

Selon un rapport parlementaire, le ministère des Armées risque de tomber dans le "piège Microsoft" - Zone Militaire

Laurent Lagneau



« Avec des si, on mettrait Paris en bouteille », dit-on. Mais il n'en demeure pas moins que la France a eu en main tous les atouts pour favoriser l'essor de la micro-informatique dans les années 1970, avec le micro-ordinateur Micral, alors en avance sur les Altair 8800 et Apple II américains, ou encore avec le projet Cyclades qui, mené par l'ingénieur Louis Pouzin, annonçait l'Internet tel que nous le connaissons aujourd'hui. Mais les décisions prises à l'époque, comme le choix du réseau Transpac [et donc du Minitel], ne permirent pas de profiter pleinement de ces avancées [*]... Alors que, outre-Atlantique, une nouvelle industrie faisait ses premières gammes.

Aussi, faute de solution française [voire européenne], le ministère des Armées s'est donc tourné vers des logiciels américains, notamment ceux fournis par Microsoft. Évidemment, cela n'est pas sans poser quelques interrogations... Surtout quand l'on sait que cette société [a collaboré](#) avec la National Security Agency [NSA, renseignement électronique américain] pour renforcer la sécurité de son système d'exploitation Windows.

Quoi qu'il en soit, en 2009, le ministère des Armées notifia à Microsoft un contrat appelé « open bar » par la presse spécialisée car il permettait de puiser dans le catalogue de l'éditeur américain les logiciels utiles contre un prix forfaitaire de 100 euros [hors taxe] par poste de travail. Et dans le cadre d'une procédure opaque puisqu'il n'y avait pas eu d'appel d'offres. Malgré les polémiques qu'il suscita, ce contrat fut reconduit en 2013 et en 2017, pour un montant estimé à 120 millions d'euros.

Cependant, en 2021, [selon l'APRIL](#), l'une des principales associations de promotion et de défense du logiciel libre, le ministère des Armées passe désormais par l'Union des groupements d'achats publics [UGAP] pour « la fourniture de licences et l'exécution de prestations associées aux programmes en volume Microsoft AE, OV, AMO et Adobe ETLA ».

Évidemment, le ministère des Armées prend toutes les précautions possibles pour éviter tout risque d'espionnage. Sa « stratégie consiste [...] à miser sur des couches de chiffrement. Certes, le système d'exploitation est édité par Microsoft et n'est donc, de ce fait, pas souverain, mais les données ne peuvent pas être lues grâce au chiffrement. Ainsi, l'architecture de sécurité qui a été pensée pour les terminaux et les centres de données du ministère limite, en cas de compromission, l'accès aux données en clair », expliquent les députés Anne Le Hénanff [Horizons] et Frédéric Mathieu [Nupes/LFI], dans un rapport sur les défis de la cyberdéfense, rédigé dans le cadre d'une « mission flash » de la commission de la Défense.

« Si des données chiffrées ont été captées, le ministère des Armées indique que cela ne sera pas grave car il ne sera pas possible [...] de les lire. Microsoft n'a donc, de ce fait, pas accès [à ses] données », insistent-ils.

S'agissant des réseaux classifiés fonctionnant grâce à Microsoft Windows, la solution est encore plus simple : ils ne sont pas connectés à Internet. C'est ainsi le cas au sein du Commandement de la cyberdéfense [COMCYBER]. « L'outil de travail au ministère est le réseau Intradef, lequel est au niveau 'diffusion restreinte' et sur lequel rien ne transite en clair. Ainsi, si des données sont interceptées, elles seront illisibles », précisent Mme Le Hénanff et M. Mathieu.

Cela étant, le ministère des Armées utilise aussi de nombreux logiciels fournis par Microsoft.

« Pour obtenir un système informatique [SI] entièrement souverain, il faudrait également une filière souveraine pour les composants matériels et leurs logiciels [processeurs, microcontrôleurs, etc.] ainsi qu'une filière pour les applications logicielles [suite bureautique, navigateurs, etc.]. Aussi, le développement d'un système d'information entièrement souverain paraît inatteignable et d'un coût prohibitif », soulignent les rapporteurs.

« S'agissant [...] de Microsoft, son rôle se limite à fournir des logiciels. Les infrastructures sur lesquelles [ceux-ci] tournent sont propriété de l'État et les tâches de configuration et d'administration sont assurées entièrement par des personnels étatiques ou des sociétés de confiance de la Base industrielle et technologique de défense. À date, il n'est pas envisagé d'apporter de changement majeur à cette doctrine », poursuivent-ils.

Seulement, cette pratique pourrait ne pas durer étant donné que Microsoft envisage de commercialiser ses logiciels « en tant que services » [« Software as a Service » – SaaS]. En clair, les applications ne seraient plus stockées sur le disque dur d'un ordinateur mais hébergées par un serveur distant.

« Ce risque est une véritable épée de Damoclès qui pèse sur la protection des données des services de l'État mais surtout sur notre souveraineté. Cela est dû au fait que le modèle émergent consiste au seul achat de droits d'utilisation de solutions hébergées à l'étranger. D'ailleurs, Microsoft a indiqué que d'ici 2030, voire 2027, il n'y aura plus que des logiciels sous forme de SaaS », a expliqué Mme Le Hénanff, lors de l'examen du rapport en commission. « Le ministère des Armées, compte tenu de ses exigences en matière de sécurité et de souveraineté, ne peut accepter cette situation, et aujourd'hui, il est difficile d'estimer l'ampleur des risques... », a-t-elle continué.

Plus précisément, le « passage de Windows à une logique de service présente le risque d'une réduction graduelle de la capacité du ministère des Armées à exploiter en propre des réseaux basés sur des technologies Microsoft », met en garde le rapport, qui évoque un « piège Microsoft ». Aussi plaide-t-il pour « explorer » les possibilités offertes par les logiciels libres, comme Linux.

Mais, visiblement, la Direction interarmées des réseaux d'infrastructure et des systèmes d'information [DIRISI] est prudente sur ce sujet.

« Contrairement à certaines idées reçues, libre ne veut pas dire gratuit et l'utilisation [...] des logiciels libres a un coût. Réduire la dépendance à Microsoft poserait des problèmes de compatibilité, aurait un coût équivalent et serait chronophage en termes de formation et de maintien en compétence des administrateurs », a en effet expliqué la DIRISI aux deux députés. « Cela demanderait surtout de disposer d'un minimum de ressources humaines internes dédiées et expertes sur un large panel de logiciels libres, ce qui semble inaccessible à court ou moyen terme compte tenu des tensions actuelles en termes de ressources humaines dans le domaine du numérique », a-t-elle ajouté.

En outre, si la décision de passer aux logiciels libres devait être prise, il n'est pas certain que « toutes les fonctionnalités actuelles du socle et des systèmes métiers puissent être préservées en l'état ». Et elle « aurait des répercussions sur la capacité du ministère à faire évoluer l'architecture de sécurité de son socle et donc à assurer la sécurité de ce dernier » et serait susceptible de retarder « les travaux nécessaires pour s'assurer de notre interopérabilité avec nos alliés et la capacité de la France à être nation cadre », avancent les rapporteurs.

À noter que, depuis une dizaine d'années, la Gendarmerie nationale a déjà fait le grand saut vers les logiciels libres, avec le développement et la généralisation de « GendBuntu », un système d'exploitation basé sur Ubuntu.

[*] Lire : « [Souveraineté technologique française : Abandons et reconquête](#) », de Maurice Allègre, qui était à la tête de la Délégation générale à l'informatique durant cette période.

Conformément à l'article 38 de la Loi 78-17 du 6 janvier 1978 modifiée, vous disposez d'un droit d'accès, de modification, de rectification et de suppression des données vous concernant. [[Voir les règles de confidentialité](#)]