« La Cyber Défense européenne, enjeu de souveraineté »

Article tiré d'une vidéo conférence
tenue le 25 novembre 2020 sur l'outil sécurisé « Bib Blue Button »

Répondre à la question de la souveraineté de la Cyber Défense européenne, c'est aborder 4 thématiques :

1) Comment sur le plan européen protéger nos valeurs démocratiques et se prémunir contre les « PsyOps », ces opérations psychologiques de manipulation de la démocratie ? La manipulation des élections américaines de 2016 autour du scandale « Cambridge Analytica », la dé-fiabilité du vote électronique, la montée en puissance des « deep fakes », la haine sur internet protégée par l'anonymat des réseaux sont autant de questions qui doivent trouver réponse. Le limogeage récent de Chistopher Krebs, le directeur de l'agence de cybersécurité américaine, qui en accord avec la déontologie, n'a pas accepté de relayer les allégations de fraudes électorales dénoncées sans preuve par le président Trump montre que la tentation de la dictature n'est jamais très loin.

2) Comment protéger les infrastructures vitales de notre pays et de nos entreprises stratégiques contre les attaques cyber ? Ce sont des réalités dont voici quelques exemples :

- le 16 novembre 2019 : le CHU de Rouen, paralysé par un rançongiciel a été contraint de revenir à « la bonne vieille méthode du papier et du crayon »,
- le 27 juillet 2020 : la société Carlson WagonLit victime d'un rançongiciel a été bloquée deux jours et a dû payer 4,5 M$ de rançon pour récupérer ses données,
- Le 20 octobre 2020, Sopra Steria, entreprise de 46000 personnes et 4,4 Md€ de chiffre d'affaire a arrêté très rapidement une attaque par le rançongiciel Ryuk qui a affecté le système d'authentification et a entraîné le chiffrement d'une partie de ses données,
- Le 12 avril 2012, l'Élysée a mis en évidence une opération d'espionnage attribuée de façon formelle à nos alliés états-uniens,
- Le 23 décembre 2015, un piratage des systèmes industriels SCADA, basé sur le programme «BlackEnergy" et le logiciel malveillant, KillDisk a provoqué une importante coupure d'électricité le 23 décembre dans la région d'Ivano-Frankivsk, dans l'ouest de l'Ukraine.

La menace à la fois est endogène et exogène au réseau dont le coût mondial est chiffré à 4Md$ en 2020 avec une croissance de 50 % annuelle.

3) Comment protéger les citoyens européens contre la collecte de données personnelles et sensibles par des puissances étrangères ? Comment protéger les sociétés européennes contre le cyberespionnage ? Il y a eu dans ce domaine des avancées juridiques incontestables sur le plan européen :

- comme l'adoption par le parlement du règlement 2016/679, le règlement général sur la protection des données applicable partout en Europe depuis le 25 mai 2018,
- comme l'invalidation par la Cour de Justice Européenne, de l'accord transatlantique mal-nommé « Privacy Shield » qui autorisait le transfert de données sensibles de citoyens européens,
- comme le Cyber Act européen qui acte la création de l'ENISA, agence de cybersécurité européenne,

- et comme le futur Digital Services Act en préparation qui doit donner un cadre législatif à l'espace informationnel pour les 20 ans à venir.

Mais malgré cela, la volonté politique actuelle de la France en matière de souveraineté numérique n'est toujours pas au rendez-vous comme on le voit avec le projet de « Data Health Hub », un guichet unique d'accès à l'ensemble des données de santé confié à Microsoft pour développer l'intelligence artificielle appliquée à la santé. Alors que ces données sont celles de tous les citoyens français et concernent l'ensemble des systèmes informatisés des acteurs français de la santé, ce projet de recherche qualifié d' « intérêt public », concept juridiquement flou, ouvre aux GAFAM la porte de nos données de santé et au pouvoir financier qu'elles représentent.

4) Enfin le sujet militaire de la guerre permanente dans le cyberespace qui est le cinquième milieu après la terre, la mer, l'air et l'espace. Le cyber ouvre la voie à un nouveau théâtre de guerre qui donne un avantage décisif à l'attaquant.

Le sujet sera traité en trois parties, d'abord en évaluant la menace, puis en proposant des réponses, au niveau français, enfin au niveau européen.

LA MENACE

.

En 2017, l'ANSSI, historiquement plutôt tournée vers le haut du spectre, a observé des campagnes d'attaques aux effets stratégiques, systémiques, au travers de la diffusion de codes destructeurs, donc pour du sabotage. Elle a également constaté des attaques ciblées sur les sous-traitants, sur le maillon le plus faible d'une chaîne logistique, pour toucher l'objectif final majeur, le grand compte, qui est lui mieux protégé. Enfin, elle a observé des attaques cyber cherchant à déstabiliser certains processus démocratiques.

En 2018, ce furent davantage des attaques informatiques furtives, cherchant à anonymiser les modes opératoires *via* des outils publics.

En 2019, les tendances observées lors des deux dernières années se sont accrues, avec notamment la montée en gamme des « rançongiciels », des attaques moins massives, plus ciblées sur de gros acteurs, capables de payer la rançon (par exemple celle médiatisée sur le groupe M6).

En 2020, elle a fait face à la généralisation des rançongiciels, mais aussi au retour des attaques stratégiques, ciblant des acteurs importants, avec exfiltration de données avant chiffrement, dont le but n'est pas uniquement lucratif, mais parfois aussi économique et politique.

La manipulation de l'information, dans le cadre d'élections par exemple, devient une tendance structurante mais n'est pas suivie par l'agence, qui traite de la technique cyber.

Il faut une Vision globale. Le CEMA Russe a très bien exprimé en 2013[1] que l'utilisation de moyens non militaires pour atteindre des buts stratégiques et politiques allait s'accroître et dépasser l'efficacité des armes. C'est ce qui se passe dans le champ du numérique et du cyber où la situation se dégrade.

Une menace importante est celle des « cyber-corsaires », de jeunes « hackers geeks » plus efficaces que s'ils agissaient en tant que fonctionnaires. On peut citer par exemple un escroc russe, un protégé de Poutine. Ces corsaires sont protégés et renvoient l'ascenseur en tant que de besoin. L'Iran pratique aussi cela. Ce « ***Rançongiciel plus*** » cache de l'espionnage. Pourquoi attaquer un hôpital si ce n'est pour faire pression sur un pays ? C'est de la cyber-coercition. Et ce sont aux États de réagir. Le cyber est aussi un outil de désinformation ou d'influence, comme par exemple lors du piratage de la boîte mail de Mme Clinton. Beaucoup d'entreprises, à l'exception de celles qui font partie des Opérateurs d'Importance Vitale (OIV), ont un niveau de sécurité très faible, en particulier une mauvaise intégration des filiales qui viennent de tous les horizons. Le

[1] La doctrine « Gerasimov », théorisée en 2013 par le général Valeri Gerasimov, chef d'état-major des armées russes, préconise l'utilisation de moyens non-militaires pour atteindre des objectifs stratégiques.

niveau de sécurité est bien celui du maillon le plus faible. Il n'y a pas d'écosystème Etat / industrie, comme cela a été le cas pour PALANTIR aux USA. La priorité de la DGSE est de lutter contre le terrorisme, pas de transférer ses outils à la DGSI ou à l'industrie. La Bonne surprise est qu'il y a une réaction qui démarre.

Au plan industriel, si l'on prend l'exemple d'EDF (168 000 salariés, 60 milliards de CA, 900 filiales, un million d'objets connectés hors Linky), c'est un périmètre très vaste à gérer. EDF a des contrats réglementaires qui permettent de bien protéger les systèmes d'information. L'entreprise est aussi sous la directive de protection du patrimoine scientifique et technique. S'oppose à elle des lois extraterritoriales, celles des USA, mais aussi celles en Asie. La menace touche certes les postes de travail et les serveurs mais aussi les machines industrielles. EDF porte naturellement une très forte attention à tout ce qui touche à la sécurité du nucléaire, source majeure d'électricité en France. Mais elle a à faire face aussi aux attaques des activistes antinucléaires. EDF fait face à des États décomplexés. L'Iran et la Russie sont très actifs. En 2019 et 2020, le nombre de failles de sécurité a doublé. Ceux qui demandent des rançons volent les données avant de les crypter et on peut se demander ce qu'ils font des informations recueillies (exemple des plans de prison dans le cas du piratage de Bouygues).
EDF compte 1200 incidents par an, de 130 jusqu'à 600 menaces détectées par mois. 50 vulnérabilités demandent une réponse urgente et une centaine de gros incidents ont lieu par an, comme l'attaque déjouée contre SOPRA, sachant que l'agresseur avait réussi à pénétrer dans le système d'information et qu'il a fallu 15 jours, 24h sur 24, pour régler le problème. EDF essaie d'être leader cyber dans le domaine de l'énergie, et est dans le Conseil d'ECSO (European Cyber and Security Organisation). Il y a des initiatives au niveau de la régulation qui ont un impact au niveau européen.

LES REPONSES EN FRANCE

Le cyber comprend des leviers de puissance. Une agence ne peut répondre seule, il faut un travail interministériel dans le cadre de politiques publiques. L'État doit s'assurer que les Opérateurs d'Importance Vitale (OIV) ont les moyens et les compétences pour faire face aux attaques.
Le premier levier est réglementaire, pour protéger les activités et infrastructures critiques, par exemple sur les référentiels à appliquer, ou les schémas de certification à suivre.
Le deuxième levier est culturel, même s'il y a du mieux, les décideurs ne sont pas encore assez conscients des effets des attaques. La sécurité cyber est vue comme une contrainte et non comme une protection. Souvent hélas, les entreprises comprennent trop tard, après une attaque.
Le troisième axe est la défense, qui passe par une meilleure connaissance de la menace, par des systèmes de détection, des systèmes de réponse aux incidents de sécurité et également une pratique de la gestion de crise. Au bout du compte, en matière cyber, il faut à la fois traiter des « zéros et des uns » et s'assurer que les pratiques de chacun ne mettent pas en danger tout le système.

En termes d'outils et d'organisation, « la seule défense n'est pas la meilleure défense ».
Pour les outils, Il faut créer des écosystèmes comme l'a fait le CEA LETI (laboratoire sur les nanotechnologies) de Grenoble autour de plus de 60 startups, avec par exemple une réussite comme SOITEC. Oui, la France sait créer des startups innovantes.
Mais il n'y a pas d'outil européen de cyber, et les grands clients ne le souhaitent pas. Dans ce qu'on appelle le Bastionnage, c'est-à-dire la protection des comptes à privilège, il y a WALLIX mais les grands clients veulent plus souvent CyberArc . La question est de comprendre pourquoi WALLIX ne réussit pas à s'imposer dans les grands groupes européens.?
Les services étatiques, ANSSI et DGSE, Comcyber, ont un bon niveau cyber et développent d'excellents outils, qui ne sont malheureusement pas transférés à l'industrie. Une très grande entreprise de défense sollicitée dans ce but, pour assurer son leadership, a répondu qu'il n'y avait pas de marché, et qu'elle ne voulait donc pas investir dans cette mission de transfert. Les USA ont une vision industrielle remarquable. La France ne l'a pas compris en 2008 -2009. Le problème est

de transformer un concept en produit utilisable par l'industrie donc vendable. C'est un métier complexe.
Les Israéliens sont très forts pour créer des LICORNES[2]. Ce n'est pas le cœur de métier de Orange ou Thales où la cybersécurité est marginale. Il faut des « pure players », des entreprises dont c'est le métier. Nos ingénieurs sont pourtant très bons. Au niveau étatique on discute d'égal à égal avec les USA. A ce niveau les outils français sont reconnus. **Il faut un campus de recherche très innovant**. Nous avons beaucoup de startups qui ne sont que tricolores. Ça ne peut pas marcher. Les exemples d'ALSID et de TEHTRIS, de niveau mondial, sont remarquables ; les fondateurs sont issus de l'ANSSI ou de la DGSE.
Notre souveraineté passe par l'innovation.
Il ne faut pas refaire PALANTIR (c'est du passé), mais PALANTIR++, avec de l'intelligence artificielle. Il faut exporter ces outils aux USA pour que nos entreprises grandissent. Le marché américain est fondamental.
Sur le plan de l'organisation, **il faut créer une force nationale cyber** comme les Britanniques, avec un GCHQ[3], et un MI6, etc. Le cyber est un domaine où il ne faut plus de séparation entre civils et militaires, entre les armées. Nous n'avons pas besoin d'une cyber armée uniquement pour des conflits armés. Nous ne sommes pas attaqués par une armée mais par des volontés politiques. Il faut rassembler tous les acteurs. Les Américains l'ont compris en réformant la NSA. En France il faudrait relier la partie défense de l'ANSSI (COSI), le COMCYBER, une partie de la DT de DGSE, la partie renseignement humain de la DRM, fondamentale, la Gendarmerie. Cette dernière a récemment simulé une cyberattaque, offensive, ce qui est louable, mais qui n'était pas coordonnée avec d'autres administrations.
Notre organisation date de 2009, il faut la repenser. Ne faire que défendre n'est pas suffisant. C'est une ligne Maginot qui peut se contourner. L'Europe Occidentale doit prendre des mesures extrêmes, c'est-à-dire contre-attaquer, pour ne pas offrir un « ventre mou ». Nos adversaires ne vont pas s'en prendre aux USA ou aux Britanniques car ils savent qu'il y aura une réaction immédiate qui va les détruire.

L'Influence des lobbies est considérable. Les Campus cyber de la Défense, celui de Rennes et celui en projet de Bordeaux sont une réponse stratégique pertinente. Plutôt qu'à Paris, il faudrait concentrer nos moyens à Rennes, autour de gros acteurs étatiques comme le Comcyber, la DT de la DGSE, une grande université, multidisciplinaire, une zone industrielle, des salles de conférence. Ce serait un écosystème complet, comme en Israël. Mais la moitié des acteurs majeurs de la cyber sont en région parisienne et demandent qu'il soit construit à la Défense ; ce qui n'est pas incompatible avec des implantations en province.

QUE FAIRE AU NIVEAU EUROPEEN?

En termes de souveraineté. Commissaire européen, Thierry Breton a parlé de la prochaine décennie comme d'une décennie numérique ou cyber. On rentre dans le domaine de la souveraineté, qui est concrètement un objet encore mal identifié de façon précise. Quels pourraient être les grands constituants de la souveraineté :

- l'autonomie d'appréciation et d'action dans le cyberespace,
- le respect des valeurs libérales européennes et la protection de nos biens immatériels (protection des données dans l'UE par exemple),
- les infrastructures que nous jugeons critiques, comme la 5G ou le Cloud par exemple.

On peut identifier 4 ou 5 gros enjeux autour de cette souveraineté :

---

[2] Startup valorisée à plus d'un milliard de dollars

[3] https://fr.wikipedia.org/wiki/Government_Communications_Headquarters : Le Government Communications Headquarters (GCHQ, littéralement « quartier-général des communications du gouvernement ») est le service gouvernemental du Royaume-Uni responsable du renseignement d'origine électromagnétique et de la sécurité des systèmes d'information.

- arbitrer entre sécurité et souveraineté, au niveau européen, le plus sécurisé n'étant pas obligatoirement le plus souverain,
- disposer d'un tissu technologique très dynamique par exemple *via* le projet de Campus Cyber à la Défense prêt à l'automne 2021, un hub national capable d'attirer des européens,
- protéger en propre nos infrastructures (réseaux, câbles téléphoniques, satellites, équipements 5G)
- définir une posture vis-à-vis des GAFAM.

Au plan industriel, EDF, par exemple, a une approche pragmatique de la souveraineté. **Certains processus, informations et données ne doivent pas être accessibles à des étrangers, même au travers de lois extraterritoriales.**

En termes de Stratégie autour du Cloud Public et de la 5G ? Avec l'arrivée du Cloud public et des outils de mobilité, depuis maintenant 10 ans, on peut de moins en moins travailler dans un environnement périmétrique contrôlé. Sauf à tout enfermer dans des réseaux industriels fermés et étanches, les échanges devront se faire dans la défiance généralisée, surtout avec l'arrivée prochaine de la 5G, dont l'objectif est de tout connecter. Avec la 5G, on a une virtualisation complète, quasiment que du logiciel. On aurait pu développer, au-dessus des couches de la 5G, une surcouche de confiance de cryptologie au niveau européen. Il n'est pas possible de tout contrôler mais il faut le faire sur quelques éléments. On aurait pu faire un appel d'offre européen car on a la compétence. Il y a eu trois initiatives sur le cloud en France : une lancée par le CFS, comité de filière stratégique, une à partir des travaux du CIGREF, sur les fameux cercles de confiance, le deuxième proche du ministère des armées, enfin celle de GAIA-X franco-allemand, auquel participe EDF.
A propos du cloud, L'UE a un bon niveau de certification et de qualification. Deux systèmes sont matures : un en France et un en Allemagne. Il faut une qualification dynamique. Le système logiciel n'est jamais figé et la qualification ne doit pas se faire sur une « photographie » à un instant donné. Il faut faire face à la problématique de fournisseurs qui n'existent plus en Europe ou sont rachetés par les US. Nous avons besoin d'un contrôle sur les équipements au niveau européen.

En termes de priorités pour l'UE. La directive européenne NIS sur les activités d'importance essentielle est bien mais la question est de savoir si les réponses sont à la hauteur de l'enjeu. Il faut une politique industrielle pour créer des champions. On progresse, grâce hélas au COVID, mais il reste un long chemin à faire. L'investissement sur GAIA-X c'est 600 millions d'Euros, l'Europe prévoit aussi 1,7 milliards d'euros sur la cyber entre 2021 et 2026. De leur côté, les USA consacrent 20 milliards de dollars par an sur le Cloud Public, alors que nous consacrons nos ressources ailleurs, par exemple cette année 10 milliards sur l'automobile qui n'est pas une technologie souveraine. Nous ne ferons pas un cloud européen de même niveau que les USA ou la Chine ; donc le défi est de faire différemment, d'utiliser autrement ces clouds existants, en les détournant à notre avantage.

l'Europe est une chance car c'est le plus grand marché. il faut :

- une réglementation et une reconnaissance de la sécurité des produits, pour créer le marché,
- des startups sur ces marchés, pour qu'elles puissent grandir,
- une volonté des politiques et des industriels.

Pourquoi y-a-t-il tant d'acteurs extérieurs sur le cloud européen : Alibaba, Google, IBM ?
La diversité des 27 États ne facilite effectivement pas la tâche, il faut une coopération entre quelques États (France, Allemagne, Pays Bas, Suède), en faisant des compromis, et former un noyau dur européen. En France cela dépend des secteurs, nous sommes bons en technique et en compétence mais pas en organisation ni en commercialisation. Il y forte complémentarité avec les Allemands. **Pourquoi pas ne pas créer une cyberforce franco-allemande**, en fusionnant BSI et ANSSI ?

Il convient d'évoquer la Joint European Disruptive Initiative (JEDI), sorte de DARPA, organisation privée, sous forme d'association, autour d'une quarantaine de personnes bénévoles, avec seulement deux salariés. C'est une agence de programmes sur des thèmes identifiés, avec des ressources propres faibles. Il y a 50 projets cyber innovants en France, qu'il faudrait fusionner dans une masse critique, avec une organisation souple et réactive comme JEDI. Il faut créer un seul guichet de financement au lieu de 10. Un bon modèle a été EUREKA piloté par industriels, très mal vu par Bercy et la Commission européenne, qui n'étaient pas décisionnaires.
Nous serions capables de reproduire TEAM 8 israélien, qui a levé 800 millions de dollars. Sur un projet, ses dirigeants font venir une cinquantaine d'experts pour une durée limitée. Le gouvernement israélien finance 50% des projets dans une approche top down. Il faut une synergie entre universitaires et experts opérationnels. TEAM 8 dispose de beaucoup de fonds et vient de réaliser 3 belles réussites.
Il y a aussi un exemple californien qui fédère chercheurs, fonds et experts : le « Y Combinator ». Il faut inciter les Experts étatiques à lancer startups en payant pendant 3 ans leurs salaires. Il faut des idées et des avantages financiers, fiscaux et autres. Les hommes ont les a.

Terminal européen souverain ? C'est une utopie. L'Open source n'est pas plus sécurisée. OPEN SSL a eu une faille pendant 10 ans. Sécuriser un logiciel est d'une extrême complexité. Il faudrait 7 000 ingénieurs sur un Operating System. Idem pour les composants.

A propos des Startups. Quel est leur intérêt si elles sont rachetées par les Américains dès qu'elles démarrent ? La difficulté est la deuxième levée de fonds à 100 millions qui est encore très difficile en Europe. Il faut une politique européenne d'achats. Il devrait exister une forme de lien entre acheteurs et producteurs. C'est contraire à la libre concurrence mais ce serait bien si on pouvait. disposer d'une facilité à acheter ce dans quoi on a investi, mais pas au coup par coup.

En conclusion la prise de conscience de la menace au niveau stratégique est encore lente, parfois trop tardive. Les réponses au niveau européens sont pertinentes. Elles doivent être basées sur l'innovation, sur la création d'écosystèmes réunissant toutes les parties prenantes, autour de campus cyber et de forces cyber, comme le font Américains et Britanniques. Cela ne peut pas se faire à 27 mais autour de quelques pays, en particulier la France et l'Allemagne

Avec la participation de :
Olivier LIGNEUL, Directeur cybersécurité du Groupe EDF
Bernard BARBIER, CEO de BBCyber
Marc-Antoine BRILLANT, Sous-directeur adjoint Stratégie de l'ANSSI
Thierry LEBLOND, Ingénieur Général de l'Armement (2s),
Président de Scille[4], Membre du Conseil d'EuroDéfense-France

[4] Scille est une société spécialisée dans la transformation numérique de grands comptes et dans le partage de données sensibles sur le cloud, éditeur du logiciel parsec.cloud (https://parsec.cloud)