OPINIONS

« L'affaire Pegasus montre parfaitement les faiblesses de l'Europe en matière de cyberagressions »

TRIBUNE

Collectif

Face aux différentes attaques, l'Union européenne et la France doivent accepter la notion de rapport de force et oser des mesures de rétorsion, estiment Bernard Barbier (ex-DT de la DGSE), Edouard Guillaud (ex-chef du CEMA) et Jean-Louis Gergorin (ex-chef du CAP du Quai d'Orsay) dans une tribune au « Monde ».

Publié aujourd'hui à 03h24, mis à jour à 06h57 | Lecture 7 min.

Le site Web de la firme israélienne NSO, à l'origine du logiciel espion Pegasus. MARIO GOLDMAN / AFP

Tribune. Actuellement, la France et plus généralement l'Europe subissent des cyberagressions massives. D'une part, de type cyberespionnage, avec notamment le logiciel Pegasus, vendu par la société israélienne NSO et utilisé hors de son cadre légal, le cybervol de technologies, par exemple par la structure APT31 (Advanced Persistent Threat, entité permanente, souvent étatique, de hackeurs), en l'espèce, chinoise ; et, d'autre part, de cybercoercition, notamment des attaques de type rançongiciel *[logiciel rançonneur, de l'anglais « ransomware »]* provoquées par des cybercriminels jouissant d'une sorte d'impunité en Russie.

L'affaire Pegasus montre parfaitement les faiblesses de l'Europe. C'est une application sophistiquée qui permet une écoute « active » des téléphones portables grand public en injectant un logiciel

malveillant utilisant une faille inconnue du système d'exploitation Apple (iOS) ou Google (Android). Les systèmes de type Pegasus « contournent » ainsi le chiffrement maintenant généralisé des messageries de smartphones telles WhatsApp ou Signal.

Écouter aussi | **Pegasus : au cœur d'une enquête mondiale sur l'espionnage de téléphones**

Dès les attentats de 2015, on a constaté l'utilisation par Daech de ce chiffrement, qui rend inopérants les systèmes d'écoute judiciaire « classiques ». D'où le développement, par des Etats, d'outils qui peuvent être indispensables dans la lutte contre le terrorisme, mais dont l'usage a été totalement dévoyé par certains pays afin de surveiller des opposants, des journalistes et des hommes politiques, français entre autres. C'est précisément un tel dévoiement qui s'est produit dans la commercialisation mondiale, par NSO, de Pegasus, outil développé initialement par Israël pour lutter contre le terrorisme.

Mais, face à cette menace, on constate que de nombreux Etats, notamment les Européens, n'ont pas développé ce type d'outils que de nouvelles vagues terroristes pourraient rendre indispensables. Dans ce contexte, il serait de l'intérêt national et européen que la France maîtrise ce type de technologies. D'abord pour pouvoir les détecter et les neutraliser, et, si une menace terroriste majeure le nécessitait, pour les utiliser à cette seule finalité, de façon très encadrée.

Piller nos secrets industriels

Il est également essentiel que l'Union européenne (UE) réagisse à un aspect révélateur du scandale Pegasus : le gouvernement israélien a officieusement communiqué sur le fait d'avoir obligé NSO à bloquer tout usage de son logiciel contre les téléphones à préfixe international en + 1 (Etats-Unis) ; il est même avancé, sur les forums spécialisés, que les préfixes en + 7 (Russie) et + 86 (Chine) bénéficieraient aussi de cette mansuétude, qui protège donc de toute intrusion les citoyens de la première puissance mondiale et probablement ceux de ses deux challengers autoritaires, dotés de puissantes capacités cyberoffensives.

Lire aussi | **« Projet Pegasus » : comment la société israélienne NSO Group a révolutionné l'espionnage**

L'UE devrait immédiatement réagir en exigeant du gouvernement israélien qu'il enjoigne à NSO de bloquer toute utilisation de Pegasus sur des portables européens, sauf sur demande judiciaire d'un Etat membre. Parallèlement, l'Europe devrait adopter une directive étendant le champ du RGPD *[règlement général sur la protection des données]* à toute captation non judiciairement autorisée de données d'un portable européen, avec de lourdes pénalités financières pour les entités responsables ou complices de ces vols.

Le directeur général de l'Anssi *[Agence nationale de la sécurité des systèmes d'information]*, Guillaume Poupard, a lancé, mercredi 21 juillet, une importante alerte en désignant implicitement, par la mention d'APT31, pour la première fois, le pays responsable : la Chine. C'est une grave campagne d'espionnage contre les entreprises françaises destinée à piller nos secrets industriels. Notre pays et surtout l'Europe doivent réagir très fermement face à cet espionnage massif, accepter la notion de rapport de force et oser enfin des rétorsions au-delà de l'emblématique, et si pratique, Huawei.

Lire la tribune : « Huawei est une arme stratégique de l'Etat chinois pour réprimer les Ouïgours »

Dans les neuf dernières semaines précédant l'affaire Pegasus, le monde avait déjà assisté à une série d'annonces publiques dans le domaine cyber qui laisse pantois : attaque par un rançongiciel paralysant partiellement la distribution de carburants aux Etats-Unis ; prises de position martiales du président Biden parlant de mesures de rétorsion ; disparition autoproclamée d'un premier groupe de

pirates ; saisie d'une rançon par le FBI ; sommet Biden-Poutine en grande partie focalisé sur le cyber ; attaque majeure affectant un millier de PME dans le monde et provoquant une conversation Biden-Poutine ; disparition d'un deuxième groupe de pirates et, enfin, fermeture temporaire du site du ministère russe de la défense, officiellement victime d'une attaque par déni de service *[visant à perturber ou à paralyser le fonctionnement d'un serveur informatique]*.

Encore ne s'agit-il que de ce qui est public…

Pression américaine

Au début de cette année, nous avons proposé une mobilisation stratégique fondée sur quatre volets : renseignement, protection, action sur les pays abritant les auteurs de ces méfaits et riposte directe. Sans doute, le président Macron a annoncé, le 18 février, un plan national de cybersécurité doté d'un milliard d'euros ; le président américain a signé, le 12 mai, un *executive order [décret présidentiel]* ambitieux. Mais il s'agit de mesures intérieures, qui ne traitent pas le facteur crucial : la quasi-impunité dont jouissent les maîtres d'œuvre de ces attaques criminelles.

Le 16 juin, Joe Biden a annoncé un tournant majeur à l'issue de sa rencontre avec Vladimir Poutine : seize types d'infrastructures critiques seraient désormais *« off limits »*. Toute cyberattaque contre ces infrastructures provoquerait une riposte « sur le mode cyber ».

De fait, le 14 mai, le groupe de cybercriminels DarkSide a admis avoir cessé ses activités « sous la pression américaine » : tous ses sites étaient bloqués. Le 14 juin, le ministère de la justice américaine a fait saisir, par le FBI, la majeure partie de la rançon payée par Colonial Pipeline *[la firme avait versé 4,4 millions de dollars aux pirates informatiques qui avaient paralysé un réseau d'oléoducs sur la Côte est des Etats-Unis]*.

Lire aussi | **Face aux rançongiciels, les Etats-Unis fortifient leur réponse judiciaire**

L'attaque d'envergure par rançongiciel du 3 juillet, à partir d'une vulnérabilité du logiciel de supervision Kaseya, a donné à voir la réponse russe. Elle a permis au groupe de *ransomware* russe REvil d'infecter plus d'un millier d'entreprises dans le monde. Le président Biden s'en est entretenu, dès le 9 juillet, avec le président Poutine, lui demandant fermement de mettre fin aux activités de REvil. Le 13 juillet, l'ensemble des sites de REvil a disparu subitement. Que ce soit le résultat d'une cyberattaque américaine ou d'une suppression spontanée ou imposée par les services russes, il est indéniable que la stratégie de riposte commence à avoir un impact significatif.

La France et ses partenaires de l'UE doivent impérativement tenir compte de cette nouvelle donne stratégique.

En juin, en Europe, Joe Biden a explicité que la réponse cyber face à une attaque sur les infrastructures critiques serait américaine, même si les Etats-Unis préviendraient leurs alliés. Une telle concertation portera essentiellement sur le renseignement mais n'impliquera pas une extension du parapluie cyber aux alliés.

Les groupes cybercriminels tireront logiquement les conséquences de ce nouveau contexte en réduisant leurs opérations contre les Etats-Unis et en intensifiant, en contrepartie, leurs raids dans la riche Union européenne qui, pas plus que ses Etats membres, n'applique de doctrine de riposte effective même si elle en discute.

La France se trouve donc confrontée à une problématique rappelant celle qui amena le général de Gaulle à décider le développement d'une capacité nationale et autonome de dissuasion nucléaire tous azimuts.

Elaborer une doctrine stratégique

Aujourd'hui, notre pays subit une cyberguérilla permanente et croissante, se manifestant par des attaques de type rançongiciel, des vols de données, de surveillance type Pegasus ou par

prépositionnement, dans les infrastructures critiques, de maliciels *[logiciels malveillants]* activables à distance.

Ces actes restent toujours sous le seuil des hostilités caractérisées, tel que défini par le traité de l'Atlantique Nord. Les Etats se contentent de subir et de réparer. Ainsi de l'attaque qui a visé l'opérateur belge Belnet *[un service public qui assure l'accès à Internet de plusieurs institutions]*, paralysant pendant plusieurs jours différentes structures publiques, dont le Parlement wallon, quelques heures avant un débat sur la situation des Ouïgours ; ou de celle, également avec le rançongiciel d'origine russe, qui a fortement perturbé le système de santé irlandais en mai.

La France possède le potentiel scientifique, industriel et opérationnel pour répondre au défi que constitue la confrontation, dès le temps de paix, dans le cyberespace.

Lire notre enquête sur le business du « ransomware » : Comment les cybercriminels revendent leurs lucratifs rançongiciels

Il est indispensable, pour y parvenir, d'élaborer d'abord une doctrine stratégique, qui affirme que notre pays ripostera, y compris par des moyens cyber, à toute attaque contre les systèmes d'information des infrastructures publiques ou privées qu'il juge essentielles, quels que soient leurs auteurs, étatiques ou criminels. La mise en œuvre de cette doctrine devra s'appuyer sur un effort prioritaire de renseignement permettant de renforcer ses capacités nationales d'attribution, comme elle a su le faire en matière d'observation spatiale.

Cela complétera le plan national de renforcement de la cybersécurité par la mise en place d'un programme d'innovation technique et scientifique, d'une ampleur identique aux programmes qui nous ont permis d'atteindre l'autonomie stratégique nucléaire. Tout aussi indispensable, une coordination cyber devrait être créée au niveau du chef de l'Etat, chef des armées, dans le respect des structures opérationnelles existantes.

Dotée d'une telle doctrine et organisation, appuyée sur une volonté de mise en œuvre effective et des moyens, la France pourra coopérer de façon équilibrée avec ses alliés et développer des partenariats spécifiques avec ceux de ses partenaires ne désirant plus subir l'escalade des cyberagressions. Et pourra, bien sûr, rendre plus franc et respectueux le nécessaire dialogue avec les autres acteurs majeurs de la confrontation cyber, à commencer par la Russie et la Chine, mais aussi ceux qui abritent ou utilisent ces autres cybercorsaires que sont les sociétés vendant, sans aucune restriction, des logiciels de surveillance personnelle.

¶ **Bernard Barbier** est ancien directeur technique de la DGSE (direction générale de la sécurité extérieure) ; **Jean-Louis Gergorin** est ancien chef du Centre d'analyse et de prévision du Quai d'Orsay ; **l'amiral Edouard Guillaud** est ancien chef d'état-major des armées.

Collectif