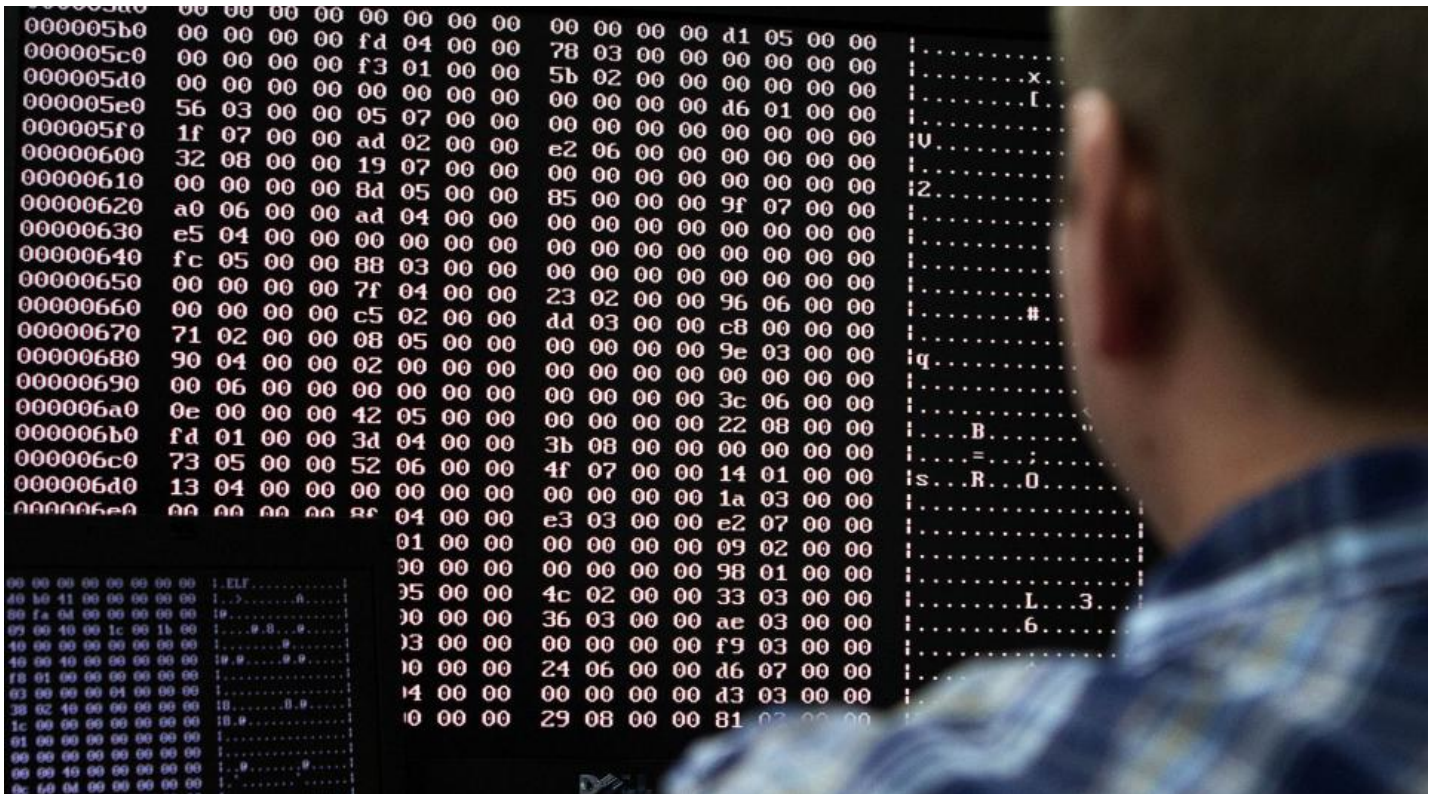


## Cybersécurité : la France prend des mesures contre les cyberattaques



L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié trois arrêtés sectoriels, pour se protéger de tentatives de sabotage industriel.

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) veille sur les réseaux informatiques gouvernementaux ou ceux des entreprises les plus sensibles, comme EDF ou la SNCF et révèle avoir détecté ces derniers mois, des intrusions dans les ordinateurs de certaines sociétés. Cependant, aucune donnée n'a été volée. Ce qui laisse craindre des préparatifs en vue de tentatives de sabotages ou d'attaques terroristes. "La menace cyber doit être prise au sérieux au même titre que le risque d'attentat, d'intrusion ou d'attaque visant les infrastructures vitales de la France", a affirmé Louis Gautier, secrétaire général de la défense et de la sécurité nationale. "...La menace terroriste, aujourd'hui, dans le domaine cyber, c'est de la configuration de sites, de la captation éventuelle de données, c'est du déni d'accès. Mais demain, il peut y avoir des prises de contrôle de système de sécurité, du sabotage de ses systèmes ou de systèmes industrielles qui peuvent avoir des conséquences physiques", a-t-il déclaré.

### Protéger les secteurs d'importance vitale

Pour éviter une cyberattaque de grande envergure, l'ANSSI et le SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale) ont annoncé conjointement, la publication de trois arrêtés sectoriels concernant la gestion de l'eau, les produits de la santé et l'alimentation. Ces trois arrêtés sectoriels fixent les règles relatives à la sécurité des systèmes d'information des OIV (Opérateurs d'Importance Vitale) prévues par l'article 22 de la LPM (Loi de Programmation Militaire) du 18 décembre 2013. Ces règles prévoient notamment l'identification des systèmes d'importance vitale (SIIV), la notification des incidents de sécurité à l'ANSSI et les contrôles pour suivre la mise en place du dispositif. D'ores et déjà, les différents secteurs d'importance vitale ont donc pour obligation légale de se protéger. "L'idée c'est de bien s'assurer que les opérateurs qui gèrent ses réseaux d'eau ont bien la maîtrise de leur système d'information et éviter que les attaquants développent une nouvelle forme, par exemple, de terrorisme ou de demande de rançon vis-à-vis de ses opérateurs.", a expliqué Guillaume Poupard, le directeur de l'ANSSI.