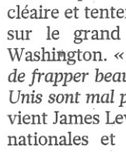
La cyberguerre mondiale a déjà commencé

Attaques tous azimuts contre les entreprises et les États, course aux armements : un nouveau champ de bataille émerge sur les réseaux informatiques où pourraient se jouer les guerres du futur et où les terroristes sont parfois en position de force.



ISABELLE LASSERRE
ilasserre@lefigaro.fr

« *Un beau matin, les hommes découvriront avec surprise que des objets aimables et pacifiques ont acquis des propriétés offensives et meurtrières.* » Lorsqu'ils écrivaient ces lignes dans *La Guerre hors limites*, en 1999, les colonels chinois Qiao Liang et Wang Xiangsui imaginaient-ils que l'informatique deviendrait l'une des armes les plus prisées du XXIe siècle ?

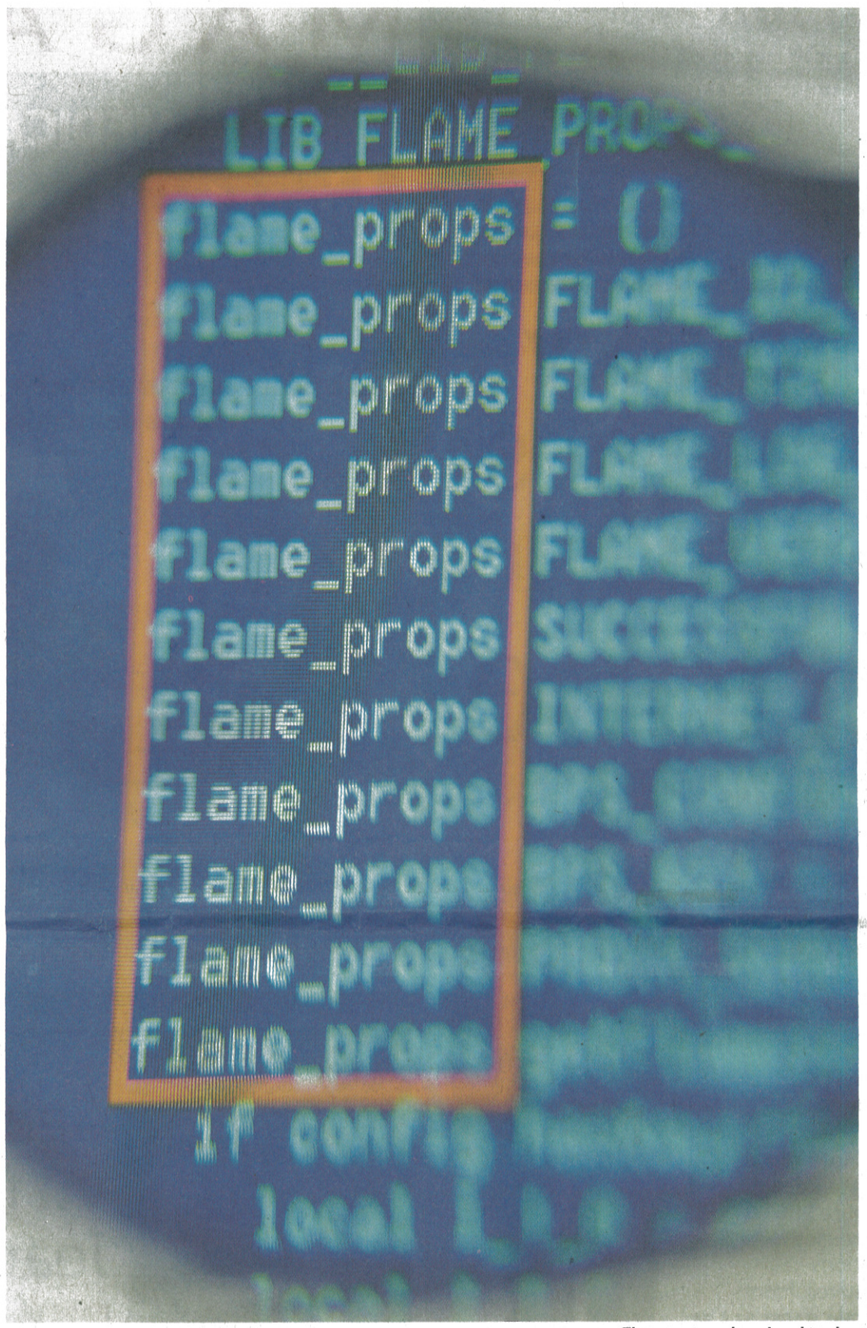
La cyberguerre est déclarée. Le réseau global est devenu un lieu de confrontation militaire majeur. Rapide et inatteignable comme un nuage, la morsure guerrière d'Internet glisse le long des conflits et s'infiltre dans tous les points chauds du globe. La dernière fois qu'elle a fait parler d'elle, c'était en août dernier, dans les entrailles d'Aramco, la compagnie nationale pétrolière d'Arabie saoudite, et de RasGas, une entreprise qatarienne, toutes deux visées par un virus baptisé « Shamoon ». L'acte de sabotage, revendiqué par un « Groupe de la jeunesse arabe » mécontent des liens entretenus par la famille régnante saoudite avec les États-Unis, a entraîné la destruction de 30 000 ordinateurs d'Aramco. Selon le secrétaire américain à la Défense, Leon Panetta, il s'agit « *probablement de l'attaque la plus destructrice que le secteur privé ait jamais vécu* ». La gigantesque entreprise a mis un mois à récupérer ses facultés. Elle a dû revenir au fax pendant plusieurs semaines !

Mais ce n'est pas tout : depuis la fin du mois de septembre, six grandes banques américaines sont attaquées par un groupe se référant au prêcheur musulman antisioniste des années 1920 et 1930 Izz ad-Din al-Qassam. L'« opération Ababil » s'est fixé pour but le retrait de la Toile du film à scandale *L'Innocence des musulmans*. Le site d'une des principales banques françaises aurait été atteint à la mi-octobre par le même virus. Dans le domaine de la cyberguerre, une étape nouvelle a été franchie. « *C'est la première fois qu'un signal politique à visée stratégique est diffusé dans cette région du Golfe* », explique l'amiral Arnaud Coustillière, responsable de la cyberdéfense à l'état-major des armées, lors d'une réunion du cercle Strategia.

Un risque de « cyber-Pearl Harbour »

Aux États-Unis, certains ont vu la main de l'Iran dans ces dernières attaques. La République islamique aurait pris pour cible l'industrie saoudienne et les institutions financières américaines pour se venger des attaques menées contre son programme nucléaire et tenter de prendre la main, dans la région, sur le grand rival sunnite saoudien, allié de Washington. « *L'Iran a découvert un nouveau moyen de frapper beaucoup plus tôt que prévu et les États-Unis sont mal préparés pour répondre à cela* », prévient James Lewis, au Centre pour les études internationales et stratégiques (CSIS), l'un des plus grands experts de la question.

La réponse du berger à la bergère ? En 2010, un ver malfaisant extrêmement puissant baptisé Stuxnet, introduit dans le programme nucléaire iranien par une simple clé USB, avait détruit un cinquième au moins des centrifugeuses iraniennes, ralentissant d'un an environ la marche de la République islamique vers la bombe atomique. Issu du programme américain de cyberattaque « Olympic Games », Stuxnet, comme ses petits frères Flame et Duqu, était porteur d'une mission stratégique : remplacer les frappes militaires préventives envisagées par Israël pour empêcher l'Iran de se doter de l'arme atomique. Acheter du temps, en quelque sorte, afin de permettre aux sanctions internationales imposées à l'Iran de faire effet.



Flame est un des virus les plus sophistiqués jamais imaginés. Il peut se propager via le réseau ou une clé USB. Véritable espion, il est capable de dérober tout type de données et même d'enregistrer les conversations qui ont lieu autour de l'ordinateur infesté.
PRNEWSFOTO/NORMAN ASA

Avec Stuxnet, le domaine de la cyberguerre, jusque-là souvent limité à des actions d'espionnage, a pris un tournant. « *Il semble que l'on ait franchi le Rubicon* », estime Patrick Pailloux, le directeur de l'Anssi, l'Agence nationale de la sécurité des systèmes d'information. Stuxnet est « *la première attaque majeure de cette nature ayant entraîné des destructions physiques affectant une infrastructure importante* », a affirmé Michael Haydn, ancien patron de la CIA. Depuis, la guerre de l'ombre fait rage entre l'Iran, les États-Unis et Israël. Dernier rebondissement, le laboratoire spécialisé russe Kaspersky vient de détecter un nouveau virus, Mini Flame, dans des ordinateurs en Iran et au Liban. « *Un outil chirurgical d'attaque de grande précision, conçu pour voler des données et pénétrer les systèmes infectés* ».

Certes, en matière de cyberoffensives à visées stratégiques, il y avait eu des précédents. En avril 2007, la petite Estonie, sans doute le pays le plus dématérialisé du monde, dont 98 % des transactions bancaires s'effectuent en ligne, fut entièrement paralysée par des « *dénis de service* », une saturation des sites de ses médias, banques et institutions gouvernementales. L'ancien occupant russe a tout de suite été montré du doigt. Moscou aurait réagi à la décision de Tallinn de déboulonner la statue d'un soldat soviétique au cœur de la capitale. Ce fut la première cyberguerre de grande ampleur. Quelques mois plus tard, en octobre 2007, un virus israélien s'attaqua aux systèmes de défense sol-air de la Syrie, rendant la défense antiaérienne de ce pays inopérante et permettant ainsi aux chasseurs de Tsahal de bombarder le réacteur nucléaire d'al-Kibar. En août 2008, l'invasion de l'Ossétie du Sud par les chars russes, en Géorgie, fut précédée par des attaques coordonnées menées contre les sites du gouvernement et des principaux médias. Une sorte de préparation psychologique à la guerre visant à déstabiliser le président Mickaël Saakachvili, dont le portrait fut remplacé, sur certains sites, par celui d'Adolf Hitler.

En quelques années, la cyberguerre est devenue « *une arme stratégique, qui pèse dans les conflits. Les actions se développent tous azimuts. Nous entrons dans une nouvelle ère* », explique l'amiral Coustillière. Aux États-Unis, le chef du Pentagone, Leon Panetta, estime qu'il existe désormais un risque de « *cyber-Pearl Harbor* ». Le cyberespace, prévient-il, est « *le champ de bataille du futur* ».

La guerre en réseau se substituera-t-elle un jour aux modes d'action militaires traditionnels ? Les virus deviendront-ils aussi efficaces que les bombardements aériens ou les raids des forces spéciales ? On n'en est pas encore là. Mais ce qui est certain, c'est que tout le monde s'y met. La Chine a créé un nouveau corps d'armée dédié au cyber, au sein duquel travaillent 9 600 hommes. La Russie a depuis longtemps investi ce champ prometteur. En 2011, l'Iran a conçu un « cybercorps » destiné à répondre aux attaques menées en 2010 contre son usine de Natanz. « *Les militaires iraniens sont prêts à battre nos ennemis dans le cyberespace* », a prévenu son chef, le général Gholamreza Jalali. L'Iran s'est aussi fait une spécialité de l'achat des capacités offensives sur le marché, confie un spécialiste du dossier. C'est désormais la course aux armements. « *De nombreux pays développent ou songent à développer des capacités. Ce qui n'est pas très rassurant* », explique Patrick Pailloux à l'Anssi.

100 ingénieurs et « hackers » suffisent

Arme très asymétrique, comme le furent par exemple les IED, les engins explosifs improvisés des insurgés en Afghanistan, l'attaque informatique se concentre sur les maillons faibles de ses cibles. Elle est accessible aux groupes terroristes et aux États faillis. « *Le ticket d'entrée n'est pas cher et il est particulièrement facile d'acquérir une capacité offensive dans ce domaine* », confirme un spécialiste. Il suffit généralement d'une centaine de bons ingénieurs et de *hackers*. Certes, une attaque aussi sophistiquée que Stuxnet ne peut pas avoir été conçue par le premier venu : elle requiert beaucoup de renseignements et implique forcément la participation d'un État. « *Une action cyber menée contre un pays suppose aussi, généralement, un contexte international tendu, car c'est un effet stratégique qui est recherché* », précise l'amiral Coustillière.

Plus facile et moins onéreuse que le long chemin qui mène à la bombe atomique, la cyberattaque offre en outre davantage de discrétion, les actions pouvant être, grâce à l'abolition des frontières induite par Internet, facilement cachées. Contrairement à la guerre conventionnelle, les pays les plus développés, entièrement informatisés, sont ici les plus vulnérables.

Mais les groupes terroristes et les États non démocratiques ne sont pas les seuls à avoir investi le versant offensif du cyber-champ. Ayant indirectement reconnu être à l'origine du premier virus ayant visé l'Iran, les États-Unis et Israël s'inquiètent désormais des capacités de riposte de leurs adversaires. Les autorités américaines redoutent que des attaques informatiques fragilisent les systèmes d'armes et atteignent les capacités opérationnelles de leurs armées. En 2011, un virus introduit dans une base aérienne du Nevada a réussi à infecter les postes de contrôle des drones déployés en Afghanistan...

Les « lacunes » de la France

Le Pentagone, comme Tsahal, a depuis longtemps développé des capacités destinées à contrer les menaces. Au sein du « Cyber Command » sont testées, dans le plus grand secret, de nouvelles recettes de cyberattaques. En 2010, les États-Unis ont reconnu avoir mené des cyberopérations contre les insurgés en Afghanistan. Ils ont depuis prévenu qu'ils pourraient utiliser leur programme d'attaque pour mener des frappes préventives sur Internet s'ils estimaient que la sécurité de leur pays était menacée ou si des raids informatiques étaient menés contre le gouvernement, l'armée ou l'économie.

Rien de tel pour l'instant en France. Dans un rapport écrit pour le Sénat, l'ancien ministre Jean-Marie Bockel estime que « *l'ampleur de la menace* » comme son caractère stratégique ont été « *largement sous-estimés* » dans le livre blanc de 2008, qui a pourtant créé l'Anssi. Alors que les attaques contre les grandes entreprises publiques et les institutions, y compris l'Élysée, Areva et le ministère de l'Économie, se comptent par dizaines, la France affiche de nombreuses « *lacunes* » dans son dispositif de défense. Quant au domaine offensif, il reste complètement tabou. « *Ce blocage intellectuel entraîne un repli sur soi. Il favorise la fuite des cerveaux et prive le pays d'une réflexion doctrinale* », regrette un expert. Certains en sont persuadés : dans les batailles futures, la supériorité informatique d'une nation pourrait bien déterminer, dans certains cas, l'issue des affrontements armés. « *Une stratégie purement défensive reviendrait à construire une ligne Maginot du XXIe siècle* », prévient Michel Baud, officier de l'armée de terre, dans *Politique étrangère*. ■

« L'Iran a découvert un nouveau moyen de frapper beaucoup plus tôt que prévu et les États-Unis sont mal préparés pour répondre à cela »
JAMES LEWIS, DU CENTRE POUR LES ÉTUDES INTERNATIONALES ET STRATÉGIQUES