CONFÉRENCE

LES ENJEUX GÉOPOLITIQUES DU CYBER POUR L'UNION EUROPÉENNE

INVITÉ : M. Emmanuel MENEUT, chercheur spécialiste des questions de cybersécurité

COMPTE RENDU DE LA CONFÉRENCE DU **22 SEPTEMBRE 2021**

ÉVÉNEMENT LABELLISÉ **LA FABRIQUE DÉFENSE**

Propos recueillis le mercredi 22 septembre lors de la conférence : « Les enjeux géopolitique du cyber pour l'Union européenne ». L'invité, Emmanuel MENEUT est ingénieur de l'École centrale de Marseille, diplômé de l'Université américaine de Paris et docteur de l'Institut Catholique de Paris, spécialiste de l'impact des ruptures technologiques sur les régimes internationaux en Asie.

En quoi est-ce que l'espace cyber représente aujourd'hui une rupture technologique, et quels sont les enjeux politiques pour les Etats qui l'investissent ?

La cybersécurité est une dimension importante aujourd'hui des relations internationales et de la géopolitique, et si on se place du point de vue du décideur, c'est un nouvel environnement décisionnel. Il est confronté à différents environnements : il y a l'environnement de la dissuasion nucléaire ou l'émergence des environnements criminels. Le cyberespace et son enjeu de cybersécurité sont structurés autour de la course aux cyberarmes. Avec cette course, les stratégies qui se trouvent être le plus souvent renforcées sont celles de la diplomatie coercitive. La diplomatie coercitive est l'usage de la menace pour convaincre un adversaire de changer de comportement. Cette stratégie peut être déployée par un outil diplomatico-militaire, mais quand elle échoue, elle conduit à une guerre et qui avait une probabilité limitée de succès puisqu'il est compliqué de rendre crédible le fait d'utiliser la force sans le faire. On pense à des exemples peu convaincants, comme la première guerre du Golfe où la menace des Américains et de la coalition d'intervenir n'a pas été suffisante pour convaincre Saddam Hussein de se retirer et, il a fallu que la coalition intervienne réellement.

Avec des cyberarmes, on peut crédibiliser la diplomatie coercitive sans escalader jusqu'au conflit. La diplomatie coercitive devient une stratégie qui rencontre l'adhésion et est de plus en plus souvent utilisée par des cyber puissances. Le cas de l'Estonie est d'ailleurs considéré comme la première cyberguerre.

Cela s'est véritablement développé depuis 2009 avec l'attaque israélienne des installations nucléaires syriennes : l'opération Orchade. Les forces aériennes israéliennes ont fait un aller-retour dans l'espace aérien syrien sans qu'ils ne s'en rendent compte. Tout l'espace aérien avait été contrôlé par les Israéliens.

Il y a également eu la fameuse attaque des centrifugeuses iraniennes, l'affaire Stuxnet. Cela a permis de retarder le développement du programme nucléaire iranien de deux ans, ce qui a évité à Israël d'intervenir en Iran. Voilà un peu l'enjeu politique pour les Etats aujourd'hui.

L’émergence du cyberespace fait que les cyberarmes sont de plus en plus utiles et ont de plus en plus de cibles dans le cadre de la diplomatie coercitive.

Selon vous, l'espace cyber est une rupture technologique qui tend à polariser les Etats plutôt qu'à les rendre interdépendants, et dont l'utilisation se fait selon une logique offensive, contrairement par exemple à la stratégie de dissuasion, défensive, de l'arme nucléaire. Pourriez-vous nous parler de ces éléments et nous préciser quel est leur impact sur la coopération entre les Etats ?

Initialement, si les ruptures technologiques, c’est-à-dire la diffusion et la production de nouveaux services, sont la clef qui permet de voir notre niveau de vie évoluer, dans le champ de la géopolitique et de la sécurité elles sont souvent perçues comme des défis à la sécurité. En effet, une rupture technologique est une nouveauté, et la particularité de cette nouveauté c’est qu’elle se diffuse selon une courbe en S. La première partie de cette courbe c’est l’incubation pendant laquelle on conçoit cette nouveauté, ensuite il y a une diffusion rapide qui est non-linéaire et imprédictible. Sur le marché américain, le smartphone a mis trois ans à se diffuser à plus de 50 % de la population. Cette rupture est un nouveau service au niveau du bien-être et du confort, mais elle peut être un enjeu de sécurité. Par exemple, pour produire les smartphones il faut du coltan, or cette matière première se trouve qu’en République démocratique du Congo, au Kivu, région qui est sécuritairement très instable. Il y a donc un enjeu d’approvisionnement. Pour reprendre le smartphone aujourd’hui, plus de 90 % des applications utilisent un signal GPS, qui est une vulnérabilité parce qu’aujourd’hui on est capable de leurrer un signal GPS et de porter atteinte auxdites applications.

Ces ruptures technologiques sont dans le secteur digital ; les cyberarmes donnent un avantage à l’attaquant contrairement à l’arme nucléaire qui donne un avantage à la défense et qui a un effet dissuasif. Là, les cyberarmes, dès qu’elles sont élaborées, sont utilisées pour préparer une éventuellement cyberguerre. L’activité de cyberguerre est quotidienne. Si cette activité est quotidienne, la défense est très difficile et coûte cher. Les Américains, pour produire le C17, ont investi plus de 40 milliards de dollars en recherche et développement (R&D). Les cyberguerriers chinois ont récupéré les 630 000 fichiers qui contenaient tout le programme R&D et piraté 10 000 ordinateurs chez Boeing. Cette cyberattaque a coûté moins de 400 000 dollars. On a toujours intérêt à pratiquer ces dernières, et par conséquent le seul moyen pour les entreprises est de se défendre au mieux. Elles seront toujours en dessous des capacités d’attaque

des adversaires, donc ce sont les Etats qui doivent s'investir dans cette cybersécurité. Il faut qu'ils soient en permanence dans l'attaque des adversaires potentiels pour les dissuader d'instrumentaliser et pour éviter de pousser trop loin l'avantage à l'attaquant. A partir de là, on a un équilibre des puissances qui est mis en place, et cet équilibre réactive des mécanismes qu'on avait vus au début de la guerre froide, mais qui nuisent aux stratégies de coopération. On a là l'origine des mesures qui ont été prises par le président Trump d'interdire l'utilisation de Huawei au marché américain. La diminution des interdépendances économiques et de leur rôle de stabilisateurs par l'émergence de ces mécanismes de cyberattaques permanentes fait qu'on voit apparaître dans la société internationale des pôles de cyberpuissances. Ils réactivent une forme de guerre que j'ai appelé dans mon article « la guerre froide 2.0 ».

L'Union européenne (UE) est justement un acteur central du multilatéralisme, qui défend l'approche d'un cyberespace sûr, ouvert et coopératif. Quel est le positionnement de l'UE dans cet espace, et vis-à-vis des grandes puissances qui l'investissent ?

Le multilatéralisme est le mot clef. Ce que l'on peut dire sur l'UE c'est qu'elle a une prise de conscience des cybermenaces qui est aussi rapide que cela l'a été aux Etats-Unis. En 2009, les Américains ont créé leur *cyber command* ; en 2008, l'UE a eu conscience des cybermenaces, notamment en raison de Stuxnet. Le niveau de conscience stratégique est similaire. L'UE se dote d'agences et de services pour sécuriser les réseaux, pour la lutte pour la cybersécurité et en soutien aux agences nationales des pays membres. Le levier des Etats-Unis en matière de cybersécurité c'est la dissuasion offensive. Donc en permanence, les cyberguerriers américains tentent de pénétrer les réseaux chinois, et réciproquement de l'autre côté du Pacifique. En ce qui concerne l'UE, le levier c'est la cohérence juridique sur le continent européen parmi les 27 pays membres. Ce levier est important parce qu'il va permettre d'établir des modalités de la gouvernance, du cadre réglementaire dans lequel les entreprises vont s'inscrire pour produire de la cybersécurité, donc faire la part entre ce qui est requis et ce en quoi il est nécessaire d'investir pour acquérir la confiance des utilisateurs et des consommateurs des produits et services numériques. Cela permet aux entreprises de se positionner sur un marché unique, et donc de développer leurs compétences et efficience. C'est aussi important parce que cela va permettre d'améliorer la qualité des moyens de cybersécurité qu'ils mettent en place. Par contre, il y a également une limite : c'est la dissuasion offensive. L'UE est une organisation internationale du point de vue sociologique, et donc elle n'a pas la fonction politique de désigner un adversaire. Par exemple, la Chine est une rivale systémique mais elle

n’a pas été désignée comme une ennemie. Donc en l’absence de désignation d’un adversaire, on ne peut pas pratiquer la dissuasion offensive qui consiste à pénétrer les réseaux chinois, à s’introduire dans les réseaux d’électricité et à envoyer quelques signaux à la Chine, d’établir un équilibre des puissances. Donc c’est une différence majeure pour l’UE, qui peut jouer avec une autre fonction : sociabiliser les cyberpuissances telles que la Chine et les Etats-Unis pour que celles-ci acceptent le cyberespace comme un bien commun, sur lequel toutes les entreprises ont intérêt à investir pour développer un niveau de confiance suffisant entre les marchés de consommateurs potentiels. Cela va être un défi diplomatique pour l’UE. Elle va être confrontée d’une part à une Chine qui revendique et affirme sa souveraineté numérique, notamment sur sa population, et puis des Etats-Unis qui voient le cyberespace comme un moyen de conquête des internautes qui sont loin de leur marché domestique. Donc entre ces deux stratégies, positions diplomatiques, l’UE va devoir jouer un rôle de stabilisation, sur lequel les institutions européennes ont beaucoup d’expérience maintenant puisque cela fait plus d’un demi-siècle qu’elles pratiquent ce genre de négociations.

Par rapport à la centralité des Etats-Unis dans le rapport de force lié au cyberespace, quelle est la place de l'OTAN pour l'UE sur les questions de cyberdéfense ?

Alors je ne comparerais pas les moyens en termes de sécurité. Je pense qu’il faut les prendre en termes de complémentarité et couplage éventuel. L’OTAN a un rôle important sur le continent européen depuis 1949. Elle a permis et permet toujours d’équilibrer en termes de forces conventionnelles contre des adversaires potentiels (on pense notamment à la Russie). On peut dire que dans le domaine du conventionnel et du nucléaire, l’OTAN joue son rôle et celui-ci devrait perdurer puisque la grande majorité des pays membres de l’Union souhaite que ce rôle perdure. Par contre, dans la cybersécurité, on s’est très tôt rendu compte que les alliances n’étaient pas forcément calquées sur les mécanismes des relations internationales, qui sont inadaptés.

Par exemple, en 2008, lors de la cyberattaque contre l’Estonie, pays membre de l’OTAN, les dirigeants estoniens ont invoqué l’article 5, et on a bien vu avec la réponse des autres pays que l’on n’allait pas utiliser des moyens conventionnels pour dissuader les *hackers* russes de submerger les serveurs estoniens de messages et de rendre la vie impossible aux Estoniens, qui ne pouvaient plus se connecter à leur compte en banque ou lire leur journal. La réponse de l’OTAN au cas estonien fut limitée. Elle a envoyé quelques experts, et le retour d’expérience sur cette cyberattaque ça a été le centre recherche de Tallin et la production du

manuel éponyme, qui permet d'avoir un ensemble de bonne pratiques et de recommandations à développer pour avoir une bonne culture de cybersécurité entre les pays membres de l'OTAN, mais on n'est pas allé au-delà. C'est simple à comprendre : l'anonymat qui est associé aux cyberarmes rend quasiment impossible, pour une alliance, de fonctionner. Les pays membres d'une alliance confrontés à une cyberattaque, dont l'anonymat est très significatif, sont conduits à une décision sous un voile d'ignorance, qui fait que les pays membres d'une alliance ne vont pas se mettre d'accord, parce qu'elle n'a pas d'effet suffisant pour la qualifier d'agression. Donc cet article 5, qui repose sur l'agression constatée d'un pays par d'autres pays membres, ne pourra pas être utilisé.

De plus, l'anonymat étant une constance de la cyberguerre, on va avoir une difficulté pour les pays membres de l'alliance à se mettre d'accord sur les adversaires. Selon Stephen Walt, grand spécialiste des alliances, une alliance ne peut être effective et durer dans le temps uniquement s'il y a une perception commune des menaces, et avec cet anonymat, on ne peut pas constituer une perception commune des menaces entre les pays, donc les alliances ne sont pas forcément l'outil adapté pour essayer de produire de la cybersécurité et répondre à une cyberpuissance menaçante. Pour l'instant, on observe des cas de coopération pour des opérations bien spécifiques pour renforcer le succès de cyberarmes. Le cas le plus documenté est la construction de la cyberarme Stuxnet entre les services américains et israéliens. Donc, le rôle que l'on peut envisager pour les alliances est encore à démontrer.

Vous insistez sur l'importance des acteurs du numérique et leur interdépendance avec leurs Etats, comme ont pu l'être les complexes militaro-industriels pour d'autres ruptures technologiques dans le secteur de l'armement. L'UE n'est pas un Etat, mais dispose de nombreuses entreprises et centres de recherche liés au numérique. Est-ce que cela peut être un atout, ou au contraire un frein dans son développement sur les enjeux du secteur ?

Non, au contraire, j'ai dit que les institutions européennes pouvaient être considérées davantage comme des organisations internationales que comme des Etats. Mais ce sont des organisations internationales qui sont très particulières, et qui ont développé une capacité à permettre à des entreprises de développer leurs activités dans un cadre appelé le marché. Donc l'UE a tout à fait les moyens de permettre le développement d'un écosystème d'entreprises digitales qui soient efficientes et qui pourront produire de la cybersécurité. Là, elle a un rôle qui est tout à fait normal, qui est naturel et a un savoir-faire et des moyens permettant de développer

des écosystèmes pour les entreprises. A ce niveau-là, l'UE a une carte à jouer, notamment avec le cadre juridique. Le but sera de développer un point de vue commun selon lequel le cyberespace est un bien commun. Le principal enjeu du cyberespace sera de réduire le risque d'utilisation du cyberespace comme un environnement privilégié de la diplomatie coercitive. On se place à un niveau de stratégie en termes de relations internationales et entre l'ensemble des acteurs tant étatiques que non étatiques (comme l'UE). Les entreprises sont les entités sociales qui permettent aux ressources humaines de se développer en matière de moyens, tant de cyberattaque que de défense. Ce sont des entités qui pourront orienter les ressources humaines vers la production de sécurité.

QUESTIONS DU PUBLIC

Depuis deux ans le ministère des Armées recrute beaucoup dans les profils dits cyber. Sommes-nous en retard dans le recrutement de ces cyberguerriers ou pas du tout ?

Il n'y a pas nécessairement de retard en termes de volume, mais il y a des difficultés en matière de profils. On a tendance à assimiler les activités de cybersécurité à des activités de développement informatique par des ingénieurs ou des techniciens, mais ce n'est pas ça. La cybersécurité nécessite d'être capable de faire une analyse des menaces, des enjeux géopolitiques, de développer des stratégies de diplomatie et de relations internationales, donc les spécialistes cyber viennent autant du secteur technique que des sciences sociales. Elle est là la grande difficulté : c'est d'arriver à convaincre les étudiants venant des sciences sociales de s'investir dans ce secteur de la cybersécurité. Une première raison de s'investir c'est que ce qui est fondamental dans la cybersécurité c'est la capacité à analyser une menace pour permettre à une entité, un Etat ou une entreprise, de dimensionner les ressources qu'elle va devoir consacrer pour réduire le risque porté par cette menace. Ce n'est pas une capacité qui est développée dans les écoles d'ingénieurs. La deuxième difficulté c'est d'arriver à convaincre les étudiants en matière de sciences sociales qu'ils ne doivent pas être victimes du syndrome de l'imposteur.

Une bonne familiarité avec votre smartphone et vous avez le niveau technique suffisant pour discuter avec un technicien de la cybersécurité.

Les entreprises recrutent, mais cette tendance est-elle encore vraie ou cela a-t-il tendance à s'amenuiser avec le temps, parce qu'un recrutement massif a été fait ?

La dynamique du marché est toujours aussi forte, mais le niveau d'exigence a monté. Maintenant, il faut avoir fait son stage ou son mémoire dans la cybersécurité ce qui n'était pas le cas il y a quelques années. Cela permet de montrer son appétence pour ce domaine.

Ne pensez-vous pas que le multilatéralisme est un frein pour l'émergence d'une puissance européenne, les autres puissances ne jouant pas avec les mêmes règles, notamment au niveau de la protection des données personnelles ?

Je crois qu'il ne faut pas poser la question en se disant que l'UE n'est pas un Etat donc c'est un problème. L'UE est l'UE, il y a un processus historique donc il faut la regarder comme une entité avec des forces et des faiblesses. Il faut réussir à construire une stratégie en rapport avec ces dernières. Parmi les atouts qu'elle a, il y a la capacité de sociabilisation des acteurs qui interviennent sur le continent européen, que ce soient des entités étatiques ou des entreprises. Après, de toute façon, dans le domaine de la sécurité il faut être lucide : on est souvent réactif et peu proactif. Ce sont donc les difficultés que l'on va rencontrer au fur et à mesure du développement des services digitaux qui vont les conduire à faire pression sur l'UE, pour que celle-ci s'investisse dans le cadre réglementaire, et peut-être qu'à terme les Etats réussiront à mettre ensemble des moyens et des ressources, on verra émerger des agences européennes avec des moyens plus importants.

Les cyberattaques, armes invisibles stratégiques, impactent-elle la sécurité énergétique ? Une guerre invisible sera-t-elle le prochain défi géopolitique ?

Alors, la guerre invisible a lieu tous les jours. Par contre, les cyberattaques qui échouent sont visibles. Dans cette guerre invisible, il y a un niveau d'effet qui est très large. Elle consiste à pénétrer les réseaux de l'adversaire, à lui signifier que l'on a des capacités et que l'on subit les attaques, mais il ne faut pas qu'elles dépassent un certain seuil, ou pas. Ainsi, toute la difficulté réside dans la fixation de la ligne rouge de l'acceptabilité de l'intrusion et du risque de la perte de contrôle de ses infrastructures vitales. C'est le même mécanisme que pendant la guerre froide. En Europe, on avait un rideau de fer très précis qui était dessiné, on savait donc quelle ligne les soldats du Pacte de Varsovie ne devaient pas franchir.

Cette guerre invisible est stratégique dans le sens où elle implique les Etats. Les Etats n'ont pas le choix que de s'impliquer pour compléter la cybersécurité des entreprises en pratiquant la dissuasion offensive et donc on a un équilibre des puissances classique dans le cyberespace qui se met en place. C'est comme ça que l'on peut analyser ces enjeux de cybersécurité.

Le domaine de la santé est particulièrement visé aujourd'hui par les cyberattaques, plus particulièrement des *ransomwares*. On sait que des réponses nationales sont en train d'être construites pour renforcer ce secteur, mais pensez-vous qu'une réponse européenne voire internationale pourrait permettre une meilleure coopération pour lutter contre ces attaques ?

Alors, les attaques que nous avons observées sur les hôpitaux semblent provenir de réseaux criminels. Ils ont pour objectif de s'enrichir rapidement à partir de l'identification d'une faille dans les réseaux informatiques et d'exploiter cette faille le plus rapidement possible. Pour l'instant c'est ce que l'on observe. Ce type de cyberattaque bénéficie déjà du soutien de l'Union européenne. Après, en termes de coopération au niveau global, on est plus limité dans l'échange d'informations parce que les réseaux criminels sont souvent à l'étranger et sont des acteurs tiers des Etats dans leur propre cyberattaque. C'est un dommage collatéral du fait que l'anonymat est renforcé par l'usage de réseaux criminels. Ils bénéficient d'un peu d'impunité pour pratiquer des cyberattaques qui leur permettent de s'enrichir et d'entretenir leurs ressources humaines qui sont à l'origine des cyberattaques. Le levier le plus important serait de convaincre les pirates qui travaillent pour des réseaux criminels qu'ils peuvent gagner plus en faisant de la cybersécurité dans les entreprises. C'est le défi majeur. Dans la fameuse conférence des pirates aux Etats-Unis, le directeur de la CIA va tous les ans tenter de recruter des jeunes pirates européens pour les convaincre de construire la cybersécurité des Etats-Unis.

Et cela fonctionne ? Cela existe également en France ?

Ah oui ! On suppose qu'il y a un nombre constant de personnes qui peuvent travailler pour les réseaux criminels ou pour les agences étatiques. C'est le problème. La clef de la cyberpuissance c'est les ressources humaines. Donc c'est toutes les institutions sociales qui

permettent à ces ressources humaines de manger tous les jours : ou bien ils vont faire cyberguerriers ou bien ingénieurs responsables en cybersécurité.

L'Union européenne a pour objectif de devenir un acteur majeur du numérique au niveau de la recherche et développement. Est-ce que le cyber fait partie intégrante de ce processus stratégique ou est-ce qu'il reste à part selon un angle essentiellement sécurité/défense ?

L'UE est un acteur majeur pour la promotion d'un écosystème de recherche dans les moyens de la cybersécurité, mais cet écosystème est en complément des moyens propres développés par les Etats et leurs agences. Donc la cybersécurité c'est la conjonction d'un ensemble d'acteurs qui partagent, au mieux leur intérêt, des ressources humaines, leur savoir-faire et des outils qu'ils mettent au point.

L'attaque contre les centrifugeuses iraniennes (Stuxnet) nécessitait que le ver puisse être uploadé sur le site. Désormais, une telle attaque contre l'Iran serait extrêmement difficile à mener, existe-t-il des technologies capables de s'immiscer dans de tels sites ?

Je voudrais faire tomber tout de suite un mythe des cyberattaques : elles ne consistent pas à appuyer sur la touche « Enter » d'un clavier et à couper l'électricité d'un pays. Pourquoi ? Parce que lorsqu'on commet une attaque, il faut énormément d'informations sur la cible que l'on veut atteindre. Tout simplement parce que si l'on est un acteur responsable, on utilise toujours une arme en contrôlant les effets de cette arme.

Dans le cas de la coopération entre Israéliens et Américains pour Stuxnet, la partie la plus longue a été la phase de tests pour être sûrs que Stuxnet allait bien attaquer les bonnes centrifugeuses. Cette collecte d'informations pour préparer une attaque, c'est du renseignement humain. Bien sûr, il y a du renseignement image, du renseignement signal, etc., mais c'est principalement du renseignement humain. Surtout dans la capacité d'intrusion, il y a très souvent de l'ingénierie sociale. Aujourd'hui, quand vous faites appel à un consultant en cybersécurité, il y a toute une partie d'étude des vulnérabilités sociales de l'entreprise, comme la résilience dans son système de sécurité à l'entrée de l'entreprise, tout simplement parce que si un pirate pénètre à l'intérieur d'un bureau et trouve un mot de passe, il a accès à tout le système.

La cyberattaque de TV5 Monde c'est parce que le directeur de la régie avait été interviewé et que sur le tableau blanc derrière lui, il y avait le mot de passe de l'administrateur système. L'ingénierie sociale est aussi importante que toute la partie conception. Donc les dimensions humaine et sociale d'une cyberattaque sont aussi importantes que la dimension technique.

Vous parliez de l'importance d'une réponse sociale aux attaques cyber. Une campagne de prévention massive auprès du grand public ne serait-elle donc pas une première réponse, notamment pour se prémunir d'une attaque criminelle ? Une coopération internationale sur ce genre d'opérations de communication et de formation existe-t-elle ?

Alors, des formations propres à cela, à ma connaissance non, mais parce que cela s'acquiert sur le terrain. L'enjeu de la formation des collaborateurs d'une organisation étatique ou non étatique c'est que tout le monde à un profil différent concernant les risques. Il y en a qui aiment le risque : ils vont tomber sur une clef USB par terre dans le parking de l'entreprise, ils vont la prendre et la brancher pour voir ce qu'il y a dedans, voire l'utiliser. Même à la NSA certains ont été vulnérables à cette technique.

La difficulté de la formation réside dans le fait qu'il est nécessaire qu'elle cible les bons publics et qu'elle mette en place les bons moyens de formation, en adaptation avec le public ciblé. C'est un problème d'ingénierie de formation.

Pourriez-vous donner votre avis sur la création d'une unité conjointe de cybersécurité en Europe, pour lutter notamment des cyberattaques ?

L'UE a tout intérêt à sociabiliser les acteurs pour faire prendre conscience du caractère de bien commun du cyberespace.

En parlant de la Chine, COMAC a-t-il bénéficié des attaques cyber pour l'avion C-19 ?

Pour vendre en Chine, les entreprises européennes et américaines doivent passer une *joint-venture* avec des entreprises chinoises. Dans cette *joint-venture*, il y a une clause de transfert des technologies. Donc le C-19 a bénéficié de ce transfert de technologies, notamment de la part d'Airbus avec de la technologie 3-20. Ensuite, les Chinois ont acheté un A320, et ils

l’ont totalement démonté. Puis, ils ont fait du cyber espionnage. Les pratiques de cyber espionnage sont tellement pratiquées depuis deux décennies qu’il serait étonnant que les avionneurs américains et européens n’aient pas subi quelques piratages qui aient permis à l’avionneur chinois de monter en puissance plus rapidement. Les Chinois répondent « vous devriez être content que l’on vous espionne cela montre que vous êtes les meilleurs ».

La France lance-t-elle également des cyberattaques contre ses rivaux, et fait-elle de l’espionnage industriel ?

C’est une question très difficile. A ma connaissance non, aucune cyberattaque révélée, donc qui aurait échouée, n’a été attribuée à la France.