CYBERCERCLE

Petit déjeuner débat du **13 janvier 2016**

LA DECLINAISON DE LA STRATEGIE NATIONALE POUR LA SECURITE DU NUMERIQUE

avec

Guillaume POUPARD

Directeur général de l'ANSSI

sous la présidence de

Gwendal ROUILLARD

Député du Morbihan

COMPTE RENDU

(Gwendal ROUILLARD) Nous voyons sur les réseaux sociaux des publications qui appellent de plus en plus à notre vigilance. On est à ce titre sur une trajectoire de type « prise de conscience et arbitrage », à l'image du Livre Blanc sur la Défense et la Sécurité Nationale de 2013, qui avait posé l'enjeu de la cybersécurité. Depuis, il y a eu un important cheminement jusqu'à l'élaboration de la Stratégie Nationale pour la Sécurité du Numérique avec ses cinq axes. La France se mobilise afin d'établir un cadrage stratégique de la cybersécurité. Trois points se dégagent et nécessitent une attention particulière : la compétitivité des entreprises françaises, l'action en région et la mobilisation des réseaux d'entreprises dans le territoire pour répondre aux appels à projet de la BPI, et enfin, la formation, initiale et continue.

Le Parlement veille beaucoup sur l'ANSSI et est très attentif à sa montée en puissance, clé de la sécurité numérique française. En parallèle, les entreprises en région ont besoin de l'ANSSI pour soutenir leurs actions, c'est pourquoi l'ANSSI va déployer des représentants régionaux.
La cybersécurité fait partie du quotidien du Parlement français, qui est en permanence en mouvement sur la loi et le cadre juridique, notamment en termes de renforcements budgétaires.

La France a longtemps sous-estimé la question des mentalités et des symboles, pourtant fondamentale. L'Etat peut se doter d'une stratégie, d'entreprises et d'un Parlement impliqués, néanmoins nous avons des jeunes générations qui s'interrogent et parfois, manquent de repères. Certains exemples sont parlant et illustrent bien le rôle que joue Internet dans l'endoctrinement. Ce sentiment d'appartenance à la nation et à la patrie est un chantier de travail principal de notre pays. Une réflexion partagée sur la France – la nation – la patrie, est fondamentale et doit passer par internet et les réseaux, compte tenu de leur prise d'importance dans la société.

(Guillaume POUPARD) L'ambition de la France est de faire partie des quelques nations qui comptent dans tous les domaines stratégiques, et notamment le cyber. La stratégie nationale pour la sécurité du numérique n'est pas une stratégie pour la cyberdéfense mais bien pour la sécurité du numérique, terme plus englobant et traduisant mieux les enjeux et défis qui se posent.
Il n'existe pas de modèle établi dans le domaine de la cybersécurité, chacun a sa propre organisation en tenant compte de ses particularités propres. En France, nous avons opté pour une **séparation stricte des missions offensives et défensives**. Cela ne traduit pas une opposition mais au contraire, une répartition claire des missions, qui peuvent s'avérer complémentaires. De plus, les acteurs doivent s'appuyer sur l'ANSSI, agence interministérielle rattachée au premier ministre, ce qui créé une **neutralité qui dynamise l'action**.

La sécurité numérique est un sujet transverse, qui nécessite l'implication de l'ensemble des acteurs. L'enjeu est de donner des objectifs communs réunissant une diversité d'acteurs ayant chacun un rôle à jouer. Au niveau du secteur public, en plus des ministères traditionnellement impliqués, à savoir Défense et Intérieur, l'ANSSI travaille désormais avec le ministère de l'Economie, de plus en plus concerné par ces problématiques au regard du nombre croissant d'entreprises victimes d'attaques informatiques. Bercy est concerné avec la compréhension commune que le numérique ne peut se développement que s'il est inclus dès le départ dans les projets **: le développement du numérique se fait dans le même temps que la sécurité numérique**. En outre, d'autres administrations ont un rôle majeur à jouer, notamment le ministère des Affaires Etrangères et du Développement International car la diplomatie est fondamentale dans le développement du cyber. Nous pouvons citer également le ministère de la Justice ou de l'Enseignement, par exemple. On imagine mal, dans les années à venir, qu'un ministère n'ait pas de rôle à jouer dans la sécurité du numérique. Afin d'être le plus efficace possible et atteindre des buts communs, l'ANSSI a décidé de développer ce travail de stratégie de manière interministérielle et coordonnée.

La stratégie nationale pour la sécurité du numérique est un travail réellement coopératif, excluant toute lutte d'égos compte tenu du nombre d'acteurs différents impliqués. Une véritable confiance entre individus, et institutions, s'est instaurée, laissant à chacun de la place pour le rôle qu'il a à jouer.

Les cinq axes de la stratégie sont complémentaires :

1) Réaffirmer que les questions de sécurité numérique sont liées à celles de souveraineté nationale.

La sécurité de la nation repose de plus en plus sur les questions de cybersécurité. Une nation qui veut conserver sa souveraineté doit faire de la cybersécurité une priorité nationale et le fait que le premier ministre présente la stratégie le confirme. Il y a une véritable continuité des travaux, dont le point de départ est la LPM votée en 2013, à l'origine de la réflexion sur la protection des OIV contre les menaces cyber. L'ANSSI vise l'applicabilité de la plupart de ces règles au 1er juillet 2016, certaines d'entre elles incluant un délai d'application compte tenu de la complexité de la mise en application immédiate. Le pilier de la souveraineté nationale est essentiel, il passe par de la règlementation et des solutions pratiques, industrielles, disponibles, de confiance et efficaces. Cela fait écho aux travaux de qualification menés par l'ANSSI pour établir une filière de cybersécurité de confiance.

2) Les entreprises non OIV ont également un rôle important à jouer.

Des attaques informatiques massives contre les industries et PME/PMI peuvent devenir des questions de sécurité nationale.
Le fait qu'une PME qui se retrouve en difficulté suite à une attaque cyber n'a pas d'incidence en termes de sécurité nationale néanmoins, quand les attaques se multiplient et deviennent massives, cela peut entrer dans le domaine de la sécurité nationale. Il faut apporter une réponse à cette menace dans les domaines de la prévention et de la sensibilisation mais surtout, il est nécessaire d'agir en aidant les victimes d'actes de cybermalveillance. Actuellement, le statut de victime cyber n'est pas reconnu clairement, ce qui rend plus difficile la recherche de réponses judiciaires efficaces et le passage par des organismes traditionnels de compensation des risques (assurances).

3) La formation à la cybersécurité.

Il existe de nombreuses formations de qualité mais on observe une inadéquation entre l'offre et la demande. Il faut continuer à développer la formation, initiale et surtout, professionnelle qui nécessite un véritable travail. On constate que de nombreuses personnes n'ont jamais fait de sécurité informatique dans leur cursus et on doit remédier à cela, notamment pour les codeurs et les développeurs. Il faut former les étudiants, qui seront amenés à être des experts numériques, aux question de sécurité.
De plus, il faut sensibiliser et véhiculer les bons messages auprès des jeunes, dès la fin du primaire, en leur expliquant les notions basiques de la sécurité. Cette initiation à la sécurité doit être inclue au même moment que la sensibilisation au numérique : une fois encore, sécurité et numérique doivent aller de pair.

4) Inclure les industries dans le développement de la cybersécurité.

La France a besoin d'une industrie forte, nationale et structurée par le processus de qualification. Ce processus est ouvert aux acteurs étrangers mais ce n'est pas une faveur, c'est sur la base d'une évaluation qu'on remet la qualification. Ce travail est compliqué et prend du temps mais il est indispensable afin de savoir qui est compétent et de confiance.

5) Le contexte cyber doit s'envisager à l'international.

La France a un rôle majeur à jouer pour porter ses valeurs dans le domaine cyber, que ce soit pour venir en aide aux Etats les moins avancés, faire du *capacity-building*, aller vers les pays alliés pour les aider à monter en puissance. Nous ne faisons pas uniquement cela par philanthropie mais parce qu'en cyber, comme pour tous les domaines stratégiques, en protégeant nos alliés nous nous protégeons nous-mêmes. Nous avons besoin de porter des messages dans les instances internationales, notamment à l'ONU et l'OCDE. Beaucoup d'entre elles parlent de cyber, avec des projets et cadres qui commencent à émerger malgré la complexité lié au fait qu'au sein même de celles-ci, nous sommes amenés à échanger avec ceux qui nous attaques.
La France doit également passer à l'échelle européenne pour les sujets cyber mais pour aboutir à une souveraineté européenne dans le domaine du numérique, il est impératif de passer par une souveraineté dans le domaine de la sécurité. La France n'attend pas l'Europe pour avancer mais elle est ravie lorsque ses idées peuvent être reprises à l'échelle européenne. La directive NIS sur la sécurité des réseaux, par exemple, en cours d'adoption au niveau européen, ressemble à la démarche française de la Loi de Programmation Militaire. L'Europe est un cadre efficace car elle permet aux Etats de rester souverains tout en collaborant davantage et pousser certains membres à être plus actifs dans la cybersécurité.

En termes de relation bilatérale, notre allié européen le plus proche est l'Allemagne, avec qui nous menons des discussions sur nos dispositifs nationaux respectifs. Bien que différents, ceux-ci sont tout à fait compatibles et il serait pertinent de les mutualiser pour façonner une démarche européenne.

Tous ces éléments mettent en exergue l'impératif de trouver un compromis entre efficacité et confiance. Les différents services de l'Etat impliqués ont tout pour aider les industriels à aller vers l'exports, afin qu'ils deviennent des *leaders* mondiaux dans le domaine cyber.
La France a les moyens d'être optimiste : elle dispose de toutes les cartes nécessaires pour jouer un rôle de premier ordre dans le domaine de la stratégie cyber. Il y a une bonne compréhension globale de la part des acteurs concernés des objectifs à atteindre et des arbitrages budgétaires permettent de déployer davantage de moyens. Cela octroi d'importantes responsabilités à l'ANSSI, qui doit porter la question de la cybersécurité de manière à continuer à protéger la sécurité et la croissance économique du pays face à une menace qui ne va cesser de croître.

Questions

CDT Jean MONTEMONT, DGRIS, ministère de la Défense
Est-il prévu de décliner cette stratégie en un plan d'action public ?

Guillaume POUPARD : La prochaine étape est le développement d'une stratégie par entité, par ministère. Le ministère de la Défense est déjà doté d'une stratégie établie par exemple.
Chacun décline sa stratégie, l'ANSSI décline la sienne, qui sera en partie publique et en partie classifiée. L'objectif global est commun mais il faut que chacun se retrouve vraiment acteur selon ses compétences propres. L'idée est aussi de rassembler des individus et entités qui ne se sentent pas encore concernés mais ayant pourtant un rôle important à jouer.

M. François-Bernard HUYGHE, IRIS
Se pose aujourd'hui la question implicite d'un contre discours contre le djihadisme. Il y a un débat entre les partisans d'un contre discours mené au premier degré, et une autre tendance qui pense à des méthodes

plus indirectes, telles que l'infiltration de sites ou forums djihadistes, sabotages etc. Quelle est votre position sur le contre discours ?

Guillaume POUPARD : Cela ne fait pas partie des missions de l'ANSSI sur le fond, mais l'Agence intervient pour sécuriser informatiquement les démarches de contre discours. L'ANSSI est dans le soutien technique et opérationnel.

Gwendal ROUILLARD : La France a encore beaucoup de travail en contre discours, mais surtout pour construire un discours et en particulier envers les jeunes générations.

M. Daniel CONDROYER, AUSY
Quels types profils sont recrutés au sein de l'ANSSI ?

Guillaume POUPARD : L'ANSSI recrute surtout des jeunes sortis d'écoles et qui viennent après une première expérience. Le numérique est un domaine qui évolue très vite donc les générations les plus jeunes sont les plus adaptées et compétentes. Les recrutements sont également menés conformément aux moyens : il est évidemment moins coûteux de recruter un jeune que des seniors disposant d'une véritable expérience dans le secteur privé.
Il n'y a pas une école qui fournit l'ANSSI en particulier car plusieurs formations sont solides malgré un certain manque de notions de sécurité. Afin de contrer cela, l'ANSSI travaille avec les enseignants pour les former à ces sujets.

L'Agence recrute également de plus en plus de personnes qui ne sont pas de culture ingénieure mais plutôt orientés sciences humaines et Science Po. Ces recrutements sont très positifs car le besoin de coopération national et international est important. En outre, nous avons besoin de développer une pensée, une doctrine, nationale, autour du cyber et porter ses messages à l'international, compatibles aux valeurs de la France.

M. Joël NOIROT, SNCF
La séparation stricte entre cyberdéfense et cyberoffensive est-elle réellement efficace ? Nous avons parfois besoin de riposter à certains groupes : pour cela on se défend alors que si nous disposions de moyens de riposte, la menace pourrait être éliminée.

Guillaume POUPARD : La séparation des missions est nécessaire mais le fait de disposer d'une capacité cyber offensive est nécessaire.
Aujourd'hui, il faut avant tout être capable de se défendre sur le cyberespace et être prudent, tout en développant une capacité offensive.

La séparation entre l'offensive et la défense empêche les conflits d'intérêts car la répartition des missions est claire mais n'est pas signe de manque de coopération. Par ailleurs, dans la LPM un article considère qu'aujourd'hui, en cas d'attaque, les services dont l'ANSSI sont autorisés à mener des opérations techniques visant à caractériser l'attaque, voire la faire cesser. L'important est qu'il ait un équilibre raisonnable entre défense et attaque.

M. Michel BENEDITTINI
Il faut aller plus loin : plutôt que de développer une filière de cybersécurité, il faut développer une filière de produits sécurisés. Que pensez-vous de la dialectique « produits sécurisés et sécurité des produits » ?

Guillaume POUPARD : Dans le domaine des industries de sécurité, le dialogue est plus simple que lorsque nous travaillons avec la FrenchTech notamment. Ce type d'acteurs doit prendre en compte les questions de sécurité dès le départ, et ne pas être orientés uniquement sur l'innovation.
Il faut mettre davantage d'énergie et les aider pour qu'ils considèrent les questions de sécurité comme étant de leur responsabilité. Ils doivent surtout comprendre que la sécurité est un investissement sur le long terme, qui leur sera bénéfique. Actuellement, ces entreprises ne sont pas réticentes, nous sommes confrontés à des acteurs numériques qui demandent de l'aide car ils ont compris que la sécurité numérique était indispensable au développement pérenne du numérique.

La sécurité ne consiste pas qu'en des budgets et contraintes supplémentaires. Elle est nécessaire et les experts de la sécurité doivent être dans un dialogue pour que la sécurité ne soit pas quelque chose d'absolu et accepter que le tout sécurisé n'existe pas.

M. Pierre-Luc REFALO, CapGemini
Quelle analyse fait l'ANSSI de l'attaque de TV5 Monde ?

Guillaume POUPARD : La leçon est très claire : nous sommes tous des cibles.
Dans la relation avec le secteur des médias en tant que cibles, il y a un avant et un après TV5. Ils sont tous dans une démarche vertueuse mais récente de sécurisation de leurs systèmes.
Savoir d'où vient l'attaque importe peu à ce stade, l'effet est le même.

En conclusion, ces attaques sont en quelques sortes positives pour l'ANSSI car elles facilitent les efforts de sensibilisation : nous sommes toujours plus attentifs après une attaque.

Pour nous contacter
Tél : 09 83 04 05 37
contact@cybercercle.com

LES PARTENAIRES DU CYBERCERCLE