Le diner-débat du 10 mars 2023 avec Guillaume Poupard : une nouvelle initiative de la CAIA qui tient toutes ses promesses !

Après notre premier dîner-débat organisé le 10 janvier dernier autour de notre camarade Marwan Lahoud (X83 et IA 88), **nous avons eu le plaisir d'accueillir lors de notre second diner-débat, notre Camarade Guillaume Poupard**, Directeur Général Adjoint de Docaposte, au titre de son expérience de Directeur Général de l'ANSSI[1]. **Trente-sept de nos camarades ont participé à cette soirée, dont la moyenne d'âge était de 50 ans et quatorze d'entre eux avaient 40 ans ou moins : nous avons donc atteint la cible que nous nous étions fixés.**

Les échanges ont été très riches, ouverts, avec une grande liberté de ton pour tous les intervenants, la règle de Chatham-House s'appliquant, la teneur détaillée des échanges reste en confidentialité entre les participants au dîner.

Olivier Martin a rapidement présenté Guillaume et sa carrière, en soulignant notamment l'obtention d'un DEUG de psychologie à l'université Paris-VIII, puis d'une thèse sous la direction de Jacques Stern[2] à l'École normale supérieure de la rue d'Ulm dans le domaine de la cryptographie.

Dans un premier temps sont rappelées la perception de la cybersécurité en France à l'arrivée de Guillaume à la tête de l'ANSSI et ses principales évolutions jusqu'à ce jour.

Il est rappelé qu'avant 2000, le mot cyber n'existait pas. La cybersécurité commence en 2007, avec l'attaque russe contre l'Estonie. Pour exister, L'Estonie a misé sur le numérique, ce pays étant ainsi en 2007 le pays le plus numérique au monde. Devant le déplacement d'un monument à la gloire du soldat russe, La Russie lance une très grosse attaque cyber de représailles, massive, simple, de type saturation (DDOS, Distributed Denial of Service). L'Estonie est totalement désorganisée pendant plusieurs semaines.

Sous l'autorité de Patrick Pailloux, premier directeur de l'ANSSI entre 2008 et 2014, auquel Guillaume rend hommage pour son action de premier directeur de l'ANSSI, on prend alors conscience des risques cyber mais peu d'exemples concrets touchent directement notre pays. En fait, à cette époque, le panorama informatique est très segmenté, ce qui est favorable pour la sécurité de ces systèmes. En ce qui concerne la DGA, les Directeurs de Programme sont plutôt rétifs à la prise en compte de cette nouvelle contrainte, car la prendre en compte impose des surcoûts et une réduction des performances des systèmes d'armes.

---

1 *Agence Nationale de la Sécurité des Systèmes d'Information*

2 *Jacques Stern est le chercheur français vivant ayant le nombre le plus important de publications aux congrès CRYPTO/EUROCRYPT, les plus prestigieux en cryptologie.*

Puis sont rappelées les premières attaques cyber en France : Bercy en 2010, Elysée en 2012, l'affaire Snowden en 2013 qui révèle les pratiques américaines d'espionnage, attaques de cyber espionnage en général peu médiatisées car la discrétion reste alors de mise pour préserver son image. Les attaques cyber apparaissent alors comme pouvant non seulement servir des objectifs d'espionnage et de compromission, mais également conduire à des destructions de systèmes industriels, de fait plus aisées que les opérations d'espionnage (le cas StuxNet est notamment évoqué).

Mais l'ensemble des acteurs reste néanmoins à convaincre, tâche difficile devant la faible perception de cette menace. Cette prise de conscience est néanmoins accélérée par l'attaque contre TV5 Monde en 2015 et définitivement acquise après les trois grosses attaques en 2017 : Wannacry , NotPetya, la campagne électorale présidentielle en France en 2017.

La LPM de 2017 prend en compte cette nouvelle menace, conduisant à l'élargissement des missions de l'ANSSI et à la mise en place des Opérateurs d'importance vitale.

Enfin, se généralisent à partir de 2019, les attaques ransomware lancées par les réseaux mafieux. Certes moins structurés et moins compétents que les Etats, ils visent cependant des cibles beaucoup plus diverses et plus « faciles », comme les hôpitaux, même en pleine crise Covid[3]

Durant sa période à la tête de l'ANSSI, le travail en équipe a constitué une vraie satisfaction pour Guillaume, non seulement au sein de l'ANSSI, mais également entre l'ANSSI, la DGA et ses grands partenaires du « C4 » : DGSE, DGSI, ComCyber, administrations fières de leur autonomie. Parmi les frustrations, Guillaume a cité l'administration « administrante » avec notamment des personnels qui sur-appliquent des règles qu'ils ne comprennent pas.

Quant à la contribution de ta formation et de sa partie de carrière au sein de la DGA pour permettre à un ingénieur de l'armement d'assumer efficacement un poste de responsabilité comme la direction de l'ANSSI, il est d'abord rappelé que piloter un organisme comme l'ANSSI exige certes des compétences managériales mais surtout des compétences techniques et de maitrise des projets absolument indispensables. Ainsi, Guillaume souligne l'intérêt d'avoir connu divers mondes avant de prendre la Direction de l'ANSSI : la poursuite d'une thèse universitaire et l'expérience acquise au sein d'autres administrations avec les responsabilités au sein de la DGA. **En résumé, Guillaume confirme l'importance de favoriser la mobilité des ingénieurs de l'armement, la circulation des hommes étant une richesse.**

De nombreuses questions furent alors posées par les participants à ce diner-débat dont la synthèse des échanges est donnée ci-après.

[3] *Si en métropole, un malade pouvait encore être transféré sur un autre hôpital non attaqué, la situation aurait été dramatique pour les malades de l'hôpital de Papeete, sans possibilité de transfert vers un autre hôpital.*

S'interrogeant sur la faible efficacité cyber apparente des Russes en Ukraine, il est dans un premier temps rappelé que le système de défense de l'Ukraine fut très largement neutralisé par les attaques cyber des Russes durant la période 2015-2017, ce qui a conduit à considérer ce pays comme très faible en matière cyber. Pour redresser la situation, les autorités ukrainiennes ont accepté de remettre en ce domaine leur souveraineté entre les mains des Etats-Unis et notamment des GAFAM, afin de pouvoir faire face aux éventuelles attaques cyber russes. Avant le début du dernier conflit en Ukraine, ce dernier a su faire face alors que les attaques cyber russes ont été très sophistiquées et très puissantes. En réalité, l'Ukraine s'entraine en ce domaine avec l'aide des Américains depuis plus de 10 ans, s'appuyant notamment sur une segmentation maximale de leurs systèmes d'information : il n'y a donc pas eu d'effet de domino face aux attaques russes qui les ont visés.

Les notions de cloud européen et cloud souverain apparaissent confuses. Pour le cloud européen, la France souhaite avancer, mais nous n'en avons pas les moyens. En effet, les Pays-Bas y sont idéologiquement opposés, souveraineté équivalent à protectionnisme à leurs yeux, l'Irlande est évidemment hostile à toute mesure anti-GAFAM, l'Allemagne souhaite préserver l'accès de son industrie automobile aux marchés chinois et américains et les autres pays européens privilégient la préservation de leurs liens avec les Etats-Unis.

Par ailleurs, le cloud souverain français est un des sujets les plus complexes. Sa réelle faisabilité reste douteuse. La vision de Cédric O[4] et Bruno Lemaire apparaissait comme une solution de type « Cloud de confiance », par l'importation de solutions américaines opérées par des Français. Mais elle n'est pas souveraine car, si les GAFAM retirent leur soutien, tout s'arrête à la première mise à jour.

En réalité, nous ne disposons plus en France et en Europe de capacités souveraines en matière d'infrastructures. Il est également rappelé l'impasse que semble prendre l'Etat en essayant d'assurer la maitrise d'œuvre de ce cloud souverain sans la coopération avec les grands industriels, indispensables pour assurer la fabrication des produits de série.

Il est clairement rappelé que La maîtrise de la cryptographie et de la cryptanalyse est essentielle pour notre souveraineté. La cryptographie en couche basse dans le Cloud peut être très utile pour le stockage. Mais quand on monte dans les couches, au niveau Office 365 par exemple, il n'y a plus réellement de crypto. La solution serait un cryptage très profond, et chiffrer dans les puces, mais cela impliquerait de faire confiance aux fondeurs qui aujourd'hui sont tous américains. Enfin, la cryptographie homomorphe n'apparait pas aujourd'hui comme très efficace.

Si la distinction en France des organisations cyber offensive et cyberdéfense étonne, compte tenu des expériences différentes aux Etats-Unis et au Royaume-Uni, il est précisé qu'en cas de

[4] *Ancien Secrétaire d'État chargé de la Transition numérique et des Communications électroniques*

regroupement au sein d'une même entité, le cyber offensif, plus attirant, prend le dessus, et la cyberdéfense s'avère alors de plus en plus négligée. Le modèle français de séparation est ainsi jugé plus efficace que le modèle britannique de regroupement mais, alors que la NSA doit se réorganiser tous les 5 ans pour remettre l'accent sur la cyber défense, le Royaume-Uni peut compenser cette inefficacité en disposant dans ce domaine de six fois plus de personnels que la France.

Pour conclure, la coopération avec les pays européens en matière de cybersécurité est abordée. En synthèse, la coopération la plus ouverte apparait être avec le Royaume-Uni qui s'améliore, après une période difficile liée au Brexit. En effet, très contraint par son alliance « Five Eyes », le Royaume-Uni souhaite préserver une certaine autonomie, notamment en se rapprochant de la France. Avec le reste de l'Europe, cela semble plus compliqué. La cybersécurité relève du domaine défense, la coopération se fait essentiellement en interétatique et peut alors s'exercer sur trois niveaux :

- Le développement de compétences et de capacités locales, mais assez difficile pour les pays 100% atlantistes
- La mise en place de réseaux de partage stratégiques d'information, l'UE soutenant ces échanges grâce à l'ENISA[5]
- La coordination des défenses des Etats Membres en cas d'attaque cyber, via la mise en place de mécanismes de coordination qui restent à construire. Cet objectif reste difficile d'autant plus que la guerre en d'Ukraine a conduit les Etats-Majors à développer ses propres capacités nationales et à privilégier l'OTAN comme cadre de coopération.

ICA Jacques Doumic
Capgemini
Membre du Conseil de la CAIA

[5] *Agence de l'Union Européenne pour la cybersécurité*