NSA : dernières révélations, elle sait déjouer les communications chiffrées

La NSA a mis en place un programme consacré à la lutte contre les techniques de chiffrement, le plus grand obstacle à son "accès sans restriction au cyberespace".

Selon le *Guardian,* le *New York Times* et le site Internet Propublica, la NSA et son allié britannique, le Government Communications Headquarters (GHCQ) ont développé plusieurs méthodes pour contourner les méthodes de chiffrement censées protéger la confidentialité des données qui circulent sur le Web. Des techniques qui, selon le *Guardian*, "compromettent largement les garanties avancées par les entreprises d'Internet sur la protection des informations de leurs utilisateurs".

La diffusion de cette information n'a visiblement pas plu aux Etats-Unis. Le renseignement américain a expressément demandé aux trois organes de presse de ne pas la diffuser, au risque que des "cibles étrangères" n'adoptent de nouvelles formes de chiffrement qui seraient plus difficiles à contourner. Selon les documents rendus publics par Edward Snowden, la NSA a mis en place depuis une dizaine d'années "Bullrun", un programme consacré à la lutte contre les techniques de chiffrement des communications, qu'elle considère comme le plus grand obstacle à son "accès sans restriction au cyberespace".

Bullrun aurait conduit en 2010 à une grande percée technologique, permettant à la NSA de rendre "exploitables de vastes quantités de données" interceptées grâce à des écoutes de câbles Internet. Le GCHQ aurait, de son côté, réussi à déchiffrer le trafic de Hotmail, Google, Yahoo! et Facebook à l'aide d'un programme similaire, baptisé "Edgehill". Des documents font également état d'un accès, dès cette année, aux données d'un "opérateur majeur des télécommunications" ainsi que d'un "service de communications de pair à pair de premier plan". Une description qui pourrait bien correspondre au programme Skype.

Selon le *Guardian*, l'agence américaine consacre 190 millions d'euros par an pour travailler avec les entreprises technologiques pour "influencer secrètement" sur la conception de leurs produits. L'objectif est d'insérer dans les systèmes de chiffrement des vulnérabilités, ou "back doors", que la NSA pourra ensuite exploiter pour espionner les données. L'agence américaine influerait également sur les standards mondiaux de chiffrement pour les détourner à son avantage. La NSA considère les techniques de déchiffrement comme vitales pour mener à bien ses missions d'antiterrorisme et de renseignement extérieur.