

Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: 151 (2006)
Heft: 5

Artikel: Comment les terroristes communiquent : mythes et réalités
Autor: Cécile, Jean-Jacques
DOI: <https://doi.org/10.5169/seals-346600>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 11.01.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

Comment les terroristes communiquent : mythes et réalités

S'agissant des moyens de communication utilisés par les terroristes, il importe de dissiper certains mythes. Le premier d'entre eux concerne la stéganographie, qui consiste à noyer une information dans la masse d'une autre et qui permet, en théorie, de véhiculer discrètement des données.

■ **Jean-Jacques Cécile**¹

Malgré ce qu'ont prétendu certains médias américains, les terroristes ayant perpétré les attentats du 11 septembre 2001 n'ont pas, de l'aveu même du FBI, utilisé la stéganographie. Quelques jours avant l'attaque, une équipe de scientifiques appartenant au *Center for Information Technology Integration* de l'University of Michigan a, de manière fortuite, passé au crible deux millions d'images extraites d'Internet avec de puissants logiciels spécialisés ; pas un seul message caché par stéganographie n'a été découvert. D'autres organismes ont également fait chou blanc, par exemple le *Center for Secure Information Systems* de la *George Mason University* dont les travaux étaient, en février 2001, financés par la *National Security Agency (NSA)*.

De même, l'utilisation du logiciel de cryptage *Pretty Good Privacy* par les terroristes apparaît être un mythe. Le FBI affirme que les pirates de l'air du 11 septembre 2001 n'ont pas crypté leurs messages. Du reste, le niveau de sécurité induit par l'utilisation de *PGP* est tout re-

latif : *Pretty Good Plaisanterie* ne résisterait pas aux ordinateurs de la *NSA*. Le logiciel comprendrait des « erreurs » de programmation facilitant le décryptage et des liens peuvent être établis entre la société possédant les droits d'exploitation de *PGP* et la *National Security Agency*.

Troisième mythe : selon le *Washington Post*, Ben Laden aurait eu ses entrées au sein d'une compagnie de télécommunications satellitaires contrôlée par un membre de sa famille, ce qui lui aurait en particulier permis de contourner les écoutes américaines. Une enquête rapide du quotidien britannique *The Guardian* a montré que la société n'existait pas.

Comme souvent, la réalité est plus triviale ! Pourquoi les terroristes se compliqueraient-ils la vie, alors qu'il existe des moyens simples et éprouvés ? Il est de notoriété publique que l'un des principaux problèmes rencontrés au quotidien par la *NSA* concerne la surabondance d'informations à exploiter. En conséquence, un message codé anodin envoyé à une banale *chat room* a plus de chances de passer inaperçu qu'un message

crypté. Les terroristes ayant planifié et exécuté les attentats du 11 septembre ont donc utilisé des méthodes à la fois plus simples et plus furtives :

– Messageries grand public (adresse e-mail de Zacarias Moussaoui : pilotz123@hotmail.com).

– Messages codés (substitution d'un mot par un autre selon des règles définies par avance et connues des seuls expéditeur et destinataire).

– Agents de liaison (femmes, enfants) transportant physiquement des supports informatiques (disquettes).

Si l'on sort du contexte limité aux attentats du 11 septembre 2001, on constate que la simplicité reste de mise ainsi que le démontrent les méthodes qui ont été effectivement utilisées :

– Déport d'un émetteur (un téléphone mobile est mis en œuvre par un subalterne à une distance de deux kilomètres de l'autorité, l'acheminement des messages entre les deux s'effectuant par estafette).

– Utilisation de plusieurs téléphones mobiles pour transmettre un message par bribes.

¹ Directeur de recherche au Centre français de recherche sur le renseignement (www.cf2r.org)

S'agissant des messages codés, les exemples suivants peuvent être relevés :

- Le mot arabe «hadutta» (comptine pour enfants) a camouflé le mot «explosifs».

- Les substances biologiques ou chimiques ont parfois été désignées par le mot «al zabadi» (lait caillé).

- Le régime des taliban et al-Qaeda sont respectivement devenus «Omar & Brothers Company» et «Abdullah Contracting Company».

L'utilisation de ces messages codés anodins est encore plus efficace, dès lors que des tactiques élémentaires de guerre de l'information sont parallèlement mises en œuvre. Pendant l'été ayant précédé le 11 septembre 2001, les services de renseignement américains ont intercepté une trentaine de mes-

sages émanant d'opérationnels ou de sympathisants d'al-Qaeda et faisant référence à des événements imminents. La plupart étaient des fausses alertes. Fin octobre 2001, sur une période de dix jours, de nombreux messages ont été envoyés en Afghanistan, notamment depuis le Canada; ils ont provoqué une alerte fédérale aux Etats-Unis, mais rien ne se passa.

Plus généralement, il est évident que la langue arabe constitue une certaine forme de codage systématisé élémentaire.

Selon des chiffres rendus publics, les services du *Federal Bureau of Investigation* spécialisés en matière de traduction employaient 900 linguistes en septembre 2001; il y en avait 1200 en septembre 2004. Pour l'année fiscale 2001, 21 millions de dollars de services en

matière de traduction ont été budgétisés; ce chiffre s'élevait à 70 millions pour l'année fiscale 2004. Pourtant, au sein du *Federal Bureau of Investigation* :

- En septembre 2004, 24% des communications interceptées étaient stockées sans être traduites.

- En avril 2004, 123 000 heures d'enregistrements étaient en souffrance en matière de contre-terrorisme et 370 000 en matière de contre-espionnage. Ces pourcentages représentaient globalement 30% des interceptions audio.

- Suite à des problèmes rencontrés en matière de stockage des enregistrements, certains d'entre eux sont parfois effacés avant même d'avoir au moins été succinctement exploités.

J.-J. C.