TRIBUNE

Hack back : une cyber légitime défense ?

Francis Teitgen, avocat au Barreau de Paris, Teitgen & Viottolo, ancien Bâtonnier de l'Ordre
et **Nicolas Ludmann**, Managing Partner, ALCEE

Les entreprises conduisent actuellement des transformations digitales à marche forcée afin de rester compétitives. Néanmoins, en exposant progressivement à Internet leurs processus critiques, elles deviennent de plus en plus vulnérables aux cyber-attaques qui se multiplient et peuvent aller jusqu'à remettre en cause leur survie. Les dirigeants se retrouvent ainsi confrontés à un dilemme.

Cette situation est d'autant plus préoccupante que les stratégies défensives de cybersécurité, malgré des budgets conséquents et en augmentation constante, affichent leurs limites face à des attaques évoluées menées par des organisations criminelles ou des concurrents mal intentionnés. Elles ressemblent de plus en plus à des lignes Maginot numériques, sans efficacité avérée, accumulant des moyens importants dans des zones convenues. Dans ce contexte, les services de l'État, et notamment l'ANSSI, affichent un discours ambigu : d'un côté ils s'opposent fermement à l'adoption de stratégies offensives de cybersécurité également appelées hack back ; de l'autre, ils concentrent leurs actions sur les seules infrastructures vitales nationales et renoncent, de fait, à défendre les autres secteurs d'activité.

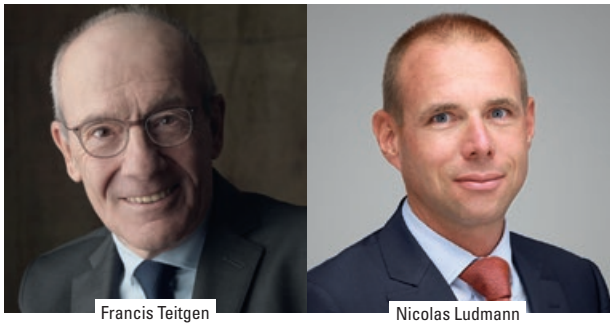
CETTE POSITION EST INTENABLE

Il en va d'autant plus ainsi qu'aux États Unis, l'*Active Cyber Defense Certainty Act* pourrait être voté lors de la prochaine session 2019-2020. La situation serait ainsi définitivement clarifiée pour les entreprises américaines. Et plus critique alors pour les entreprises européennes.

Un changement de paradigme de cybersécurité intégrant le *hack back* nous paraît dès lors non seulement inévitable mais encore souhaitable et le plan d'action associé évident :

1. augmenter ses capacités de détection des intrusions ;
2. identifier de manière certaine ses agresseurs ;
3. neutraliser leurs attaques en portant le combat numérique sur leur territoire.

Un tel positionnement, délibérément affiché et assumé, pourrait atténuer l'exposition aux risques des entreprises et leur permettrait de déployer plus sereinement leurs innovations digitales. Néanmoins, une question fondamentale se pose : de telles actions de *hack back* sont-elles légales ? Une entreprise privée ne peut pas, *proprio motu*, répondre de manière agressive à une cyber-attaque. Cette affirmation s'évince du principe selon lequel nul ne saurait s'immiscer dans le système d'information d'autrui sans l'accord de ce dernier.



Francis Teitgen — Nicolas Ludmann

CETTE RÉPONSE N'EST PAS SATISFAISANTE

En cas d'agression, une personne en état de légitime défense peut répliquer à son agresseur sous réserve que le moyen employé soit proportionné à l'attaque dont elle est victime et qu'aucune autre riposte n'était raisonnablement envisageable. Dans de telles circonstances même la commission d'une infraction pénale n'est pas punie car elle est légitimée à raison des circonstances. De la même manière, la légitime défense de l'entreprise doit pouvoir être mise en œuvre en cas de cyber-attaque. Les opposants à ce principe évoquent notamment le risque d'abus de riposte par une prétendue victime qui ne s'emploierait pas sérieusement à identifier son agresseur et, adoptant une position belliqueuse, s'introduirait frauduleusement dans le système d'information par exemple de son concurrent. Il nous semble que cet argument est sans pertinence. On ne saurait prohiber l'exercice d'un droit pour l'unique raison que d'autres bénéficiaires de ce dernier pourraient en abuser. Il faut à la fois assurer la défense des entreprises victimes tout en préservant l'inviolabilité des systèmes d'information. Le respect des principes essentiels suivants pourrait permettre d'atteindre ce but :

- en premier lieu, l'entreprise attaquée doit utiliser un *modus operandi* structuré pour identifier son agresseur et elle devra le démontrer en cas de contestation ;
- en deuxième lieu, elle devra toujours riposter de manière proportionnée et être capable de rapporter la preuve du respect de ce principe dans l'hypothèse d'une critique du *hack back* qu'elle aura mis en œuvre ;
- enfin, il lui reviendra d'établir la gravité de la tentative d'attaque dont elle a été la victime et de la mise en péril de ses intérêts fondamentaux.

Que les entreprises françaises se défendent en respectant ces principes ! ■