OPINIONS • DÉFENSE

« Qu'elles soient étatiques ou criminelles, les intrusions informatiques doivent être combattues par une stratégie nationale et globale »

TRIBUNE

Bernard Barbier
Ancien directeur technique de la DGSE

Jean-Louis Gergorin
Ancien chef du Centre d'analyse et de prévision du Quai d'Orsay

Amiral Edouard Guillaud
Ancien chef d'état-major des armées

La « cybercoercition » implique de combiner renseignement, protection, action internationale et capacité de riposte, soulignent, dans une tribune au « Monde », trois anciens hauts responsables de la défense française.

Publié aujourd'hui à 06h30 | Lecture 5 min.

Tribune. Au début de l'année 2020, dans un monde qui n'imaginait pas encore à quel point la pandémie de Covid-19 le déstabiliserait, nous alertions sur l'ensemble des menaces cyber et appelions à la réflexion comme à l'action face à ce que nous avons baptisé la « cybercoercition » : toute intrusion informatique visant à intimider les dirigeants d'un Etat ou d'une entreprise pour obtenir des avantages politico-stratégiques dans un cas, une rançon financière dans l'autre.

La lettre ouverte du Club informatique des grandes entreprises françaises (Cigref), le 18 novembre 2020, au premier ministre, Jean Castex, est un cri d'alarme des entreprises. Le nombre de cyberattaques réussies, notamment par des rançongiciels *(« ransomware »)* bloquant le système informatique d'une entreprise jusqu'au paiement d'une rançon, a encore quadruplé en un an.

Les attaques sont de plus en plus sophistiquées et visent entreprises et services publics. Elles proviennent en quasi-totalité d'un écosystème criminel qui s'est développé dans des pays n'ayant pas ratifié la Convention de Budapest sur la cybercriminalité (2001).

Activité criminelle rentable

En toute impunité, de puissants groupes pratiquent aussi bien la cyberextorsion directe que la vente à tout acheteur criminel des outils techniques permettant celle-ci : *« ransomware as a service »*. La tolérance intéressée des services officiels des Etats les abritant et l'importance de leurs gains font de

la cyberpiraterie l'activité criminelle la plus rentable et la moins risquée de l'histoire humaine, ce qui explique sa croissance exponentielle.

La pénétration, révélée en décembre 2020, des systèmes informatiques d'un millier d'entités publiques et privées américaines, dont la totalité des grands ministères, la NSA, Microsoft et la très performante société de cybersécurité FireEye, constitue une véritable *« rupture stratégique »*. Il s'agit de la modification non détectée d'une mise à jour d'un logiciel de gestion de réseaux. L'ajout d'un « cheval de Troie », nommé « Sunburst », de mars à mai, a permis de prépositionner au cœur des systèmes les plus critiques un implant, qui, à ce jour, ne paraît avoir été utilisé qu'à des fins d'espionnage. Il aurait pu tout aussi bien être un vecteur de sabotage.

Lire aussi | **Panique et incertitude aux Etats-Unis après une sévère opération d'espionnage informatique**

Jusqu'à la découverte récente et l'identification précise de Sunburst, l'Etat qui l'a créé – la Russie, selon la quasi-totalité des responsables officiels américains sauf Donald Trump – a disposé d'une *« capacité de première frappe numérique »* contre des infrastructures civiles et militaires critiques des Etats-Unis. Sunburst n'a été décelé que lorsque ses commanditaires ont volé les outils techniques offensifs de FireEye. Il est probable que cette capacité d'insérer un cheval de Troie indétectable dans une mise à jour de logiciel soit déjà exploitée ailleurs. La menace est donc critique.

Un plan de lutte en quatre volets

Dans ce contexte, la cybercoercition, qu'elle soit étatique ou criminelle, doit être combattue par une stratégie nationale d'anticoercition intégrée et globale. Celle-ci comporterait quatre volets étroitement liés : renseignement, protection, action internationale et capacité de riposte.

Le renseignement doit identifier les responsables des attaques et les signatures techniques de celles-ci. Pour ce faire, la coopération entre services de renseignement officiels, agences de cybersécurité et entreprises spécialisées de confiance est primordiale.

La protection est une condition nécessaire mais non suffisante de la sécurité. A cet égard, l'attaque Sunburst est une alerte majeure sur la nécessité de ne plus s'en remettre aux seules certifications initiales des logiciels. Des mécanismes de contrôle des mises à jour doivent être instaurés. Enfin, il est anormal que la France, exportatrice de cerveaux numériques, n'arrive pas à mieux stimuler la création et le développement d'entreprises de logiciels de cybersécurité, mettant fin au duopole américano-israélien dominant le marché européen.

L'action internationale doit non seulement viser à réguler le cyberespace dans la suite de l'appel de Paris du président Macron, le 12 novembre 2018 *[discours d'inauguration de l'Internet Governance Forum, à l'Unesco],* mais aussi utiliser tous les moyens bilatéraux et multilatéraux pour inciter les Etats auteurs ou protecteurs de cyberattaques à changer de comportement. Les sanctions individuelles ne sont que l'un des outils, à l'efficacité limitée ; le poids commercial de l'Union européenne offre des perspectives importantes.

« Des objectifs ambitieux et atteignables doivent être fixés. Vouloir éradiquer la cybercriminalité est illusoire ; la réduire est à notre portée »

Enfin, la doctrine française de cyberdéfense doit prévoir la possibilité de riposte proportionnée à toute attaque contre des infrastructures jugées essentielles aussi bien civiles que militaires. Sous l'impulsion de Thierry Breton *[commissaire européen au marché intérieur],* la Commission européenne vient d'annoncer de façon significative une nouvelle stratégie de cybersécurité.

Pour lutter au bon niveau, des objectifs ambitieux et atteignables doivent être fixés. Vouloir éradiquer la cybercriminalité est illusoire ; la réduire est à notre portée. La lutte cyber pourrait s'inspirer de l'opération Atalante contre la piraterie menée dans l'océan Indien depuis 2008, qui a vu l'Union européenne s'appuyer sur un premier pays, la France en l'espèce, pour allier rapidité et efficacité.

Les ripostes d'anticoercition pourraient être effectuées par le ComCyber *[commandement interarmées de la lutte informatique, mis en place en 2017]* ou la direction générale de la sécurité extérieure (DGSE), ou par une équipe intégrée commune, comme en Grande-Bretagne, à l'échelon national ou en coopération avec des alliés. Sans l'évolution doctrinale déjà évoquée sur le caractère global de la cyberdéfense, il n'y aura aucun effet dissuasif et rien n'empêchera la répétition de plus en plus grave de ce que le CHU de Rouen a subi en novembre 2019, lorsqu'il a été frappé par une cyberattaque massive.

Lire aussi | **L'armée française va établir sa doctrine cyber-offensive**

Face aux ruptures que représentent la croissance exponentielle des rançongiciels et l'opération « Sunburst », notre pays doit très rapidement engager une réflexion stratégique et sortir de la logique incrémentale qui n'est plus adaptée au contexte. Plus que jamais, il nous paraît indispensable que le président de la République puisse s'appuyer sur un coordonnateur national cyber (CNC), à l'instar du coordinateur national du renseignement de lutte contre le terrorisme (CNRLT), qui a montré son efficacité.

Bernard Barbier, ancien directeur technique de la DGSE. Ancien directeur du Laboratoire d'électronique et de technologies de l'information (LETI), il est membre de l'Académie des technologies ; **Jean-Louis Gergorin,** chargé de cours à Sciences Po. Ancien chef du Centre d'analyse et de prévision du Quai d'Orsay, il est coauteur de « *Cyber. La guerre permanente* » (Les éditions du cerf, 2018) ; **Amiral Edouard Guillaud,** ancien chef d'état-major des armées.