivirus/la-gendarmerie-c3n-met-fin-au-botnet-retadup-800-000-machines-zombies.html. [Accès le 23 Mai 2020].

(4) Lorsque l'on parle de hack back, il s'agit d'une défense agressive, allant au-delà de ses propres systèmes. Les Etats-Unis travaillent à une formule qui donnerait à une entreprise un droit d'autodéfense cyber et d'attaquer le système qui serait à l'origine de l'intrusion.

(5) M. Duault, « Qu'est-ce que le Visa de sécurité délivré par l'ANSSI ?» 2018. [En ligne]. Available: https://yousign.com/fr-fr/blog/visa-de-securite-anssi. (Accès le 23 Mai 2020).

(6) RTBF.BE, « Un partenariat public-privé permet à 12 Bruxellois d'être diplômés en cybersécurité, » 20 Février 2020. [En ligne]. Available: https://www.rtbf.be/info/regions/bruxelles/detail_un-partenariat-public-prive-permet-a-12-bruxellois-d-etre-diplomes-en-cybersecurite?id=10430222. [Accès le 25 Février 2020].

© 132377290 Public Partnership concept on the gearwheels, 3D rendering par Alexfmx – Adobe stock

Les sphères opérationnelles du secteur public et privé peuvent générer, par une interaction favorisant le partage d'expertises, de financements et de ressources humaines, des projets collaboratifs efficients en matière de cybersécurité.

Si ces partenariats existent déjà, quel apport donnerait une plus-value à ces interactions ?

Nous avons constaté de fortes disparités tant au niveau du public que du privé sur la prise en considération de la Cybersécurité. Les petites structures (PME-PMI, collectivités territoriales…) ne sont pas forcément aussi bien préparées à faire face à la menace cyber que de grands groupes ou tout simplement elles n'ont pas les moyens de mettre en œuvre les mesures nécessaires pour y faire face. Nous avons donc identifié 3 axes de coopération : la formation de la ressource humaine, sa mise à disposition par le biais de financements agiles et enfin la garantie d'un continuum de compétence (recherche / public / privé).

Actuellement le marché du travail en Cybersécurité est en tension, comment le secteur public peut-il attirer des talents ?

Le secteur public est en effet pénalisé par ses processus de recrutement ou ses conditions salariales. Certes, ce secteur propose des missions intéressantes mais qui ne suffisent pas toujours à compenser les rémunérations proposées dans le secteur privé. Dans le même temps ce dernier recherche des profils disposant de compétences qui ne peuvent être

acquises que dans les missions proposées par les services étatiques. Une de nos propositions consiste à ce que des entreprises privées apportent une contribution financière visant à verser un salaire aux étudiants pendant leur formation, à l'image des écoles militaires. Cet effort financier se poursuit dans un premier emploi au sein de L'État en apportant un complément au salaire pour le rendre attractif. En échange, l'étudiant s'engage à servir l'État pour une durée déterminée (5 ans). À défaut, il devra rembourser les frais de sa scolarité et les indemnités perçues. Ensuite, il pourra se voir proposer un poste dans une des entreprises qui a soutenu financièrement sa formation, avec une durée d'engagement. L'indemnité de rupture se calculera alors au prorata du temps passé en entreprise.

Cette première solution s'applique plutôt aux grandes entreprises. Dans vos réponses précédentes vous évoquiez la nécessité d'aider les petites structures, que proposez-vous dans ce cas ?

Le tissu économique français est en effet constitué de 99.9% de TPE/PME[7] qui sont de plus en plus victimes de cybermalveillances. Dans la plupart des cas, elles ne disposent pas des ressources nécessaires pour se protéger contre cette menace, quand celle-ci n'est pas tout simplement méconnue. Ce constat s'applique également aux petites collectivités.

(7) B. Bellanger, « Baromètre des TPE/PME dans l'économie française en 2019, » 21 Janvier 2020. [En ligne]. Available: https://solutions.lesechos.fr/compta-gestion/c/ [Accès le 05 Aout 2020].

Dans ce cas, nous proposons la mutualisation de moyens au travers d'acteurs locaux tels que les chambres consulaires, les agences locales de développement économique qui se trouvent à l'interface « État /Economie/Politique ». Ainsi, des petites entités pourraient contribuer financièrement au recrutement d'un RSSI qui serait alors mutualisé entre les différentes structures. Ce dispositif pourrait également faciliter la mise en relation avec les services de l' État en charge de la sécurité (prévention cyber, sécurité économique…) pour répondre aux attentes des entreprises mais aussi fournir du renseignement sur l'état de la menace pour la Gendarmerie nationale, la Police nationale et le GIP ACYMA.

Reste-t-il d'autres pistes à explorer ?

Oui, nous pensons également qu'il faudrait repenser la réserve cyber en la rapprochant des territoires et de leurs acteurs. Il conviendrait pour cela de dynamiser la réserve citoyenne et d'en faire un lien fort entre les sphères publique et privée. Elle pourrait partager des bonnes pratiques de Cybersécurité, participer à des actions de prévention ou d'investigation mais aussi apporter des compétences autres que cyber (intelligence économique, escroquerie financière ou encore travail illégal). Elle pourrait prendre exemple sur

l'expérimentation HERMES menée par le groupement du Morbilhan (56) ; ce dernier assiste les entreprises du département en leur proposant des conseils contre les menaces physiques et numériques ou encore en intelligence économique. Pour cela, l'introduction d'un niveau de confidentialité adapté et encadré par des dispositions réglementaires devra être mis en œuvre. Il conviendra également d'accepter un ancrage dans les territoires malgré la distance avec le cadre de l'ANSSI et du Comcyber. La gendarmerie a désigné des correspondants régionaux pour ses réserves numériques et cyber.

Quelques mots pour conclure ?

Sans bouleverser les grands équilibres qui tiennent à la nature profonde des entités publiques et privées, il est possible de trouver dans les zones de contact entre les populations de ces deux sphères des partenariats enrichissants. Qu'il s'agisse d'une ressource qui a vocation à dessiner un parcours professionnel alternant les deux mondes, de personnels du privé qui souhaitent apporter leur contribution à l'intérêt général ou encore de mécanismes économiques qui permettent d'échanger des outils contre une plus forte souplesse en termes de charges, une grande variété de partenariats se dessine.

Une forte volonté politique semble nécessaire pour mettre en route ces mesures, lever les réticences des entreprises et décomplexer les échanges privé-public. La transformation numérique engagée en France doit se faire en lien avec la Cybersécurité qui reste le gage de confiance dans l'usage du numérique. La crise sanitaire actuelle a confirmé cette impérieuse nécessité.

L'AUTEUR

Cyril Bras remplit les fonctions de RSSI de la métropole grenobloise depuis mars 2018. Il est auditeur de la 2e session nationale Souveraineté numérique et Cybersécurité IHEDN & INHESJ. Il est par ailleurs enseignant vacataire auprès de l'université Grenoble Alpes et intervenant auprès du CNFPT.