

La guerre informatique

L'essor d'Internet a bouleversé les modes de communication et d'accès à la connaissance. Utilisé par 16 millions de personnes en 1996, Internet comptait 1,1 milliard d'utilisateurs en 2006 et **le nombre d'internautes continue de croître rapidement**. Il devrait s'élever à environ 1,5 milliard en 2011.

En matière de défense et de sécurité, **la maîtrise et la protection de l'information sont désormais de véritables facteurs de puissance**.

La guerre informatique est devenue une réalité. Les acteurs en sont les hackers, les groupes terroristes ou mafieux ainsi que les Etats. Ses principales armes sont les virus, les « chevaux de Troie » et d'autres codes informatiques malveillants. Les champs de ces agressions immatérielles sont vastes, allant de la délinquance au terrorisme informatique en passant par les actions d'espionnage, à des fins économiques par exemple, et les opérations militaires dans le cyberspace.

Dans ce contexte, le Livre blanc met en place :

- **une stratégie défensive** ; une **agence de la sécurité des systèmes d'information sera créée** pour :
 - **détecter et réagir au plus tôt en cas d'attaque informatique**, grâce à un centre de détection chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre de mécanismes de défense adaptés aux attaques ;
 - **prévenir la menace** ; l'agence contribuera au développement d'une offre industrielle de produits de très haute sécurité pour la protection des secrets de l'Etat, ainsi que d'une offre de produits et de services de confiance pour les administrations et les acteurs économiques ;
 - **jouer un rôle de conseil et de soutien** aux administrations et aux opérateurs d'importance vitale ;
 - **informer régulièrement le public sur les menaces** ; le site Internet gouvernemental www.securite-informatique.gouv.fr, lancé en 2008, sera développé pour devenir le portail Internet de référence en matière de sécurité des systèmes d'informations ;
- **une stratégie offensive** ; le Livre blanc prévoit que la France se dotera très rapidement d'une doctrine en la matière et des moyens nécessaires, afin d'être à même de :
 - **mener une riposte proportionnée** en cas d'agression ;
 - **neutraliser**, dans le cadre d'une opération militaire, les systèmes d'information et de commandement de l'adversaire afin de le paralyser ou d'atteindre ses centres de décisions.

| Lutte informatique : qui fait quoi en France ? | |
|---|--|
| Lutte informatique défensive | <ul style="list-style-type: none">• Premier ministre (Agence de la sécurité des systèmes d'information)• Ministères (Cellules spécialisées) |
| Lutte informatique offensive | <ul style="list-style-type: none">• Ministère de la défense (Etat-major des armées)• Services spécialisés |