« Il faut se demander si la France peut continuer à se passer d'une forte coordination stratégique de la cybersécurité auprès du président »

Face aux attaques numériques qui se multiplient contre les Etats, Bernard Barbier, Jean-Louis Gergorin et Edouard Guillaud, tous trois spécialistes en défense nationale, encouragent, dans une tribune au « Monde », à une réflexion commune pour sortir l'Europe de son impuissance stratégique en matière cyber.

Par **Bernard Barbier** (ancien directeur technique de la DGSE) , **Jean-Louis Gergorin** (ancien chef du Centre d'analyse et de prévision du Quai d'Orsay) et **Edouard Guillaud** (ancien chef d'état-major des armées)

Tribune. En juillet 2021, nous avons analysé les faiblesses de l'Europe face aux cyberagressions et proposé des axes de réponse. Depuis, le contexte stratégique dans le cyberespace a empiré, principalement au détriment de l'Union européenne et de ses membres.

Pour l'essentiel, cela tient à un renforcement du duopole Etats-Unis - Russie, mis en évidence dans l'affaire ukrainienne comme dans le domaine cyber : en septembre, les groupes DarkSide et REvil, responsables d'attaques rançongicielles majeures puis sabordés sous pression américaine et par les autorités russes, ont ressuscité (DarkSide devenant BlackMatter) et repris leurs attaques. La réaction américaine est la mise en œuvre de la doctrine Biden, énoncée après le sommet organisé avec Vladimir Poutine, en juin, à Genève : les responsables d'attaques contre des infrastructures critiques américaines devront être neutralisés par les autorités russes, ou à défaut par les capacités propres des Etats-Unis. De fait, le 21 octobre, trois jours après une attaque paralysant un réseau de télévision, les différents sites de REvil font l'objet de cyberattaques massives destructrices, provoquant le désarroi profond de ses cadres s'exprimant sur le Web. Quelques heures plus tard, une dépêche de *[l'agence de presse britannique]* Reuters explique que cette neutralisation technique a été menée conjointement par le US Cyber Command, le FBI et le Secret Service.

Lire aussi la tribune publiée le 26 juillet 2021 : « L'affaire Pegasus montre parfaitement les faiblesses de l'Europe en matière de cyberagressions »

Le message est entendu : le 1er novembre, BlackMatter, dénoncé pour ses attaques rançongicielles par l'Agence fédérale américaine de cybersécurité, annonce qu'il met fin à toutes ses activités *« sous pression des autorités »,* puis disparaît. Le lendemain, William Burns, directeur de la CIA, a des conversations à Moscou avec le secrétaire du Conseil de sécurité russe et avec son homologue, chef du SVR. Il aura en outre un échange téléphonique avec Vladimir Poutine. Les points à l'ordre du jour sont l'Ukraine et… la cybersécurité. Il ne fait aucun doute qu'après l'élimination américaine du groupe REvil, les dirigeants russes ont préféré prendre les devants en ordonnant à BlackMatter de disparaître.

Un écosystème basé en Russie

Pendant tout l'automne, le général Nakasone, qui dirige simultanément l'Agence nationale de la sécurité (NSA) et le Cyber Command, multiplie les interventions publiques sur les rançongiciels. Depuis le milieu de l'année 2021, ses services considèrent que de telles attaques sont des atteintes à la sécurité nationale qui légitiment l'emploi de cybermoyens offensifs pour les *« dissuader et les entraver ».* Au même moment, la Russie, par le biais de ses clubs de réflexion et un article paru le 29 septembre dans **la revue [[le quotidien ?]]]]** *Kommersant,* se félicite de cette nouvelle coopération avec les Etats-Unis contre la cybercriminalité.

De fait, les Etats-Unis ont mis fin à un étrange aveuglement occidental devant une réalité connue de tous les cyberspécialistes : la majorité des attaques par rançongiciels est le fait d'un écosystème cybercriminel, surveillé par les services russes et constitué de groupes organisés basés à Moscou tels feu REvil ou Conti, à Saint-Pétersbourg.

Lire aussi : Un homme soupçonné d'appartenir au groupe cybercriminel REvil identifié par les enquêteurs

De son côté, le Royaume-Uni a reconnu l'enjeu de sécurité nationale représenté par le cybercrime organisé dans le rapport « National Cyber Strategy 2022 » *[« Cyberstratégie nationale 2022 »]* publié par le gouvernement en décembre. Ce document complet expose une ambitieuse stratégie couvrant un écosystème innovant : résilience, sécurité, capacités offensives, lutte contre la cybercriminalité, avec une forte coordination au niveau du premier

ministre et l'objectif de faire du Royaume-Uni une *« leading cyber power » [« une cyberpuissance de premier plan »].*

La création de la National Cyber Force en est un axe fort, avec pour mission essentielle de détecter, offensivement entraver et dissuader les cyberattaques, qu'elles soient étatiques ou criminelles.

Les membres de l'Union européenne (UE) ont, dans le cadre national comme européen, une vision différente, avant tout fondée sur la cyberrésilience : la protection contre les attaques et la récupération après celles-ci, et une contre-attaque policière et judiciaire censée être dissuasive. Des opérations brillantes ont eu lieu, mais la proportion de cybercriminels arrêtés, jugés et condamnés est très faible. Les concepteurs des rançongiciels sont à l'abri en Russie, en Biélorussie, en Corée du Nord et désormais en Chine.

La résilience est une condition nécessaire mais non suffisante de la sécurité numérique. La croissance continue des rançongiciels frappant la France, pourtant championne au sein de l'UE par l'excellence de son agence de cybersécurité (Anssi), l'illustre : de fin 2020 à fin 2021, le nombre de rançongiciels déclarés sur le dispositif Cybermalveillance est passé de 46 à 107 pour les collectivités et de 298 à 496 pour les entreprises.

Des mesures de cyberrésilience peu dissuasives

Les agressions contre les Anglo-Saxons se traduisant par des ripostes fortes et efficaces, il sera plus tentant pour les attaquants de réorienter les attaques vers la riche Europe. A cette réalité quasi commerciale s'ajoute un risque stratégique. Selon des informations circulant à Washington, la Russie aurait fait savoir qu'en cas de fortes sanctions économiques euro-américaines suivant une opération en Ukraine, sa riposte serait cyber, notamment vers l'UE. Elle aurait l'embarras du choix, entre l'activation de maliciels prépositionnés dans des infrastructures et une amplification des attaques rançongicielles de ses groupes cybercriminels, qui joueraient le rôle de corsaires des temps modernes.

Lire aussi : Les options limitées des Etats-Unis face aux manœuvres de la Russie à la frontière avec l'Ukraine

Les annonces publiques prévues dans le cadre de la présidence française du Conseil de l'Union européenne sont utiles et positives pour le renforcement de la cyberrésilience, mais elles ne sont en rien dissuasives.

Cette présidence donne une occasion unique à la France de réagir face à un contexte profondément changé depuis la « Revue stratégique de cyberdéfense » publiée en février 2018, en annonçant désormais que les prépositionnements de maliciels dans les infrastructures critiques et les attaques rançongicielles devront entraîner des ripostes sur les entités commettant ces agressions. Nul doute qu'une telle doctrine, énoncée publiquement et appliquée, élèvera la qualité du cyberdialogue tant avec les Etats-Unis qu'avec la Russie.

Cette initiative devra s'accompagner du lancement d'une nouvelle « revue stratégique » couvrant l'écosystème de la cybersécurité, la résilience et les opérations défensives et offensives. Enfin, il faudra aussi se demander si, contrairement aux Etats-Unis, au Royaume-Uni, à la Russie, à la Chine et à Israël, la France peut continuer à se passer d'une forte coordination stratégique de la cybersécurité auprès du président, chef des armées.

Lire aussi : Fini les illusions de l'après-guerre froide : le retour de « l'ennemi », nouvelle réalité pour la France

En parallèle, la présidence française pourrait prendre deux initiatives : susciter une réflexion commune sur la prévention du blanchiment des rançons en cryptomonnaies et provoquer une coopération renforcée entre les pays européens techniquement et militairement compétents sur le recueil de renseignement à des fins d'attribution et d'action contre les groupes cybercriminels. L'enjeu pour l'Europe est la sécurité de ses entreprises et de ses collectivités et le refus d'être prise en étau par le duopole russo-américain et ainsi d'en devenir le champ d'affrontement.

Bernard Barbier est un ancien directeur technique de la DGSE, ancien directeur du Laboratoire d'électronique et de technologies de l'information (LETI) et membre de l'Académie des technologies ; **Jean-Louis Gergorin,** chargé de cours à Sciences Po, est un ancien chef du Centre d'analyse et de prévision du Quai d'Orsay ; **Edouard Guillaud** est amiral, ancien chef d'état-major des armées