Cybersécurité : la « stratégie du sabre laser » au cœur de la guerre commerciale entre la Chine et les États-Unis

Thierry Berthier
Chaire de cybersécurité & cyberdéfense Saint-Cyr, Thales, Sogeti

Juin 2019 – Article III.30

Depuis le début de son mandat, le président américain Donald Trump a choisi de protéger, quel qu'en soit le prix, la technologie et la propriété intellectuelle américaine face aux ambitions chinoises. Il a pour cela engagé un bras de fer économique et diplomatique avec son homologue chinois Xi Jinping sur fond de tensions géostratégiques croissantes, notamment en mer de Chine.

L'augmentation des droits de douane sur certains produits chinois et le contrôle accru des transferts de technologies sensibles vers la Chine ont provoqué des contre-mesures de Pékin, de même nature, sur les produits américains. La boucle systémique de l'escalade des sanctions est lancée sans que l'on sache jusqu'où elle nous mènera. L'imbrication des intérêts technologiques, numériques, industriels et militaires des deux superpuissances contribue clairement à la crispation générale dans un contexte propice à l'instabilité et aux turbulences des marchés.

Les différends portent essentiellement sur la téléphonie, les processeurs et les réseaux, des technologies essentielles dans le cadre de la montée en puissance commerciale de l'intelligence artificielle. Enjeux de ces passes d'armes : l'image de marque, la crédibilité des plates-formes, des produits ou des services.

Mais quelles pourraient être les armes mises en œuvre pour en découdre ? Si l'on se réfère aux cultures stratégiques chinoises et américaines, le sabre laser ferait consensus, de Star Wars, aux guerriers Mandarins de Sun Tzu. Une fois l'arme choisie par les duellistes, quelles forces placeront-ils dans leur sabre laser ? L'influence, la ruse, la déception et le discrédit lancé sur l'adversaire sans le combattre frontalement, dans la pure tradition de Sun Tzu et son *Art de la guerre*.

Le temps des duels

Les premiers duels économicostratégiques sino-américains opposant des grands acteurs de l'intelligence artificielle et de la simulation numérique ont débuté en 2015 avec l'embargo américain interdisant l'exportation vers la Chine de certains processeurs utilisés pour le calcul haute performance (HPC). Le secrétariat américain au Commerce avait refusé à la société Intel les licences d'export vers la Chine pour ses processeurs Xeon et Xeon Phi. On notera que cet embargo a été particulièrement contre-productif puisqu'il a eu pour effet principal de relancer la filière chinoise des microprocesseurs, d'accélérer le développement de processeurs HPC et de briser cette dépendance stratégique.

D'autres duels se sont succédé, toujours autour de défauts de sécurité (réels ou prétendus), de vulnérabilités prouvées ou non des systèmes, solutions, plates-formes ou produits développés et commercialisés par l'adversaire. Cette tendance à exploiter systématiquement l'argument de cybersécurité pour décrédibiliser et dévaloriser l'offre technologique du concurrent, de l'adversaire ou de l'ennemi, s'est installée à pas feutrés il y a trois ans. Elle devient beaucoup plus visible et bruyante aujourd'hui.

Avec l'arrivée de la 5G, le secteur de la téléphonie connaît des turbulences qui opposent de grands acteurs chinois et américains. C'est notamment le cas dans l'affaire Huawei qui fait l'objet d'accusations de fraudes, de vol de technologies et d'espionnage de la part du gouvernement américain. L'équipementier télécom chinois vient d'être exclu des contrats de fourniture des réseaux 5G de plusieurs pays européens à la suite de suspicions de défaut de sécurité affectant ses produits, même si cette mise à l'écart devrait se traduire par un coût supplémentaire estimé à 55 milliards d'euros.

La campagne américaine visant le géant Huawei s'est d'ailleurs aussi focalisée sur l'Europe afin de freiner des ambitions de développement sur le vieux continent concurrençant frontalement les intérêts américains. Cette affaire s'inscrit clairement dans un contexte de tensions économiques croissantes sur fond de sécurité nationale et de soupçons de liens unissant Huawei aux services de renseignement chinois.

Du côté chinois, les mêmes règles du jeu ont été validées. Ainsi, le laboratoire Keenlab de la société Tencent (le T de BATX) vient de publier un rapport de recherche très complet prouvant l'insécurité *by design* (lors de la conception) des composants de machine learning équipant les véhicules Tesla. Ce rapport, qui fait suite à une série de communications réalisées durant la conférence de cybersécurité BlackHat 2018, est particulièrement destructeur pour l'image de marque de Tesla à l'heure où les concurrents chinois montent en puissance et ne cachent plus leurs ambitions de conquête du marché européen.

Selon les tests réalisés par les ingénieurs de Tencent, la Tesla présente certains dysfonctionnements.

L'argument de sécurité est ainsi utilisé comme un sabre laser neutralisant la réputation d'un grand acteur industriel et tranchant la confiance du consommateur dans les produits qu'il commercialise. La « stratégie du sabre laser » fondée sur l'argument de sécurité ne fait que reprendre l'un des préceptes de « l'Art de la guerre » de Sun Tzu :

« Sans donner des batailles, un habile général sait l'art d'humilier ses ennemis ; sans répandre une goutte de sang, sans tirer même l'épée, il vient à bout de prendre les villes ; sans mettre les pieds dans les royaumes étrangers, il trouve le moyen de les conquérir ; et sans perdre un temps considérable à la tête de ses troupes, il procure une gloire immortelle au prince qu'il sert, il assure le bonheur de ses compatriotes, et fait que l'univers lui est redevable du repos et de la paix : tel est le but auquel tous ceux qui commandent les armées doivent tendre sans cesse et sans jamais se décourager. »

Ce cas Tencent – Tesla est l'un des premiers exemples de duel « compagnie chinoise *vs*. compagnie américaine ». Les confrontations de ce type vont s'intensifier sous l'effet de la montée en puissance des capacités chinoises en matière d'intelligence artificielle. Les technologies françaises et européennes ne seront pas épargnées. Bien au contraire, les deux compétiteurs principaux auront tout intérêt à affaiblir un troisième joueur (russe ou européen) qui viendrait troubler le duel bipolaire.
La France et l'Europe doivent donc s'entraîner et se préparer aux stratégies du sabre laser en créant des plates-formes d'intelligence artificielles sécurisées *by design*, prouvées, robustes, résilientes, irréprochables. Chez les technologies françaises, les mésaventures de type Tchapou Idemia ne doivent plus se reproduire car elles discréditent l'ensemble de la filière et provoquent un coup de sabre laser réflexe immédiat de nos amis américains…

Nous devons par ailleurs accepter le duel en testant systématiquement la sécurité des produits américains et chinois que nous adoptons. En cas de faille de sécurité avérée, nous devrons faire parler le sabre sans trembler, comme le conseille Sun Tzu.