Les Echos

Avons-nous encore les moyens de notre cybersécurité ?

LE POINT DE VUE DE NICOLAS ARPAGIAN

François Hollande a constitué une commission du Livre blanc chargée de lui remettre à la fin de cette année une feuille de route sur les questions de défense et de sécurité nationales qui concernent l'avenir de notre pays. A l'heure où la protection de nos intérêts stratégiques ne relève plus de nos seules forces armées, et que les budgets de celles-ci sont minorés sans cesse, il convient de prendre en compte les armes numériques qui disposent d'un champ d'intervention inégalé.

Depuis quelques mois, les illustrations d'actions informatiques offensives ne manquent pas : qu'il s'agisse de pénétrer les ordinateurs de l'Elysée, de naviguer dans l'informatique d'Areva durant de longues semaines ou de retarder le programme nucléaire iranien par des cyberattaques ciblées. Autant de cas où la distinction entre les sphères civiles et militaires n'a pas plus réellement de raison d'être. Un changement d'ère que les industriels de la défense ont rapidement intégré, notamment en raison des constantes révisions à la baisse des budgets alloués à leur activité par les différents gouvernements. C'est ainsi par exemple qu'au printemps 2012 le Salon Eurosatory, grand'messe traditionnelle de l'armement terrestre, a dédié une journée entière à la cybersécurité. Ou que le géant EADS voit dans sa nouvelle filiale Cassidian spécialisée en matière de sécurité numérique des opportunités de croissance. Idem pour Thales. Or aujourd'hui, sur les cinq acteurs de la cybersécurité réalisant plus d'un milliard de dollars de chiffre d'affaires, tous sont états-uniens. Le ministère américain de l'Intérieur (DHS) dépense chaque année quelque 3 milliards de dollars en recherche & développement en la matière. Et presque 8 milliards de dollars annuels pour le seul ministère américain de la Défense. Dans le même temps, les acteurs européens les plus importants font 200 à 300 millions de dollars de chiffre d'affaires, avec en outre des standards techniques différents.

Sur les cinq acteurs de la cybersécurité réalisant plus de 1 milliard de dollars de chiffre d'affaires, tous sont états-uniens.

En période de disette économique, les entreprises auront-elles les ressources pour investir dans ce secteur et pourront-elles attendre les retombées de ces investissements de long terme ? D'autant plus qu'en matière numérique, l'agresseur est toujours avantagé : vous pouvez avoir bâti une citadelle a priori imprenable, il reste toujours la possibilité par des opérations d'ingénierie sociale bien menées (usurpation d'identités, découverte de mots de passe, envoi de pièces jointes dûment contaminées…) de contourner les structures informatiques les plus robustes. Ici , ce n'est pas l'épaisseur du blindage qui fait la différence. Mais bien l'intelligence mise dans l'organisation et dans sa capacité à faire évoluer celle-ci en permanence.

Pour donner toutes ses chances à cet écosystème si particulier, l'Etat doit donc en assimiler les spécificités et ne surtout pas chercher à plaquer dessus son mode d'organisation. Qui est par essence figé, pyramidal et univoque. Alors que la logique cybernétique est déconcentrée, évolutive et interactive. La commission du Livre blanc saura-t-elle adopter cette approche pour suggérer des pistes d'actions opérationnelles qui pourront bénéficier sans délai à ce tissu économique en devenir ? Il faut le souhaiter, car notre autonomie future en matière de cybersécurité en dépend. Et donc à très brève échéance, notre souveraineté.

Nicolas Arpagian est directeur scientifique du cycle « Sécurité numérique » de l'Institut national des Hautes Etudes de la Sécurité et de la Justice (INHESJ). Et auteur de « La Cybersécurité » (PUF).