



NICOLAS TRAVETTEREIA

La machine se contrôle elle-même, mais elle ne peut pas déceler les malveillances.

Le bug annoncé des machines à voter

1200 machines pourraient être utilisées l'an prochain pour la présidentielle. Mais elles seraient vulnérables à la fraude.

L'affaire serait toute désignée pour les agents Mulder et Scully de la série télé *X-Files*. Le 18 mai 2003, dans la commune de Schaerbeek (agglomération de Bruxelles), les élections législatives fédérales ont été perturbées... par un rayonnement cosmique. Ledit rayon aurait frappé une machine à voter électronique, provoquant une sorte de bug dans sa mémoire. Un phénomène bien connu des informaticiens. Résultat de ce trouble extra-terrestre : 4096 voix d'électeurs fictifs en plus pour l'un des candidats. Ces « carabistouilles » numériques n'ont rien d'une blague belge. A quelques mois des élections présidentielles en France, elles inquiètent plusieurs collectifs et associations de ci-

toyens, ainsi que des chercheurs et des spécialistes en sécurité informatique. « Ces machines ne sont pas sûres. Il suffit de remplacer la barrette mémoire contenant le programme original par une barrette avec un programme falsifié pour renverser un scrutin », assure Pierre Muller, informaticien et animateur du site Internet www.recul-democratique.org. En 2004, en Irlande, ce genre d'arguments mis en avant par l'association Citoyens irlandais pour un vote électronique fiable (ICTE) et la Société irlandaise d'informatique (ICS) a semé le trouble dans l'esprit des responsables politiques. Le pays venait d'acheter 7500 machines à voter du fabricant néerlandais Nedap pour équiper les bureaux

de vote en prévision des élections européennes. Le lobbying des deux groupes a conduit le gouvernement à nommer dans l'urgence une commission indépendante, la CEV* (Commission sur le vote électronique), pour évaluer les risques. Conclusion : « Nous ne pouvons pas recommander ces machines. » Elles sont donc restées au placard. En juillet dernier, la

même commission pointait encore des lacunes en matière de sécurité, soulignant en particulier la nécessité de prévoir une sortie papier de chaque vote. Le votant pourrait ainsi vérifier son choix, avant que son bulletin en papier ne tombe dans l'urne. En cas de problème, le scrutin serait contrôlable sur la foi des bulletins.

« Sans cette trace physique, le vote n'est pas vérifiable. Si la machine a été détournée, la vérification après le vote indiquera le résultat que le pirate lui aura ordonné d'indiquer, explique Chantal Enguehard, du Laboratoire d'informatique de l'université de Nantes. Le contrôle de la machine auquel procède le président du bureau avant le vote est tout aussi aberrant. En fait, il ne vérifie rien. Il demande à la machine de s'autocontrôler. Cette procédure ne détecte pas les malveillances. »

« Nos machines n'ont rien à voir avec des ordinateurs. Ce sont de simples objets électroniques », se défend Hervé Palisson, directeur de France Elections, importateur des machines de Nedap. Sous-entendu, ces machines échappent au risque de piratage. L'argument est difficilement défendable, car chaque appareil contient un processeur et une mémoire sur laquelle est enregistré un logiciel écrit en langage informatique C. « La seule difficulté est de pouvoir accéder à la machine pour remplacer la mémoire et donc le logiciel », indique Pierre Muller. Or, une annexe du premier rapport irlandais indique que cette opération ne demande pas plus de deux minutes d'accès non autorisé !

OLIVIER HERTEL

✉ www.cev.ie/html/report/index.htm

REPÈRES

LE MINISTÈRE de l'Intérieur a homologué en France trois modèles de machines à voter des fabricants Nedap (Pays-Bas), ES&S Datamatique (Etats-Unis) et Indra Sistemas SA (Espagne).

LA FRANCE comptait 900 machines à voter lors du référendum de 2005. Soit un potentiel de 600 000 à 800 000 électeurs. Pour 2007, 300 machines supplémentaires pourraient être achetées.