Affaire Huawei : au-delà de l'espionnage

Un test pour la dissuasion et un impondérable dans les négociations avec la Corée du Nord

Morgane FARGHEN | Fondatrice et directrice de l'*Asia Nuclear Initiative* (http://asia-nuclear-initiative.org/), Institut Thomas More.

La société Huawei est la cible d'une intense campagne de dénigrement conduite par plusieurs services anglo-saxons (cf. H. STEWART et J. RANKIN). Le mouvement a été rejoint, depuis quelques semaines, par les capitales de l'axe libéral progressiste qui s'étaient montré jusque-là bienveillantes à l'égard de la société, en dépit de la sensibilité de certaines de ses activités.

Sont dénoncés un essor fondé sur la pratique d'un *dumping* commercial, des activités d'espionnage alléguées (cf. C. FOUQUET) et les risques afférents à ses investissements dans le futur réseau de téléphonie mobile 5G (cf. G. CHAZAN et R. WRIGHT), pour lequel la répartition des parts aura d'importantes implications pour la défense. Ce texte met l'accent sur un autre aspect passé sous silence et pourtant essentiel pour comprendre le retournement diplomatique dont la société a fait l'objet en Europe au cours des dernières semaines : les allégations d'espionnage avec une dimension défense et dissuasion.

En décembre dernier, plusieurs milliers de télégrammes diplomatiques ont été dérobés à la Commission européenne (cf. *BBC*) et livrés au grand quotidien américain le *New York Time*s (cf. D.E. SANGER et N. PERLROTH). Dans une action quasi simultanée, deux autres attaques cyber sont conduites contre le *Los Angeles Times* et un centre de réfugiés à Séoul. Attaques multiples, ciblées et visiblement coordonnées, ces incidents ont d'emblée présenté les caractéristiques d'une campagne coordonnée dans le cadre de stratégies asymétriques. Dans l'hypothèse d'une attaque d'origine nord-coréenne, l'ombre de la Chine, liée à la Corée du Nord (cf. R. PEPER) par un accord de sécurité mutuelle, a pesé et derrière elle, la société Huawei.

Fleuron du secteur des télécommunications en quête de *leadership* commercial, la société Huawei apparaît dans la galaxie des structures chinoises implantées à proximité des institutions européennes où une politique d'influence agressive est conduite par Pékin pour faire contrepoids à celle des États-Unis dans le cadre d'une

rivalité sino-américaine qui prend l'Europe à partie. À la mi-décembre, après que la Commission européenne ait essuyé le feu d'attaques cyber, et alors que tous les regards se sont tournés vers la Corée du Nord et la Chine, les deux pistes privilégiées dans l'hypothèse d'attaques d'origine étatique, la société Huawei s'est fait remarquer par un comportement suspect.

La société chinoise aurait pu faire profil bas dans les jours qui ont suivi et se tenir, au moins provisoirement, à l'écart de toute activité de nature politique ou stratégique, elle en a décidé autrement, au risque d'attirer l'attention. Pendant que l'un de ses responsables se faisait le relais d'une campagne d'influence antiaméricaine sur les réseaux sociaux, la société a annoncé la création d'un centre de cybersécurité à Bruxelles (cf. HUAWEI). Une structure à même de revaloriser l'image de la société dans le contexte *post*-attaques et avec elle, celle de la Chine, mais pouvant à l'inverse héberger de futures actions offensives et ainsi les légitimer sous couvert d'un discours sécuritaire bien fondé.

Naguère soupçonnée de *dumping* commercial et de collusion avec les pouvoirs publics par les cercles sécuritaires anglo-saxons, mais protégée en Europe où elle bénéficiait d'une politique chinoise favorable, elle est devenue l'un des suspects de premier plan d'une possible affaire d'espionnage aux implications de défense et de dissuasion.

Huawei a été créée en 1987 par un chercheur travaillant pour le compte des forces armées chinoises au moment où la Chine a lancé ses vastes projets de développement des hautes technologies à partir d'une double stratégie de coopération avec les pays avancés et de captation technologique. La société incarne, par sa réussite commerciale autant que par les dimensions sensibles de ses activités, le succès et les ambivalences de la politique développement de la Chine depuis une trentaine d'années. Prise à partie dans un conflit d'influences entre la Chine et les États-Unis qui se mène jusqu'en Europe, elle confronte les chancelleries européennes à un dilemme sécuritaire majeur. La crise nucléaire nord-coréenne a ses ramifications en Europe, les attaques cyber en sont probablement l'une des dernières manifestations tragiques, et la société Huawei en est peut-être l'un des acteurs.

À quelques semaines de la relance des négociations sur la péninsule coréenne et du prochain sommet entre le *leader* nord-coréen Kim Jong-un et Donald Trump, l'Affaire Huawei est bien plus qu'un simple dossier d'espionnage, même si elle met en évidence, en effet, les pratiques peu scrupuleuses d'un fleuron technologique des télécoms rompu aux pratiques déloyales. Selon l'issue des enquêtes, la responsabilité attribuée et les adaptations des politiques de défense, l'Affaire Huawei a le potentiel de peser sur les équilibres au sein de la compétition/rivalité sino-américaine et au-delà, sur les négociations en perspective sur la péninsule coréenne et l'évolution de la question nucléaire nord-coréenne.

À l'abri des critiques en Europe, au moins jusqu'à l'épisode des attaques cyber, la société Huawei a vu ses soutiens se retourner les uns après les autres au cours des dernières semaines, à mesure que se sont répandues les appréhensions sur le double jeu de cette société et avec elles, sa possible implication dans les attaques. Du scepticisme bienveillant, les chancelleries européennes sont passées progressivement à une inquiétude légitime. Suspectée d'espionnage par plusieurs services de sécurités occidentaux et implantée à quelques encablures du quartier européen à Bruxelles, la société était prédisposée à attirer les regards dans l'hypothèse d'actions malveillantes de cette nature et de cette intensité.

Dissuader la Commission européenne de prendre des positions défavorables à Pyongyang sur la question nucléaire offrait à la Corée du Nord et à son allié un mobile pertinent pour conduire de telles actions, s'il s'avère en effet qu'elles ont été produites à l'instigation de l'un de ces deux pays visés en premier lieu par les soupçons d'attaque d'origine étatique. Le vote d'une résolution à l'ONU pour dénoncer les dérives autoritaires de Pyongyang et le coût financier de son programme nucléaire (cf. L. Byrne), sous l'impulsion de la Commission européenne donnait à Pyongyang les raisons objectives de redouter une inflexion européenne au profit d'une politique moins favorable à ses intérêts que lors des épisodes précédents.

Depuis plusieurs mois en effet, les Européens se sont moins préoccupés de soutenir une politique de dénucléarisation exigeante aux côtés des Américains, qu'à donner la réplique à une politique américaine de tarifs douaniers, destinée à sanctionner l'Europe dans le cadre d'une diplomatique coercitive qui n'avait plus seulement pour objet de faire pression sur la Corée du Nord et ses alliés, mais aussi les pays ayant rejoint le discours stratégique de ces deux pays. Paris et Bruxelles avaient adopté le discours de paix de Pékin sur les risques d'escalade, elles en subissaient les frais. La diplomatie coercitive n'a pas suscité d'introspection à Paris et à Bruxelles, elle les a au contraire rapproché de Pékin.

Les attaques cyber seraient dans ce scénario hautement probable, une tentative d'intimidation pour à nouveau retourner les positions diplomatiques de l'Union européenne. Une forme de représailles à la résolution votée à l'ONU contre Pyongyang et un chantage opéré avec des moyens non conventionnels, offensifs, et difficiles à détecter/qualifier, néanmoins déstabilisateurs. Autant de caractéristiques conformes aux stratégies asymétriques compatibles avec les pays dotés, ou aspirants, non alliés comme la Corée du Nord et la Chine (cf. Tribune News Service).

Si la société n'a pas aidé leurs auteurs en apportant un soutien logistique en amont, ce qui en ferait un complice, elle a au moins contribué à en amortir les retombées en participant à la contre-campagne d'influence pour entretenir le doute, faire diversion ou en atténuer les retombées. Dans les deux hypothèses

privilégiées, la société est apparue au premier plan d'une enquête dont l'objectif reste pour les organismes de sécurité mobilisés, d'en définir le rôle.

Par leurs implications, les attaques cyber ont de nouveau confronté les politiques de défense européennes à un dilemme stratégique important. Les attaques cyber contre la commission et leur corollaire, l'Affaire Huawei, confrontent les politiques de défense européenne à des choix de politique de sécurité, de défense et de dissuasion dont l'issue est de nature à redessiner les paramètres et la grammaire des rapports de force à l'échelle régionale, mais aussi au sein de l'alliance transatlantique et à l'internationale jusque sur la péninsule.

Placée au cœur de toutes les attentions, et de plus en plus isolée, la société est devenue le nouveau catalyseur des dilemmes de sécurité et de défense, y compris et même surtout en France. Seul et dernier pays doté de l'arme nucléaire de l'UE, la France a refusé de se laisser dicter sa politique extérieure et n'a pas accepté de laisser discréditer sa stratégie de défense cyber par la Corée du Nord ou ses alliés à qui elle tendait la main. Le discours prononcé par le président français Emmanuel Macron lors du Forum de Paris pour la paix en novembre 2018 était un geste d'ouverture et d'apaisement. Il a été mis en échec.

Piquée, Paris définit une riposte à partir de messages clairs destinés à dissuader les auteurs à recommencer en leur démontrant que leurs actions sont contre-productives (cf. V. Adam). À l'inverse d'un désengagement, Paris a rehaussé son implication dans la gestion de crise, énonçant son intention de rejoindre la coalition des forces dépêchées dans les eaux au large de la péninsule pour lutter contre les contournements de sanctions. Elle a redéfini sa doctrine cyber dans laquelle elle énonce la possibilité de représailles de même nature, et a signé, le 22 janvier 2019 à Aix-la-Chapelle, un Traité de sécurité mutuelle (controversé) avec l'Allemagne.

Un mois après les attaques, l'affaire Huawei divise les politiques publiques en France, comme elle l'a fait ailleurs, en particulier au Canada où l'arrestation de la responsable financière de la société pour espionnage, et les représailles de Pékin, ont suscité quelques résistances en particulier de l'ambassadeur d'Ottawa à Pékin (cf. A. Pélouas). Alors que Bercy a déclaré, une semaine après les attaques, que les investissements de la société sont les bienvenus en France (cf. *AFP*), une déclaration reprise par l'ambassadeur de France à Pékin, en janvier, cette ligne est déjà rompue.

Dans le contexte international actuel, dominé par les rapports de forces dans un environnement multi-crises, les temps de réactions se sont contrits. Le temps de l'enquête est parfois incompatible avec celui de la réplique, un avantage pour les stratégies asymétriques dont la force est précisément de profiter des vulnérabilités de cette nature dans les démocraties libérales. Le risque de voir les enquêtes se perdre dans des querelles d'experts pouvait conduire à la paralysie.

Après les attaques contre un hôpital londonien et un grand groupe français en 2017, la Commission européenne, le *Los Angeles Times* et un centre de réfugiés en 2019, les prochaines attaques seraient à nouveau rehaussées en intensité et dans la force symbolique. Elles pourraient potentiellement atteindre le Quai d'Orsay ou d'autres ministères. Les attaques ont humilié la Commission et mis en échec le discours de Paris. Accepter, se taire, supporter serait incitatif, et reviendrait à envoyer un feu vert à Pyongyang et Pékin pour recommencer.

⁂

Jusqu'en décembre dernier, Pyongyang et Pékin ont bénéficié de la sympathie de l'axe libéral progressiste pour relaxer la pression américaine. Cette tendance est désormais inversée. La pression internationale s'alourdit sur Pyongyang et derrière elle, sur Pékin. Les deux alliés s'ingénient depuis plusieurs mois à retarder ou compliquer le travail de non-prolifération nucléaire sur la péninsule pour lequel la Chine devrait, en qualité de signataire du Traité de non-prolifération (TNP), et membre permanent du Conseil de sécurité, être non pas un acteur perturbateur, mais un soutien actif et coopératif. Les attaques ont redéfini les équilibres.

Éléments de bibliographie

Adam Victoria, « Le gouvernement "conscient des risques" d'espionnage liés à Huawei », *Boursier.com*, 24 janvier 2019 (www.boursier.com/).

AFP, « Les investissements de Huawei "bienvenus" en France pour Bruno Le Maire », *Le Point*, 7 décembre 2018 (www.lepoint.fr/).

Byrne Leo, « UN Committee passes resolution condemning North Korea's human rights record », *New York News.org*, 15 novembre 2018 (www.nknews.org/).

« European Union diplomatic communications 'targeted by hackers' », *BBC*, 19 décembre 2018 (www.bbc.com/news/world-europe-46615580).

Chazan Guy et Wright Robert, « Germany looks to ban Huawei from 5G », *Financial Times*, 18 janvier 2019.

Fouquet Claude, « Huawei licencie son employé arrêté en Pologne pour espionnage », *Les Échos*, 11 janvier 2019 (www.lesechos.fr/).

Huawei, « Huawei Transparency and Cybersecurity Centre in Brussels », 25 mai 2018 (https://huawei-brussels-office.prezly.com/huawei-transparency-and-cybersecurity-center-in-brussels).

Macron Emmanuel, « Discours du président de la République », Forum sur la gouvernance de l'*Internet*, UNESCO, 12 novembre 2018 (www.elysee.fr/)

Pélouas Anne, « Affaire Huawei : Justin Trudeau limoge l'ambassadeur du Canada en Chine », *Le Monde*, 28 janvier 2019.

Peper Rosie, « North Korea may be behind a massive cyber attack on a South Korean bitcoin exchange », *World Economic Forum*, 22 décembre 2017 (www.weforum.org/).

Sanger David E. et Perlroth Nicole, « Cyberattack Disrupts Printing of Major Newspapers », *The New York Times*, 30 décembre 2018 (www.nytimes.com/2018/12/30/business/media/los-angeles-times-cyberattack.html).

Stewart Heather et Rankin Jennifer, « Theresa May to urge EU leaders to take action on cyber-attacks », *The Guardian*, 17 octobre 2018 (www.theguardian.com/).

Tribune News Service, « How did barely connected North Korea become a hacking superpower? », *South China Morning Post*, 1er février 2018 (www.scmp.com/).

Courriel de l'auteure : morgane.farghen@cea.fr