La cybercriminalité constitue-t-elle une

Par Menhaouara Mourad*

Oui et sans le moindre doute. Tel est le message qu'ont voulu nous transmettre, à juste titre, les experts qui ont eu le mérite d'organiser dernièrement un colloque international autour de cette problématique.

A les écouter, personne parmi les dirigeants d'entreprises et d'organismes publics ne peut et ne doit ignorer ce risque et faire comme si cette menace ne le concerne pas. J'appuie totalement cette mise en garde, non seulement pour les risques que cette forme de criminalité fait peser sur le capital informationnel et immatériel de nos entreprises, mais bien au-delà, c'est-à-dire pour des enjeux hautement stratégiques touchant à notre souveraineté nationale. En même temps, je ne suis pas certain que nos dirigeants soient suffisamment conscients du danger auquel ils sont exposés pour qu'ils consentent à réagir et prendre les mesures idoines visant à anticiper ces menaces par la mise en place d'une politique de prévention et de protection. Le prétexte de l'absence quasi générale de l'utilisation des NTIC dans le fonctionnement des organisations institutionnelles, des entreprises, est souvent mis en avant par certains dirigeants et autres opérateurs économiques pour dire finalement qu'ils ne sont pas concernés. Et d'ajouter : «Même si cela arrive, on sait quoi faire ! Ou bien, la situation est sous contrôle et nous avons pris les mesures qu'il faut.» Ce type de réaction traduit en fait un déficit systémique qui est celui du culte de l'infaillibilité (ou du syndrome dit du *Titanic*). Pour ces dirigeants sûrs d'eux, le retour de manivelle leur sera fatal s'ils ne se départissent pas de leurs fausses certitudes. Certes, l'usage des TIC n'est pas encore cet outil technologique auquel nos entreprises ont recours pour fonctionner, communiquer et traiter l'information. Pour autant, comme toute entreprise de par le monde, il faut peut-être leur rappeler que pour assurer leur développement et évoluer, elles doivent, pour ce faire, conquérir des marchés, faire face à la concurrence et se protéger. Cela ne peut se faire qu'en s'ouvrant au monde. Autrement dit, pour faire court, nos dirigeants, pour innover, se différencier par rapport à la concurrence et transformer rapidement l'information en connaissance, doivent intégrer la dimension de l'intelligence économique comme valeur ajoutée dans le fonctionnement de leur organisation, à défaut, c'est la mort assurée de l'entreprise. Car l'entreprise compétitive de demain devra nécessairement passer par une gestion globale des données et des connaissances qui l'entourent et maîtriser le processus de création d'intelligence favorable à son développement. Dès lors, il serait temps pour nos chefs d'entreprise de s'affranchir de cette autarcie qui caractérise leur environnement, et ce, comme de véritables managers, en se connectant au monde et en s'imprégnant des modes de fonctionnement de gestion performants générés, entre autres, par les NTIC pour être à la fois offensifs, mais aussi et surtout pour se protéger par une veille stratégique de l'impitoyable lutte qui s'opère au niveau planétaire sur le plan économique. Le faible degré d'occurrence et de gravité des actes générés par la cybercriminalité en Algérie, que certains experts ont évoqués tout en les relativisant comme pour les atténuer, ne doit pas nous conduire à baisser la garde. Si les actes de malveillance résultant de cette forme de criminalité ne sont pas significatifs aujourd'hui, il est quasi certain que l'Algérie aura à connaître des cyberattaques de grande ampleur aux conséquences désastreuses. Quand ? Où ? Nul ne peut le dire sauf l'ennemi virtuel qui peut choisir sa cible et au moment du passage à l'acte. En revanche, ce qui est certain à l'échelle de l'Etat, en tant que garant de la souveraineté nationale, c'est le fait qu'au fur et à mesure que l'Algérie développe ses infrastructures de base par l'introduction de nouveaux outils de management (gestion informatisée de l'AEP, du trafic ferroviaire, aéroportuaire, de l'alimentation en gaz et en électricité…), ces systèmes seront de plus en plus vulnérables et, par voie de conséquence, exposés à des attaques informatiques. D'où l'impérieuse nécessité de mettre en place dès à présent des dispositifs de protection pour accroître la résilience de ces infrastructures des plus sensibles. Donc, il faut se préparer au pire et agir en conséquence maintenant !En Europe, les Etats membres de l'Union, conscients des risques terroristes, de sabotage et des cyberattaques, ont décidé de renforcer la sûreté des installations considérées comme vitales pour la nation. Au niveau communautaire, une directive sur la désignation et la protection des infrastructures critiques européennes (ICE) a été adoptée le 8 décembre 2008. Selon cette directive, l'ICE est définie comme «un point, système ou partie de celui-ci… indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif dans un Etat membre du fait de la défaillance de ces fonctions». Cette directive définit un cadre d'amélioration de la sûreté des infrastructures transnationales. L'enjeu pour les pays de l'UE est d'éviter les failles de sûreté et de bâtir une résilience à l'échelle européenne. Au plan national, l'Allemagne est à l'avant-garde en matière de prévention de la cybercriminalité depuis l'ouverture le 16 juin 2011 du cyber-Abswehrzentrum qui constitue le premier centre de cyberdéfense destiné à la protection des infrastructures vitales (réseaux, eau et électricité). En France, aux termes du décret du 23-02-06, des secteurs d'activité d'importance vitale (SAIV) sont répertoriés et au sein desquels sont regroupés des opérateurs qui devront mettre en place des dispositifs de protection spécifiques en vue de prémunir ces AIV de tout dommage, indisponibilité ou destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme, qui risquerait d'altérer gravement la sécurité ou la capacité de survie de la nation, ou de mettre en péril la santé ou la vie de la population. En Suisse et en Belgique, même prise de conscience des pouvoirs publics qui ont mis en place des stratégies de protection des infrastructures critiques.

Le faible degré d'occurrence et de gravité des actes générés par la cybercriminalité en Algérie, que certains experts ont évoqués tout en les relativisant comme pour les atténuer, ne doit pas nous conduire à baisser la garde. Si les actes de malveillances résultant de cette forme de criminalité ne sont pas significatifs aujourd'hui, il est quasi certain que l'Algérie aura à connaître des cyberattaques de grande ampleur aux conséquences désastreuses.

Quid de l'Algérie ?

Si de tels dispositifs existent, il serait utile que les pouvoirs publics en fassent état et de les porter à la connaissance du citoyen de manière à susciter son adhésion, et bien plus encore, son implication en tant qu'acteur dans la défense des intérêts vitaux de l'Algérie.

Dans le cas contraire, les pouvoirs publics ont tout intérêt à réagir sans plus tarder avant qu'ils ne soient confrontés à une situation de black-out d'un secteur sensible avec des conséquences dommageables pour le pays.

Il ne s'agit pas de jouer ici les cassandres ou de faire état de quelque chose qui relève du fantasme. Les exemples sont légion autour de nous, et chaque jour que Dieu fait, les médias en font leur une. Plus près de nous, l'affaire de l'espionnage des agents de la puissante NSA, révélée par un transfuge de cette organisation, a suscité une crise majeure entre les Etats-Unis et plusieurs pays victimes des ces actes de malveillance.

Outre le prélèvement illégal d'informations dites fermées, des actions de sabotage pourraient être commises au moyen d'un malware qui détecte une faille pour s'introduire dans un réseau d'un système sensible. Le cas du virus Stuxnet en est la parfaite illustration en matière de cyberattaque, dont l'Iran en a été la cible et au moyen duquel des experts américains avaient tenté de bloquer ses centrifugeuses afin d'affaiblir ses capacités d'enrichissement de l'uranium.

Le cas de l'Etat de l'Estonie, victime d'un déni de service (DOS), a assisté impuissant à une paralysie de son appareil administratif, de ses banques…, suite à une attaque qualifiée de cyberguerre avec des ennemis invisibles non identifiés. Nous pourrions citer les attaques de type APT (Advanced Persistent Threat) qui sont commanditées avec des objectifs précis tels que le contrôle d'un système d'une organisation et en extraire le contenu d'une information sensible et la vendre ensuite. L'affaire la plus retentissante signalée dans cette catégorie de cybercriminalité, c'est le programme NITRO visant 48 entreprises britanniques, japonaises, italiennes des secteurs de la défense, de la chimie, de l'automobile, qui avait été commandé à des fins d'espionnage pour capter des informations sensibles (secrets de fabrication).

Le cas de l'Etat de l'Estonie, victime d'un déni de service (DOS), a assisté impuissant à une paralysie de son appareil administratif, de ses banques…, suite à une attaque qualifiée de cyberguerre avec des ennemis invisibles, non identifiés.

En Algérie, souvenons-nous de cette affaire d'avions de combat MIG équipés de logiciels espions, découverts grâce à la vigilance des services du ministère de la Défense nationale et retournés depuis à la Russie. La liste pourrait être longue si les organisations, notamment les banques et certaines entreprises victimes de ces agissements, acceptent de les révéler. Ce qui n'est pas toujours le cas, préférant garder le mutisme de crainte de voir leur image et leur réputation écornées.

En 2011, selon Symantec, 1,8 million de menaces apparaissent chaque jour.

Il ne s'agit pas de focaliser exclusivement sur les menaces dirigées contre les entreprises en pointant du doigt de petits ha0ckers dans leur chambre ou à partir d'un cybercafé qui viendraient perturber leurs activités. Cette image d'un hacker isolé est désormais révolue. Aujourd'hui, ce sont de véritables réseaux de criminalité organisée qui agissent pour le compte d'entreprises ou d'Etats. Nous sommes face à des groupes d'experts qui se revendiquent du «cyberhacktivisme» se livrant à une véritable cyberguerre. De ce qui précède et sans exagération, on peut s'attendre à la mise à l'arrêt d'un équipement grand public (centrale électrique par exemple) réalisé clés en main par un groupe étranger. Il suffit pour cela de l'introduction d'une bombe logique dans le process qui sera activée le moment opportun. Ce cas de figure peut parfaitement se produire suite à un acte de vengeance ou de chantage. Cela est déjà arrivé en d'autres lieux. C'est aussi le risque inhérent à cette imprudence de nos décideurs à vouloir confier les projets de réalisation de l'ensemble de nos infrastructures sensibles au savoir-faire étranger ou bien à importer tous azimuts des équipements, notamment électroniques, avec une confiance aveugle, sans couverture juridique garantissant ces risques, non prévue au moment de la rédaction du contrat.

Dans le même ordre d'idées et s'agissant des menaces potentielles dirigées contre l'Algérie, il n'y a pas seulement que la cybercriminalité qui doit nous inquiéter. Malheureusement, d'autres risques «criminels» se manifestent au quotidien de manière insidieuse et qui causent d'énormes préjudices à l'économie algérienne. Sans vouloir verser dans une espèce de paranoïa, il faut savoir que l'Algérie, qui jouit d'une aisance financière, suscite des convoitises sans limite de la part de groupes d'affairistes étrangers prédateurs, lesquels, menacés d'une faillite en raison d'un carnet de commandes vide par ces temps de crise, se ruent sur l'Algérie par instinct de survie dans le but d'accaparer des parts de marché sans contrepartie et non, comme ont tendance à le croire naïvement certains responsables, par un regain d'intérêt pour l'Algérie.

En matière de guerre économique, l'objectif pour une entreprise est d'être conquérante et de réaliser le maximum de profits sans état d'âme. Pour ce faire, leur Etat de rattachement se charge de leur fournir les informations stratégiques dont elles ont besoin par tous les moyens. L'espionnage et la malveillance sont utilisés à cette fin, afin d'être en position avantageuse pour accaparer des marchés à l'international.

- En 1994 déjà, le directeur de la CIA avait pris l'engagement que l'espionnage économique allait désormais être la préoccupation majeure des services de renseignement américains.

- Du temps où Bill Clinton était président, ce dernier avait déclaré qu'un milliard de dollars d'exportations générerait 40 000 emplois (la fin justifie les moyens !).

- Dans le magazine *Courrier cadres* de décembre 2008, il est fait mention de la nécessité pour les entreprises françaises d'être agressives et d'aller en ces temps de crise chercher les contrats avec les dents, voire piquer les secrets des concurrents en se servant, le cas échéant, d'outils nécessaires à cet effet (caméra «bouton», ceinture caméra et autres attirails sophistiqués dignes des films de James Bond).

Dans cette guerre économique mondiale, l'Algérie n'est pas épargnée. Tous les moyens sont permis pour accaparer une partie de son trésor.

Parmi ces stratagèmes, je citerai le piège de l'élicitation.

Terme anglais qui pourrait se définir par l'art de faire parler les gens par la flatterie, la valorisation, le partage d'intérêts communs. Cette méthode est employée à l'occasion des foires et salons professionnels, séminaires, colloques, cocktails.