



CARTE BLANCHE À...

La cyberinsécurité devient une réalité avec Wikileaks

NICOLAS ARPAGIAN, directeur scientifique du cycle Sécurité numérique à l'Institut national des hautes études de la sécurité et de la justice (INHESJ) et auteur de *La Cybersécurité* (chez PUF), livre ses réflexions sur l'affaire Wikileaks.

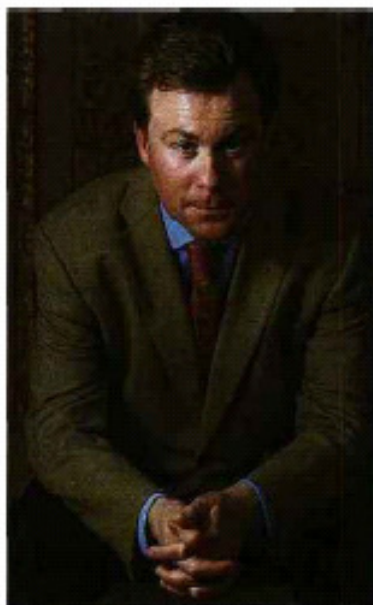
Le mode de transmission des télégrammes diplomatiques français va être révisé. C'est une des conséquences de l'explosion politico-médiatique qui a agité les chancelleries du monde entier avec la publication, par le site Wikileaks, de documents internes à l'Administration états-unienne.

Classiquement dans l'univers de la sécurité, c'est un événement marquant qui conduit à revoir les usages et les modes de travail qui prévalaient jusqu'alors. Avec la mise à disposition sur la Toile de telles quantités de mémorandums confidentiels et autres correspondances réservées, on dispose d'un cas exemplaire d'atteinte à la sécurité numérique. Toutes les composantes sont en effet réunies : un seul individu, en l'espèce peu gradé mais au contact d'informations sensibles, a pu collecter une très grande quantité de données. En les copiant sur de simples CD-Rom sur son lieu de travail.

L'information, un actif à protéger par des technologies adaptées

S'il n'avait pas choisi de rendre ces éléments publics, leur copie serait passée inaperçue. Faute de précautions techniques permettant de suivre l'usage qu'il est fait de données stockées, celles-ci peuvent être dupliquées sans que son légitime propriétaire en soit alerté. Il faudra se décider à admettre que l'information constitue un actif à part entière. Qui mérite donc d'être protégé de manière appropriée.

La transmission en mode crypté pose aussi la question de la fiabilité des solutions de codage et de leurs modalités d'emploi par des intérêts privés (particuliers, militants, entreprises...). Gages de liberté d'expression pour les uns, ces



CHRISTOPHE DUPONT/ELGE

« Wikileaks ? Transparence pour certains, atteinte à la confidentialité pour d'autres »

solutions sont aussi de véritables boucliers numériques. Une réflexion sur l'usage de ces outils de haute confidentialité par un nombre croissant d'utilisateurs est donc indispensable.

L'annonce faite par Amazon de cesser d'héberger Wikileaks, puis celles de Paypal ou de Mastercard d'interrompre les versements à son profit montrent bien que les acteurs privés sont partie prenante de la cybersécurité. Car ces opérateurs sont en mesure de rendre accessibles ou non les informations collectées. Cela illustre, en outre, le caractère international du cloud computing, qui permet de stocker les données dans des structures disséminées, les rendant davantage hors d'atteinte de ceux qui souhaiteraient les pirater.

L'affaire Wikileaks révèle aussi les disparités juridiques qui perdurent sur le net entre les différents pays. Ces derniers ne s'accordent pas entre eux sur le trai-

tement qu'il faut accorder à l'exposition de tels documents. Opportunité de transparence démocratique pour les uns, atteinte majeure à la confidentialité des travaux diplomatiques pour les autres.

Des données pourtant obscures sans un décryptage journalistique

L'émergence d'une économie d'opinion est également significative, Wikileaks annonçant être financé par des dons de personnes physiques. Elle démontre aussi que la mobilisation pécuniaire de quelques-uns peut favoriser l'émission et la diffusion d'informations à l'échelle planétaire, sans structure commerciale ni campagnes publicitaires préalables.

Le clivage apparu avec la mise en ligne des télégrammes du département d'Etat est aussi intéressant à observer. D'un côté, les tenants du secret le présentent comme la condition indispensable à la réussite des négociations intergouvernementales. De l'autre, les partisans de la transparence se réjouissent de cette mise à nu institutionnelle. Il s'agit sans doute d'une version étatique du « conflit » qui oppose les inconditionnels du site Facebook et ses détracteurs. Autrement dit, entre ceux qui estiment que la notion de vie privée est obsolète et ceux qui en font un bien sacré qu'il convient de préserver.

Enfin, le choix de Wikileaks de s'associer à des médias bien établis pour accompagner la mise en ligne de ses documents renforce l'idée que le traitement de l'information reste un métier à part entière. L'expérience nous a appris qu'il ne suffit pas de rendre disponible des matériaux bruts pour que l'opinion s'en saisisse et sache les décrypter. Il faut un travail préalable de vérification, d'explication et de présentation qui exige du temps et des compétences.

Autant de pistes de réflexion qui font de Wikileaks un cas d'école salutaire pour poser le débat de la cybersécurité, lequel concerne aussi bien les individus que les entreprises et les Etats. ■

NICOLAS ARPAGIAN