Les services de sécurité paniquent face à la 5G

Jean-Pierre Stroobants

La technologie réduirait la capacité des forces de renseignement à identifier et localiser les mobiles

BRUXELLES - bureau européen

Les responsables européens n'ont pas cédé, en mars, aux pressions américaines et n'ont pas (encore ?) banni le chinois Huawei du futur réseau sans fil 5G, mais ils découvrent que les éventuels risques d'espionnage et de menaces sur des secteurs stratégiques ne sont pas les seuls dangers auxquels les pays membres de l'Union européenne devront faire face. En effet, les services de police et de renseignement alertent sur le fait que le développement de la 5G pourrait singulièrement compliquer, voire rendre impossibles, les actuels repérages de communications, écoutes et localisations, outils indispensables dans la lutte contre les criminels et les terroristes.

Les ministres de l'intérieur ont pris connaissance, vendredi 7 juin, à Luxembourg, d'un rapport de Gilles de Kerchove, coordinateur de la politique antiterroriste de l'Union européenne (UE). Ce document, lu par *Le Monde*, détaille des mises en garde qu'avait déjà formulées, en avril, Europol. Et il va alimenter « l'étude de risques » que la Commission doit présenter en octobre, en collaboration avec l'Agence européenne pour la cybersécurité, à propos de Huawei, soupçonné d'entretenir un lien organisationnel avec l'Etat chinois en vue d'exercer des *« activités d'influence »*, mais aussi de la sécurité de la 5G en général. Des standards, ou règles minimales, devraient ensuite être définis.

La réflexion européenne a, jusqu'ici, peu porté sur le rôle des forces de l'ordre dans la future société de la 5G où, selon les experts, 20 milliards d'appareils seront bientôt connectés. Et pourtant, la nouvelle technologie *« crée la panique chez les officiels chargés de la sécurité parce qu'elle pourrait réduire dramatiquement leur capacité à mener des "interceptions légales", plus connues sous le nom d'écoutes téléphoniques »*, note une récente étude de Statewatch, une ONG britannique attachée à la défense des libertés.

Nécessité d'un débat public

Première difficulté : la 5G pourrait fortement compliquer l'identification et la localisation des appareils mobiles. Le cryptage rendrait, en effet, impossible la lecture de l'IMSI (International Mobile Subscriber Identity), le numéro code unique qui permet à un réseau de téléphonie mobile d'identifier un usager lors de chaque appel. Ce code est stocké dans la carte SIM – la puce qui enregistre les données pour l'abonné – et n'est pas connu de l'utilisateur.

Pour identifier, repérer ou localiser un suspect, la police interroge des opérateurs télécoms et un juge peut ordonner leur collaboration pour obtenir des informations sur le fonctionnement d'un système informatique et sur la manière d'accéder à des données. Sans accès au numéro code, il serait illusoire d'identifier et de tracer un usager.

Le débat sur le cryptage des données, mettant en balance la protection des données et les exigences de la sécurité, est toujours en cours. Un spécialiste du

renseignement juge qu'en tout état de cause, même s'il sera possible – par les métadonnées, ces « données servant à en décrire d'autres » – de déterminer *« qui appelle, quand, et où »,* il sera beaucoup plus complexe de connaître *« le quoi et le pourquoi ».*

Deuxième obstacle : la technique 5G rendrait obsolète l'usage d'intercepteurs (ou IMSI-*catchers*), des appareils de surveillance capables d'enregistrer le trafic des communications mobiles, de récupérer des informations à distance et de pister les mouvements des utilisateurs. Ces fausses antennes-relais, qui exploitent les faiblesses des systèmes actuels, dont la 4G, sont critiquées parce qu'elles ciblent toutes les personnes dans leur rayon d'action – et pas seulement un suspect. Europol les présente cependant comme *« indispensables pour l'exercice d'une surveillance légale ».*

Or, une nouvelle fonction de la 5G permettrait aux usagers comme aux opérateurs de détecter les intercepteurs IMSI, réduisant ainsi à néant ce que les experts de l'office policier européen décrivent encore comme *« le plus important des outils opérationnels et tactiques d'investigation ».*

Les soucis des responsables de la sécurité concernent ensuite l'architecture du réseau 5G et sa *« découpe virtuelle »,* destinée à mieux répondre aux besoins spécifiques des différents secteurs d'activité, les uns pouvant être surtout soucieux de fiabilité, d'autres de la largeur de la bande passante, d'autres encore du temps de réponse. Sur une plate-forme commune, on retrouverait donc plusieurs opérateurs, nationaux ou étrangers, peut-être soumis à des législations différentes – la sécurité restant une prérogative nationale : cette fragmentation compliquera singulièrement la tâche des forces de l'ordre.

L'évolution technologique comporte une autre caractéristique encore : « l'informatique de pointe » (Edge-Computing) utilisant la 5G permettra à des appareils de communiquer directement entre eux, sans passer par le réseau centralisé d'un opérateur. Les atouts : rapidité et sécurité. L'inconvénient pour les forces de sécurité : moins de renseignements récupérables.

Les dirigeants d'Europol et M. de Kerchove évoquent des réponses possibles : des standards et des législations plus stricts pour encadrer la 5G et des décisions qui ne seraient pas pilotées uniquement par l'industrie – la détermination des spécifications techniques internationales dépend largement d'elle et ses contributions financières lui octroient des droits de vote proportionnels au sein de l'organisme de coopération entre les instances de standardisation en télécommunications.

Statewatch souligne, quant à elle, la nécessité d'un débat public : sans nier la prise en compte des exigences du maintien de l'ordre, l'ONG note que la 5G est également porteuse de nouvelles techniques beaucoup plus invasives et menaçantes. Le contrôle des services chargés de la surveillance, en quête de nouveaux outils pour assumer leur mission, mérite donc aussi une vaste réflexion.