01 avril 2019
Minute Tech

Pourquoi le problème posé par Huawei n'est pas tant celui de l'espionnage chinois que celui des bugs de sécurité

Le dernier rapport annuel du HCSEC britanniques est sévère. Les produits et méthodes du fabricant chinois Huawei sont en effet pointées du doigt, et jugés problématiques en termes de cybersécurité.

Avec Franck DeCloquement

Atlantico :Dans la guerre qui oppose les États-Unis au constructeur chinois, le rapport britannique publié jeudi dernier à mis en lumière un certain nombre de problèmes de sécurité avec les appareils du fabricant de téléphonie Huawei. Quels sont-ils exactement ? Quelle part de risques pour les utilisateurs européens que nous sommes, et pour nos démocraties occidentales ?

Franck DeCloquement : Avant toute chose, il ne faut pas perdre de vue l'essentiel, et d'abord replacer toute cette affaire dans la perspective américaine bien plus large des affrontements géopolitiques entre grandes puissances. A commencerpar la préservation de leurs intérêts en matière de « sécurité nationale ». Intérêts féroces qui ne sont évidemment pas conjoints, ni même partageables avec leurs alliés dans de nombreux cas de figures. Loin s'en faut…Les tensions existantes en matière d'attribution des cyberattaques entre certains services de renseignements occidentaux et ceux de la NSA sont à ce titre notable. Et dans ce contexte parfaitement délétère de **guerre économique** ouverte avec la Chine,comme vous le rappelez fort justement en introduction de votre question, les Etats-Unis considèrent que l'Union européenne a pour obligation absolue de s'aligner sur les décisions stratégiques de Washington, en se conformant en l'état à leurs décisions. Et de convaincre leursalliés historiques,dans la foulée, de ne pas acheter ou déployer d'équipement de Technologies avancée Huawei, pour leurs réseaux de téléphonie mobile de prochaine génération 5G. Arguant à ce titre qu'ils craignaient que la structure des télécommunications ne soit compromise par l'usage de ces technologies chinoises. Les leurs par la même occasion.

Le géant chinois est devenu un leader incontestable de la nouvelle génération ultrarapide de l'internet mobile. Et se passer de son expertise en la matière risque indubitablement de freiner le développement de cette technologie cruciale en Europe. Ce qui explique aussi qu'un responsable du département d'Etat américain a récemment déclaré à ce propos: « nous disons qu'il faut être très, très prudent et nous exhortons les gens à ne pas se précipiter pour signer des contrats avec des fournisseurs non fiables de pays comme la Chine ». Effectuant dans la foulée une « tournée des grands-ducs » dans toute l'Europe,afin de convaincre les principaux responsables nationaux de cet impératif prioritaire aux yeux des Etats-Unis. Affirmant aussi vouloir utiliser sans ambages, tous les événements diplomatiques du secteur de la téléphonie mobile pour mettre en garde et influencer dans leurs décisions, les gouvernements européens. A ce titre, le « Cyber DiplomacyAct », visant à créer au sein du département d'Etat un bureau dédié à la « diplomatie de cyberdéfense », a reçu du « House Committee on ForeignAffairs » le 7 mars dernier, un feu vert de principe. Et en cas d'adoption du texte, le patron de la NSA Paul Nakasone, le principal représentant des États-Unis en matière de cybersécurité et de l'US Cyber Command (USCYBERCOM),

devrait alors composer avec l'arrivée d'une « diplomatie d'influence américaine » dans le giron habituel du cyber.

Les pressions faites à ce titre sont d'ores et déjà patentes. Et le « Wall Street Journal » a d'ailleurs rapporté en février dernier que le ministre de l'Economie de la chancelière Angela Merkel avaiteu à subir une forme notable de « chantage au renseignement » de la part de Richard Grenell, l'ambassadeur américain à Berlin, en cas de prise de décisions contraires aux intérêts américains... On ne saurait-être plus claire dans les termes sur les conditions du « débat » transatlantique présent et à venir. Oublié évidemment dans l'interstice – avec une très grande pudeur – l'épée de Damoclès permanente que fait peser la surveillance globale exercée par l'appareil de sécurité national américain (NSA en tête),sur la préservation des intérêts économiques et stratégiques des pays de l'union européenne. Partant pour beaucoup de relais américains en coulisses du principe que : « mieux vaut-être espionné par les moyens électroniques d'un régime démocratique ami, que par ceux coercitifs d'un régime autoritaire non-occidental »…

Cette menace « amicale » s'est encore accentuée dernièrement, quand le commandant suprême des forces alliées en Europe, le général américain Curtis Scaparrotti, a affirmé que les forces de l'Otan cesseraient de communiquer avec leurs collègues allemands, si jamais Berlin s'associait avec des groupes Chinois tel que Huawei : « Nous craignons que la structure de leurs télécommunications ne soit compromise car, tout particulièrement avec la 5G, dont la largeur de la bande passante et la capacité à soutirer des données sont incroyables », a-t-il fait savoir.

Pour autant, L'Allemagne a depuis lancé ses enchères pour l'octroi des chantiers de sa future 5G.Refusant de bannir « à priori »les équipementiers chinois comme Huawei. Faisant fi pour l'heure – au moins en apparence – des menaces très nettes de Washington de revoir très à la baisse leur coopération sécuritaire transatlantique en matière de renseignement.

Pour revenir sur la nature des risques eux-mêmes, notons que le conseil de surveillance du**Centre d'évaluation Huawei Cyber Security** qui a produit le rapport que vous évoquez, souligne la difficulté de déterminer si le code audité par le groupe est en réalité le même que celui utilisé dans les produits Huawei. Le défi posé par cette évaluation des risques sous-jacents aux produits Huawei dans leur ensemble,est lié aux problèmes plus vastes rencontrés par le secteur lui-même. C'est-à-dire, la vérification précise de l'intégrité des logiciels propriétaires. Certaines des vulnérabilités de sécurité systémique révélées dans le rapport du **« HCSEC** » sont extrêmement simples. Mais les analystes de la sécurité soulignent aussi que ce type d'audit révélerait probablement des erreurs gênantes dans les produits de la plupart des entreprises du secteur numérique, même si les erreurs de Huawei sont peut-être « plus flagrantes » que chez d'autres.

N'en doutons pas, bien que le rapport ne conclue pas que les produits du groupe Huawei incluent des « backdoors » néfastes (portes arrières dérobées en français), l'ampleur des problèmes découverts va probablement encore servir les efforts diplomatiques renouvelés de la Maison-Blanche, pour éloigner les États-Unis et leurs alliés de l'emprise de la firmechinoise. Le Royaume-Uni a tenté d'intégrer en toute sécurité les produits de Huawei à son infrastructure de télécommunication depuis près de dix ans. Mais le rapport indique également que l'exposition risque d'être trop lourde pour que le pays puisse gérer seul« le risque Huawei »lui-même. Tous les spécialistes le savent :le Royaume-Uni tente depuis très longtemps de dissocier les aspects « techniques » de la confiance numérique,et ceux en lien avec l'espionnage rendu possible par le biais des techniques digitales. Arguant que ce risque technique est le plus souvent « gérable », et qu'il existe toujours un risque de toute façon, et ceci, quels que soient l'origine ou la nationalité des dispositifs informatiques considérés…

Huawei a annoncé qu'il cherchait à résoudre ces problèmes de sécurité. Doit-on pour autant croire l'entreprise chinoise ? Qu'aurait-elle à gagner à ne pas résoudre ces problèmes ?

Du fait de son avance technologique notable en matière de 5G, on le sait très bien, les sociétés de télécommunications américaines ont en grande partie eu la volonté d'éviter Huawei depuis un rapport incriminant du Congrès datant de 2012.Mettanten avant les menaces patentes faites à la sécurité nationale des Etats-Unis, que font potentiellementpeser la pénétration des produits de la société Chinoise sur le marché intérieur. Et le président DonaldTrump réfléchit d'ailleurs actuellement à un décret visant à interdire totalement ces équipements chinois. Mais les opérateurs des réseaux d'autres pays, y compris ceux du Royaume-Uni, ont travaillé– dans l'interstice – à intégrer en toute sécurité les équipements sans fil et à faible coût de Huawei. Le Royaume-Uni avait doncinitialement créé à ce titre le« **Centre d'évaluation Huawei Cyber Security** » ou **« HCSEC** » en 2010 pour justement auditer le matériel et les logiciels Huawei à leurs sorties d'usine**.** Et ceci, **avant leur envoi aux États-Unis**. C'est pourtant d'ici que sort le constat sévère fait aujourd'hui, irradiant toute la presse internationale sur les produits et méthodes controversées du fabricant chinois.

Sur le fond,ses antennes 5G sont considérées par Washington comme une version contemporaine du « cheval de Troie ». Les Américains soupçonnentsans ambages l'entreprise de transmettre des données essentielles au régime de Pékin, en vertu d'une loi locale obligeant précisément à la collaboration pour des raisons de sécurité nationale. A l'image en cela des Etats-Unis, rappelons-le, avec leurs propres fleurons de la Tech américaine : les GAFAML'Australie, le Japon et la Nouvelle-Zélande ont déjà exclu les équipementiers chinois pour ces raisons, et les services de renseignements occidentaux qui collaborent étroitement avec les centrales américaines, ont été nombreux à adresser à l'attention de leurs gouvernements respectifs, des mises en gardes de sécurité.

Pour sa part, Huawei affirme travailler à renforcer les protections de sécurité dans son flux de travail d'ingénierie, et affirme soutenir la collaboration entre les régulateurs industriels et internationaux, afin de garantir une sécurité robuste des réseaux de télécommunications dans le monde : « Le rapport du comité de surveillance HCSEC 2019 détaille certaines préoccupations concernant les capacités de Huawei en matière d'ingénierie logicielle », a déclaré la société dans un communiqué publié dans la presse. « Les problèmes identifiés ... apportent une contribution essentielle à la transformation en cours de nos capacités d'ingénierie logicielle ». La société s'est engagée à investir 2 milliards de dollars dans des améliorations techniques. Cependant, les observateurs disent qu'il est difficile de croire les promesses de Huawei, et si la firme Chinoise accordera effectivement la priorité à des changements significatifs.

Lien vers le contenu du rapport du**HCSEC** :

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

Jusqu'alors le gouvernement américain soupçonnait, entre autres, Huawei de menacer la sécurité nationale des Etats-Unis. Avec ce rapport du HCSEC, Huawei est-il lavé de tous soupçons d'espionnage ? Quid de ces rapports avec les pays étrangers ?

Le ministre allemand de l'Intérieur, Horst Seehofer, a déclaré en substance qu'il ne voulait pas ouvrir « un nouveau front » de guerre commerciale avec la Chine, alors que Berlin se dote déjà de loi défensive pour pouvoir contrer des prises de participation dans des entreprises allemandes jugées stratégiques par le pouvoir. La chancelière allemande assure que Berlin va « discuter » de sa stratégie en termes de protection des réseaux avec ses partenaires européens, dont Washington… Mais pour l'heure, « il n'y aura pas de bannissement formel ». Le gouvernement planche sur un catalogue de mesures valables pour l'ensemble des prestataires du chantier de la 5G : opérateurs, équipementiers, fournisseurs.Celles-ci vont de la clause de non-espionnage à l'obligation de tests en laboratoire pour l'ensemble des composants.En passant par l'obligation de publier des codes source utilisés dans les infrastructures. Dans certains cas spécifiques, le gouvernement allemand pourrait aussi demander le remplacement d'équipements déjà installés, « ce qui reviendrait à pouvoir exclure Huawei de certaines infrastructures, sans prononcer de bannissement formel », détaille pour sa part le journal Handelsblatt. Mais malgré le lancement des enchères nationales sur la 5G, aucune législation spécifique n'est encore à l'agenda législatif allemand, quand en France une proposition de loi similaire a été déposée par les députés de la majorité du président Emmanuel Macron.

De son côté, le patron de Huawei en Allemagne a depuis déclaré au quotidien Handelsblatt que le gouvernement chinois ne s'était pas immiscé dans ses activités, et que la société ferait à cet effet en sorte d'assurer sa transparence aux yeux des Occidentaux. « L'Etat n'a pas de participation dans Huawei, et il reste en dehors de notre entreprise », a déclaré Dennis Zuo au journal. De son côté, l'allemand Ulrich Kelber, commissaire à la protection des données, a déclaré au quotidien Handelsblatt spécialisé dans le journalisme économique, qu'il ne disposait d'aucun élément probantallant dans le sens d'une exploitation secrète de données, sans exclure pour autant que la Chine puisse faire des choses incompatibles avec la législation européenne : « C'est pourquoi nous devrions avoir une certaine autonomie technologique – du matériel jusqu'aux solutions logicielles », a-t-il récemment ajouté. Nous en sommes là, à l'heure où nous rédigeons ces lignes.