HAL
open science

Chaînes de confiance et périmètres de certification : le cas des systèmes de "vote électronique"

François Pellegrini

To cite this version:

François Pellegrini. Chaînes de confiance et périmètres de certification : le cas des systèmes de "vote électronique". [Rapport de recherche] RR-8553, 2014, pp.30. hal-01010950v2

HAL Id: hal-01010950

https://inria.hal.science/hal-01010950v2

Submitted on 25 Jun 2014 (v2), last revised 27 Jul 2014 (v4)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Chaînes de confiance et périmètres de certification : le cas des systèmes de « vote électronique »

François PELLEGRINI

RESEARCH REPORT
N° 8553
juin 2014
Project-Team Bacchus

ISSN 0249-6399 ISRN INRIA/RR--8553--FR+ENG

Chaînes de confiance et périmètres de certification : le cas des systèmes de « vote électronique »

François Pellegrini *

Équipe-Projet Bacchus

Rapport de recherche n° 8553 — juin 2014 — 30 pages

Résumé : On désigne par « vote électronique » le fait de dématérialiser tout ou partie du processus électoral traditionnel basé sur les bulletins en papier. En dépit des apparences, il ne s'agit pas d'une simple adaptation à la marge : la dématérialisation des suffrages modifie substantiellement les propriétés du scrutin. Il importe donc de savoir si le niveau de confiance du processus électoral peut être maintenu suite à cette transformation.
Face à la complexité des systèmes informatiques, l'expert en charge de les auditer se trouve fort démuni. Même les outils théoriques ne peuvent être d'une aide efficace.
Le bon déroulement du processus électoral est attesté au moyen de chaînes de confiance, qui sont rompues par l'introduction de dispositifs opaques, conçus et mis en œuvre par des tiers. Actuellement, il n'est pas possible de garantir qu'un dispositif de « vote électronique » sans reçu de vote fonctionne de façon adéquate. De nombreux bogues l'attestent. En l'état actuel de la science, la seule possibilité offerte au législateur consiste donc à rejeter leur usage, comme l'ont déjà fait certains pays.

Mots-clés : Élection, vote, confiance, secret, vérifiable, sécurité, bogue, porte dérobée, cryptographie.

* francois.pellegrini@labri.fr

RESEARCH CENTRE
BORDEAUX – SUD-OUEST

351, Cours de la Libération
Bâtiment A 29
33405 Talence Cedex

Trust chains and certification perimeters : the case of "e-voting"

Abstract: "E-voting" consists in dematerializing some parts or all of the traditional voting process based on paper ballots. In spite of appearances, it is not a minor adaptation: the digitization of ballots modifies the propreties of the ballot in a substantial way. Consequently, it is of the utmost importance to determine whether the level of confidence in the electoral process can be preserved.

In the face of the complexity of computer systems, the expert in charge of their auditing finds himself at a loss. Even the theoretical tools cannot be of practical help.

The smooth running of the electoral process is asserted by means of trust chains, that are broken by the introduction of opaque devices, designed and operated by third parties. At the time being, it is not possible to guarantee that a receipt-free "e-voting" device functions properly. Many bugs bear witness to that. At the present state of the science, the only option offered to the lawmaker consists in forbidding their use, as several countries already did.

Key-words: Election, voting, trust, secret, verifiable, security, bug, backdoor, cryptography.

1 Introduction

1 Le développement des technologies numériques est à l'origine de bouleversements majeurs de notre société, au point que le terme de « révolution numérique » est maintenant généralement employé pour décrire ce phénomène.

La caractéristique essentielle de la révolution numérique consiste en la transformation de l'ensemble des activités économiques, par la dématérialisation partielle ou totale des échanges d'informations associés à ces activités. L'action de numérisation consiste en la transformation d'une information issue du monde physique (intensité de lumière, fréquence de vibration de l'air, ou toute autre mesure physique) en un ensemble de symboles abstraits, commodément représentés sous forme de nombres [1]. L'intérêt de cette dématérialisation est qu'elle fait entrer l'information ainsi numérisée dans le règne de l'économie des biens immatériels, qui autorise sa copie à coût marginal nul. De ce changement de paradigme découlent des économies d'échelle considérables, et la possibilité de mettre en œuvre des modèles nouveaux de création collaborative de la valeur [37, chapitre 5].

2 L'ensemble des activités humaines étant concernées par la révolution numérique, il est naturel que se pose la question de son applicabilité au processus électoral. Celui-ci diffère cependant fondamentalement de tous les autres processus considérés. Il est défini par un ensemble de contraintes, antagonistes par nature, dont le non respect met en défaut le caractère démocratique du régime qui en utiliserait une version affaiblie.

La question qui se pose au scientifique est donc la suivante : la dématérialisation totale ou partielle du processus électoral démocratique est-elle de nature à lui porter préjudice ? C'est ce à quoi nous allons nous attacher à répondre dans la suite de ce document. Nous nous appuierons pour cela sur deux des versants de l'informatique, que nous étudierons conjointement : son substrat théorique, qui la fonde en tant que science du traitement efficace de l'information, et ses applications pratiques, issues du domaine de l'ingénierie et de la technique.

3 Les mots ayant leur importance, nous avons pris soin d'encadrer le terme de « vote électronique » de guillemets, et ce dès le titre de ce document. Ils sont destinés à rappeler au lecteur qu'accoler ces deux mots n'est pas un fait acquis, mais constitue au contraire l'objet de notre discussion. Nous pourrons ainsi décider, en conclusion, s'il est opportun de les retirer, ou si le terme qu'ils enclosent représente au contraire un oxymore dangereux, auquel de simples guillemets ne sauraient servir de confinement efficace.

2 Motivation de la procédure électorale actuelle

4 La procédure de vote que nous connaissons résulte d'un processus continu d'évolution. Tant la procédure elle-même que les outils de sa mise en œuvre ont fait l'objet d'améliorations successives, afin de bénéficier des progrès techniques susceptibles de renforcer la confiance dans le processus électoral, ou au contraire en réaction à ceux susceptibles de l'amoindrir.

2.1 Conditions du scrutin démocratique

5 Dans un régime démocratique, la procédure électorale vise à garantir, avec le plus haut niveau de confiance possible, deux principes qui sont le fondement même de notre démocratie, et avec lesquels il n'est pas concevable de transiger : la liberté et la sincérité du suffrage.

1. Pour des raisons de mise en œuvre technique des ordinateurs, ces nombres sont souvent codés dans le système binaire, à base des seuls chiffres « 0 » et « 1 ». Ceci provient du fait qu'il est facile de représenter un chiffre binaire par un système physique à deux états : l'électricité passe ou ne passe pas, orientation « nord » ou « sud » d'un cristal ferromagnétique, etc.

2.1.1 La liberté du suffrage

La caractéristique première d'un système démocratique est que les citoyens puissent exprimer librement leur choix. Or, au cours de nombreuses périodes troublées, des pressions ont pu être exercées contre les électeurs, afin qu'ils votent pour un candidat particulier. Ces pressions peuvent prendre la forme de gratifications pour les électeurs ayant voté pour le candidat en question, dans le cas d'un achat de votes, ou de représailles contre ceux ne l'ayant pas fait. 6

C'est pour rendre inopérantes de telles pressions que les rédacteurs des lois fondamentales ont imposé la nécessité du secret du vote [2]. Tant que ce secret est garanti, il est matériellement impossible à un tiers d'être sûr que ses consignes ont été respectées par un électeur donné. L'électeur pourra prendre l'argent du corrupteur tout en n'en faisant qu'à sa guise, et le mafieux ne pourra mettre ses menaces à exécution, au risque de s'aliéner des fidèles et de perdre encore plus de son pouvoir.

Dans le cadre de la procédure actuelle, le secret est garanti par l'inclusion des bulletins dans des enveloppes identiques et par le mélange des bulletins dans l'urne. L'utilisation de ces deux pratiques a pour but de rompre le lien existant entre un bulletin reposant dans l'urne et l'électeur qui l'y a placé. La mise en œuvre d'urnes transparentes, si elle diminue les risques de fraude, augmente les risques de perte du secret, car il serait en théorie possible de suivre visuellement le cheminement d'un bulletin donné depuis son dépôt dans l'urne par un individu donné jusqu'à son décompte à la table de dépouillement. Deux dispositions viennent contrecarrer cette faille potentielle : le secouage de l'urne avant son ouverture, et le regroupement des bulletins par enveloppes de cent, opaques, au sein desquelles les bulletins peuvent encore se mélanger, jusqu'à leur vidage en vrac sur la table de dépouillement. Le législateur considère, sans doute à bon droit, qu'aucun spectateur humain ne dispose des capacités intellectuelles nécessaires pour surmonter ces obstacles. L'interdiction de tout enregistrement vidéo en continu des opérations permet de se prémunir contre l'aide que pourrait apporter la machine dans cette tâche. 7

Une autre façon de violer le secret du scrutin serait que chaque électeur appose un signe distinctif sur son bulletin. Un tiers malveillant présent lors du dépouillement pourrait alors s'assurer que les électeurs ont bien voté comme il leur a été enjoint. C'est pour se prémunir contre cette menace que l'article L.66 du Code électorale dispose que tout bulletin marqué sera considéré comme nul [3, 4]. De même, l'article R.68 oblige à ce que les bulletins valides soient détruits à la fin du scrutin, afin qu'aucune étude a posteriori, comme par exemple l'analyse des empreintes digitales ou de l'ADN qu'ils comportent, ne puisse être effectuée [5]. 8

Remarquons, pour conclure sur ce point, que le secret du suffrage ne peut être garanti que si le nombre de bulletins recueillis est suffisamment grand. Dans le cas hypothétique de circonscriptions unipersonnelles, on pourrait immédiatement déterminer qui a voté quoi. Il faut donc toujours garantir une « dilution » suffisante des suffrages, afin d'induire un niveau d'incertitude suffisant sur le suffrage de chacun des votants [6]. 9

2. L'article 3 de la Constitution française dispose ainsi que : « Le suffrage [...] est toujours universel, égal et secret » [19]. L'article 38 de la Loi fondamentale (« *Grundgesetz* ») de la République fédérale d'Allemagne dispose pour sa part que le vote est « général, direct, libre, égal pour tous et secret » [41].

3. La motivation de cet article est donc bien plus sérieuse que la simple limitation de la créativité des électeurs.

4. La seule faille à ce dispositif consiste à demander à ce que l'électeur introduise un nombre prédéterminé de bulletins du même candidat. En effet, l'article L.65 du Code électoral n'invalide pas ce type d'erreur, vraisemblablement pour ne pas pénaliser un électeur ayant introduit par mégarde dans l'enveloppe quelques bulletins restés collés ensemble. Il aurait été pertinent d'imposer un nombre maximal de bulletins identiques, au delà duquel le suffrage aurait été considéré comme nul, afin de ne laisser que peu de marge à cette possibilité d'identification.

5. L'action de destruction est parfois menée avec trop de légèreté, les bulletins en question étant simplement mis à la poubelle. Il nous semble, à l'aune des techniques actuelles, que leur passage à la déchiqueteuse, suivi d'un trempage dans une solution corrosive, serait une procédure nécessaire afin de détruire tous les marqueurs biologiques qu'ils pourraient comporter.

6. L'absence de dilution avait conduit à la fermeture en catastrophe de certains « bureaux de vote

2.1.2 La sincérité du processus électoral

10 Comme l'a écrit Tom Stoppard, « la démocratie ne réside pas dans l'action de voter, mais dans l'action de compter [7] » [44]. L'ensemble du processus électoral est sans objet si les électeurs n'ont pas la garantie que le résultat annoncé représente exactement la somme des suffrages exprimés individuellement par chacun d'entre eux [8].

11 Le fait que l'électeur conserve toujours lui-même son bulletin en main depuis la sortie de l'isoloir jusqu'au dépôt dans l'urne, qu'il puisse attester par ses propres yeux de la présence de celui-ci parmi les autres bulletins, voire rester jusqu'au dépouillement public et participer à celui-ci, est un élément essentiel de la confiance que les citoyens peuvent placer dans leur système démocratique. La destruction généralisée de cette confiance serait, à bien des égards, beaucoup plus dommageable que la découverte de fraudes perpétrées dans quelques bureaux [34].

12 La période de calme institutionnel que nous connaissons actuellement n'est qu'un bref moment de répit en comparaison de l'histoire politique agitée de notre pays. Les procédures ci-dessus préservent la sincérité du vote contre des attaques extérieures, mais il est également essentiel que le processus de vote puisse résister à des tentatives d'attaques internes, c'est-à-dire de la part des personnes en charge d'assurer l'organisation de l'élection. En particulier, il faut que ces fraudes internes puissent être, sinon empêchées, du moins détectées, afin que le droit du peuple à disposer de lui-même, liberté constitutionnelle, puisse s'exercer pleinement, y compris en dehors du processus électoral si celui-ci est manifestement empêché. La possibilité pour tout citoyen de déterminer par lui-même s'il peut faire globalement confiance au processus électoral auquel il est convié est donc essentielle.

13 Plusieurs autres principes doivent également être respectés afin qu'un scrutin puisse être considéré comme valide. Ces principes relevant de l'ordre de la mise en œuvre du processus électoral, ils ne sont cependant pas inscrits dans les lois fondamentales. C'est le cas par exemple de l'authenticité des suffrages. Le processus mis en œuvre doit garantir que les suffrages proviennent bien des seuls électeurs habilités à voter. C'est ainsi que, de façon réglementaire, sont mis en place un ensemble de procédures (contrôle de la pièce d'identité, etc.) destinées à vérifier que la personne qui exprimera son suffrage est bien celle dont le nom est inscrit sur la liste d'émargement. Faute de respecter ce principe, aucune interprétation ne peut être faite du résultat du scrutin.

2.2 Évolution des pratiques à l'aune de la technique

14 Les critères de secret et de sincérité sont antagonistes. Ils le sont d'autant plus que le secret doit être absolu : nul autre que l'électeur ne doit pouvoir savoir ce qu'il a voté. L'organisateur du scrutin lui-même doit être tenu dans l'ignorance des informations qu'il manipule. Cette contrainte est donc bien plus forte que dans la majorité des activités confidentielles, comme par exemple les activités bancaires, pour lesquelles l'ensemble du public doit ignorer les opérations effectuées par un client, à l'exception du banquier lui-même.

15 Le banquier, tout comme le voisin à qui nous confions un double de nos clés au cas où nous les perdrions, est un « tiers de confiance ». On désigne ainsi une personne que nous dotons de la capacité de violer notre sécurité, en échange des services qu'elle peut rendre. Le principe

numériques » lors des élections à l'Assemblée des Français de l'étranger de juin 2006 [38].

7. « *It's not the voting that's democracy, it's the counting.* »

8. On pourrait ajouter un troisième critère à l'existence d'un suffrage démocratique, qui est que le choix exprimé lors de l'élection soit effectivement pris en compte par le pouvoir en charge de l'organiser. On pourra à ce propos citer le célèbre aphorisme de Coluche : « La dictature, c'est "ferme ta gueule" ; la démocratie, c'est "cause toujours" », remis au goût du jour lors du référendum sur le Traité constitutionnel européen. Cette question sort néanmoins du cadre du propos de ce document.

du processus électoral est qu'il doit fonctionner sans tiers de confiance. L'existence d'un tiers informé est antinomique du caractère absolu du secret.

Il en découle qu'aucun tiers ne peut contrôler a posteriori la sincérité du scrutin en comparant le résultat du vote à une quelconque matérialisation de la volonté de l'électeur. Une telle trace violerait le secret du vote et porterait atteinte à la liberté de l'électeur, en la rendant accessible à ce tiers.

De même, le contenu de l'urne, en tant que tel, ne permet aucune contestation de sa sincérité du scrutin. Celle-ci ne peut se faire qu'indirectement, par confrontation entre le contenu de l'urne et la liste d'émargement, ou par la mise en évidence de procédés visant à modifier indûment leur contenu.

Toute disposition visant à accroître les garanties de sincérité du scrutin ne peut être acceptée 16
que dans la mesure où elle ne porte pas atteinte à son secret. C'est le cas par exemple de l'introduction des urnes transparentes. Celle-ci a permis d'offrir des garanties supplémentaires contre le bourrage, en facilitant la constatation que les urnes sont vides au début du scrutin et qu'elles ne contiennent pas de double fond, et a rendu plus difficile le remplacement d'une urne par une autre n'ayant visiblement pas le même nombre de bulletins. Cette introduction n'a pu se faire qu'après l'invention des matières plastiques, les urnes en verre étant trop fragiles et trop lourdes pour être déployées de façon économique. Comme nous l'avons vu plus haut, elle s'accompagne de procédures correctrices visant à ce que la transparence de l'urne ne permette pas à un tiers de suivre le cheminement du bulletin entre son dépôt dans l'urne et son dépouillement.

Un autre exemple du processus de co-évolution entre l'état de la technique et la procédure électorale concerne la nécessaire interdiction des téléphones mobiles et autres appareils de prise de séquences vidéo dans les isoloirs, car ceux-ci peuvent permettre à l'électeur de filmer ses actions dans l'isoloir, et donc être requis comme preuve de bonne exécution par les acheteurs ou racketteurs éventuels. Une telle mesure d'interdiction a d'ailleurs déjà été prise en Italie [8].

3 Nature des systèmes de « vote électronique »

Les arguments avancés en faveur de l'introduction de dispositifs numériques au sein du pro- 17
cessus de vote sont multiples. Ils vont de la réduction des coûts de mise en œuvre du scrutin à la rapidité du dépouillement, voire à l'augmentation de la fiabilité du processus électoral, du fait de la suppression supposée des erreurs humaines [9].

Afin de bien comprendre comment ces systèmes fonctionnent, nous commencerons par en décrire la structure, avant d'expliquer l'usage qui y est fait de la cryptographie.

3.1 Structure d'un système de « vote électronique »

Le terme de « vote électronique » est excessivement général. Il recouvre des situations très 18
diverses, dans lesquelles le processus électoral est soit partiellement, soit totalement délégué à des dispositifs numériques. C'est pour lutter contre cette imprécision que des nomenclatures ont été proposées [24].

Nous ne considèrerons, dans le cadre de ce document, que les systèmes dans lesquels les suffrages sont intégralement dématérialisés. En effet, les systèmes qui impriment un bulletin visible de l'électeur et qui tombe ensuite dans une urne physique, ne sont qu'une adaptation à la marge du processus traditionnel, qui n'apporte de notre part que peu de commentaires, sinon concernant son coût élevé pour un résultat déjà atteint de façon plus simple.

9. Ce qui fait un peu trop rapidement cas du fait que les équipements informatiques sont tout autant conçus par des humains.

19 La modélisation informatique du processus électoral s'articule autour de deux modules logiciels principaux. Le premier a pour but de simuler la liste d'émargement, et le second, l'urne elle-même. La principale fonctionnalité du module de gestion de la liste d'émargement est d'enregistrer la participation des électeurs qui y sont inscrits, afin que seuls ces derniers puissent voter, une unique fois. Le module de gestion des suffrages, souvent appelé abusivement [10] « urne électronique », à pour fonction de collecter et d'accumuler les suffrages exprimés par les électeurs, puis de restituer le résultat du vote, c'est-à-dire la somme des suffrages recueillis par chaque candidat et / ou liste.

20 La gestion de la liste d'émargement n'est pas un problème en soi. Cette liste étant publique, la question du secret ne se pose pas. Celle de la sincérité ne se pose pas non plus, puisque la seule information que contient cette liste est la participation ou non de l'électeur au scrutin. Tout électeur peut, en consultant ladite liste, vérifier que le système a bien pris en compte sa présence ou son absence. La seule contrainte globale la concernant est que le nombre total de participants soit toujours égal au nombre de bulletins comptés dans l'urne. La violation de cette contrainte atteste d'une intervention malveillante ou d'un dysfonctionnement de l'un des deux dispositifs, voire des deux, ou du système censé les mettre en œuvre à tour de rôle. Ce type d'anomalies, symptôme d'un dysfonctionnement grave, n'est pourtant pas rare : il a par exemple été constaté lors d'élections internes à un parti politique [14], mais aussi lors du « vote » par Internet lors des élections législatives de 2012 [39].

21 L'urne est le dispositif au cœur du processus électoral, puisque de son contenu dépend l'issue du scrutin. C'est donc sur elle que les éditeurs de logiciels de « vote électronique » concentrent l'essentiel de leurs mesures de sécurité informatique. La plus emblématique d'entre elles est la cryptographie.

3.2 Le recours à la cryptographie

22 La cryptographie est la discipline ayant pour objet de garantir la sécurité d'une communication en la présence de tiers malveillants. Elle s'intéresse aux questions relatives à la confidentialité, à l'intégrité et à l'authentification des communications.

La cryptographie est une technique réputée sûre. Comme l'a confirmé Edward Snowden lors d'une de ses interviews : « *Le chiffrement fonctionne. Les crypto-systèmes robustes, mis en œuvre de façon appropriée, sont une des rares choses auxquelles vous pouvez vous fier* [11]. » Une confirmation implicite en est que la National Security Agency (NSA), l'agence étatsunienne en charge des interceptions électroniques, a investi des sommes considérables dans l'implantation de portes dérobées [12] au sein des logiciels et matériels informatiques les plus divers, afin de contourner cet obstacle pour le moment insurmontable [4].

3.2.1 Utilisation du chiffrement asymétrique

23 Dans le cas du « vote électronique », la cryptographie est utilisée dans le but de garantir la sécurité de la transmission et de la conservation du suffrage de l'électeur, entre le dispositif de recueil de celui-ci et le dispositif de restitution du résultat du scrutin. Pour ce faire, le suffrage

10. Puisque la simulation de l'urne est réalisée au moyen d'un logiciel, le terme « urne informatique » semble plus adapté.

11. « *Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.* »

12. Une porte dérobée est une fonctionnalité logicielle, inconnue de l'administrateur d'un système informatique, et qui permet d'acquérir des privilèges et / ou d'effectuer des actions que cet administrateur n'aurait pas autorisés. Voir *infra*.

de l'électeur est chiffré avant d'être stocké dans l'urne, et ne sera déchiffré qu'au moment de la proclamation des résultats.

Les méthodes de chiffrement utilisées sont nécessairement des méthodes dites « à clé publique ». Ces méthodes sont basées sur des paires de clés jumelées, telles que ce qui a été chiffré par une clé ne peut être déchiffré que par l'autre, et réciproquement. L'une des clés est gardée secrète, alors que l'autre est diffusée publiquement. Il n'y a aucun risque à cette diffusion, car la connaissance de cette clé ne permet pas de déchiffrer ce qui aura été chiffré par elle. C'est en cela que l'on parle de chiffrement « asymétrique », par opposition au chiffrement « symétrique », pour lequel la même clé sert au chiffrement et au déchiffrement [13].

Chacun des dispositifs de recueil des suffrages contient une copie de la clé publique, qui sera utilisée pour chiffrer le suffrage de l'électeur. Le secret de celui-ci est réputé garanti par le fait qu'un tiers qui étudierait le dispositif de recueil et en extrairait la clé publique ne pourrait se servir de celle-ci pour déchiffrer les suffrages recueillis [14]. La clé privée correspondante est conservée par le président du bureau de vote et / ou ses assesseurs, et servira le moment venu à déchiffrer les suffrages.

La gestion des clés de chiffrement fait l'objet d'une procédure spécifique, parfois emprunte 24
d'une certaine solennité. La paire de clés, publique et privée, est générée aléatoirement par un logiciel dédié avant l'ouverture du scrutin. Ainsi, les paires de clés diffèrent d'un scrutin à l'autre, et la connaissance de la clé privée issue d'un scrutin précédent ne pourra servir à perturber le scrutin suivant. La clé publique est recopiée en autant d'exemplaires que nécessaire, afin de configurer les dispositifs de recueil. La clé privée est découpée en plusieurs tronçons, qui sont distribués au président du bureau de vote et à ses assesseurs. Ainsi, chacun d'eux est réputé ne pas pouvoir accéder au résultat de l'élection sans l'accord des autres. Les tronçons ne sont rassemblés, pour permettre le dépouillement, qu'une fois le scrutin clos.

Pour éviter que les suffrages ne soient conservés individuellement jusqu'au moment du dé- 25
pouillement, ce qui pourrait permettre de les corréler *a posteriori* à l'ordre de passage des électeurs, ils sont accumulés dans l'urne à mesure de leur arrivée. Ainsi, l'urne contient à chaque instant, sous forme chiffrée, le total partiel des voix obtenues par chaque candidat. Cette caractéristique découle des propriétés mathématiques des systèmes de chiffrement utilisés, appelés « chiffrements homomorphes ». La propriété d'homomorphisme garantit que la somme des valeurs chiffrées soit toujours égale au chiffrement de la somme des valeurs non chiffrées. L'urne est en fait la forme chiffrée d'une table de nombres, d'autant de cases qu'il y a de candidats, et dont toutes les valeurs sont initialement égales à zéro. Chaque case représente le nombre de voix recueillies par un candidat. Chaque suffrage est représenté sous la forme d'une table chiffrée de même taille, dont toutes les cases contiennent la valeur « zéro » sauf celles du ou des candidats [15] pour lequel l'électeur souhaite voter, qui sont à la valeur « un ». Ainsi, additionner les valeurs des deux tables revient à donner une voix de plus aux candidats choisis par l'électeur.

3.2.2 Les limites du chiffrement

En dépit de l'infaillibilité théorique de la cryptographie, son usage dans le contexte du « vote 26
électronique » ne saurait constituer une garantie de sécurité de ce dernier.

Tout d'abord, comme l'a rappelé Edward Snowden, si les propriétés mathématiques des crypto-systèmes garantissent en théorie leur robustesse, cette dernière dépend essentiellement

13. Pour plus d'informations, voir [46].

14. Il le pourrait en revanche avec un chiffrement symétrique, puisque la clé de chiffrement sert également au déchiffrement. C'est pour cette raison que les méthodes de chiffrement symétrique sont inapplicables dans ce contexte.

15. Dans certains systèmes électoraux, comme par exemple en Belgique, il est possible de voter simultanément pour une liste et pour certains candidats de la liste, en leur accordant des « voix de préférence ».

de la qualité de leur mise en œuvre. Ainsi la faille « *Heartbleed* » du logiciel OpenSSL, révélée en avril 2014, permettait-elle de compromettre la sécurité de tous les ordinateurs utilisant les versions de ce logiciel postérieures au 31 décembre 2011, date à laquelle ce bogue a été introduit [48].

Qui plus est, indépendamment de l'existence de failles techniques, la cryptographie ne peut par principe s'appliquer au « vote électronique » que de façon limitée, et son usage induit des inconvénients qui vont à l'encontre du résultat souhaité. Ainsi, si le chiffrement des données est destiné à garantir le secret du scrutin, depuis l'expression du suffrage de l'électeur jusqu'au déchiffrement de l'urne, il empêche également de vérifier la conformité des suffrages recueillis, une fois ceux-ci chiffrés, sauf à violer ce chiffrement.

27 Pour illustrer cette problématique, considérons le cas d'un « vote électronique » à distance par Internet, tel que celui mis en œuvre pour l'élection à l'Assemblée des Français de l'étranger [38]. Imaginons que le système de décompte des suffrages est celui décrit précédemment : les suffrages recueillis par chaque candidat sont stockés dans une table de totalisation comportant autant de cases qu'il y a de candidats, et le suffrage de l'électeur est représenté sous la forme d'une table de même taille, dont les valeurs sont ajoutées à la table de totalisation, cette addition s'effectuant entre les valeurs stockées sous forme chiffrée.

Chaque électeur « vote » au moyen d'un logiciel qu'il a téléchargé au préalable sur son ordinateur. Le plus souvent, le téléchargement et la mise en route du logiciel sont transparents pour l'usager, le logiciel étant inclus au sein d'une page web hébergée sur le site de l'administration mettant en œuvre le système de « vote électronique ». La fonction de ce logiciel est de recueillir les éléments d'identification de l'électeur, puis son suffrage, de construire la table correspondant à ce dernier, et de la transmettre sous forme chiffrée au logiciel serveur central de totalisation, avec les informations d'identification permettant l'interrogation et la mise à jour de la liste d'émargement.

Le logiciel étant présent sur l'ordinateur de l'électeur, ce dernier a tout à fait la possibilité d'en faire une copie. En étudiant celle-ci, et en la modifiant [16], un utilisateur malicieux pourrait par exemple créer une table chiffrée dans laquelle la case de son candidat n'est pas à la valeur « un », mais à la valeur « dix », les cases de neuf autres candidats étant à la valeur « moins un ». Le fait d'ajouter cette table au décompte des voix revient à transférer neuf voix des autres candidats vers le candidat choisi, sans modifier le nombre total de suffrages exprimés par rapport à la liste d'émargement.

Un premier moyen pour détecter ce type de fraude consisterait à déchiffrer la table reçue, pour vérifier que seule une case de la table est à la valeur « un » et toutes les autres à la valeur « zéro », avant de l'ajouter à la table de totalisation. Il faudrait pour cela déchiffrer le suffrage avant la clôture du scrutin, ce qui n'est pas possible, puisque la clé privée de déchiffrement n'est pas censée être disponible à ce stade.

Puisqu'il n'est pas possible de travailler sur la forme non chiffrée du suffrage pour en vérifier la validité, une deuxième solution consiste à comparer le suffrage chiffré avec des suffrages « gabarits » correspondant au chiffrement de toutes les combinaisons valides. Si le suffrage de l'électeur appartient à cette liste, c'est qu'il est valide, et peut donc être ajouté sans risque aux totaux partiels de l'urne chiffrée. S'il n'y figure pas, c'est qu'il est invalide, et doit donc être considéré comme nul. Or, cette simple vérification implique que le secret du scrutin est violé. En effet, puisque chaque gabarit correspond de façon univoque à une combinaison de vote valide, savoir que le suffrage correspond à un gabarit donné revient à savoir ce qu'a voté l'électeur.

Une troisième solution consiste alors à stocker l'ensemble des suffrages sous forme chiffrée,

16. Il ne s'agit pas d'un cas hypothétique, une telle rétro-ingénierie de logiciel électoral, dans le but de créer un bulletin invalide, ayant déjà été réalisée dans le contexte du vote des Français de l'étranger aux élections législatives de mai 2012. Voir infra section 7.

sans les totaliser au fur et à mesure de leur réception. Ce n'est que lorsque le vote est clos que, grâce à la clé privée, l'ensemble des suffrages est déchiffré dans la mémoire de l'ordinateur totalisateur. Leur conformité est alors vérifiée, et seuls les bulletins considérés comme valides sont totalisés, les autres étant considérés comme nuls. Remarquons à ce propos que les systèmes de « vote électronique » ne permettent pas aux électeurs de créer de bulletins nuls, alors que c'est une liberté laissée à l'électeur lors d'un scrutin traditionnel. Dans les systèmes de « vote électronique », les votes nuls sont donc soit le résultat de dysfonctionnements du système, soit de tentatives de fraude portant sur la structure des bulletins et qui ont pu être détectées. Le stockage de l'ensemble des suffrages sous forme chiffrée, qui semble constituer la meilleure solution, pose cependant lui aussi un problème. L'ordre dans lequel les bulletins sont stockés puis déchiffrés peut être corrélé à l'ordre d'émargement des électeurs au sein du système, ce qui permet au concepteur du système de connaître les suffrages de l'ensemble des électeurs [17, page 49]. Ce résultat peut tout autant être obtenu dans un système qui prétend additionner les suffrages sans en conserver de copie, mais réalise néanmoins de telles copies à l'insu des électeurs. Il en est de même avec la technique de comparaison des suffrages chiffrés avec des gabarits prédéterminés, qui peut être mise en œuvre de façon tout aussi cachée.

Ainsi le « vote électronique » à distance viole-t-il doublement les principes qui fondent le 28
système électoral démocratique. D'une part, parce que l'absence d'isoloir empêche tout secret du vote : personne ne peut savoir si l'électeur devant son ordinateur n'est pas sous le regard d'un tiers prêt à le gratifier ou à mettre ses menaces à exécution, voire à voter à sa place. Le fait de voter à distance, que ce soit de façon dématérialisée ou bien par correspondance papier, ne permet aucunement de garantir l'authenticité des suffrages [1]. D'autre part, parce que les suffrages générés par le logiciel de cet électeur ne présentent aucune garantie de conformité, et que la vérification de cette conformité implique que le tiers en charge de la création du logiciel totalisateur soit en capacité de violer le secret du suffrage de l'électeur, du fait des traces qu'il lui est possible de conserver.

3.3 L'incontournable tiers technique

Dans le système de vote traditionnel, tout a été fait pour garantir l'absolu secret du suffrage de l'électeur, y compris vis-à-vis des personnes en charge de mettre en œuvre le processus électoral. Dans le cas du « vote électronique », le recours à un intermédiaire technique pour l'encodage, la transmission et le décompte des suffrages permet par nature à cet intermédiaire d'accéder au contenu des suffrages, soit en amont du processus de chiffrement, soit en aval, soit même au vol, par l'étude des messages chiffrés. Le secret du vote n'est plus absolu, quel que soit le niveau de cryptographie mis en œuvre. La cryptographie robuste protège contre les tiers absolus, mais aucunement contre les tiers de confiance chargés de la mettre en œuvre.

L'exemple précédent met en lumière l'impossibilité, pour l'électeur, d'échapper à la curiosité 29
du « tiers technique » qui a conçu le système de « vote électronique ». Ce tiers technique est, de ce fait, un tiers de confiance. De ce constat découlent deux questions essentielles pour que l'électeur puisse accorder sa confiance à un système de « vote électronique ». Premièrement, est-il possible de garantir que ce tiers de confiance se comporte de façon loyale, et n'a pas perverti le fonctionnement du système informatique qu'il a conçu ? Deuxièmement, est-il possible à un tiers absolu de contourner les sécurités mises en œuvre par un tiers technique loyal, afin de pervertir à son profit le processus électoral ? Les sections suivantes visent à répondre successivement à ces deux questions.

4 Portée des menaces

30 Afin de prendre la mesure de l'insurmontabilité de la tâche dévolue aux experts en charge d'auditer les systèmes informatiques servant au « vote électronique », il nous semble nécessaire de donner un rapide aperçu de la complexité de ces systèmes et de la difficulté d'en détecter les failles. Que le non spécialiste de l'informatique ne s'effraie pas : si nous exposerons parfois certaines considérations techniques afin de justifier nos assertions, notre discours se placera majoritairement dans un cadre conceptuel. Celui-ci nous permettra de mettre en évidence, à travers différents exemples, les principes abstraits qui fondent cette insurmontabilité.

4.1 La faiblesse inhérente des systèmes complexes

31 Les attaques qu'il est possible de mener contre un système informatique sont d'une époustouflante diversité. Ceci tient à la complexité croissante de ces systèmes, constitués d'un assemblage de multiples technologies. Or, chacune d'elles, ainsi que leur intégration, sont conçues par des équipes distinctes. Les caractéristiques internes de chacun des dispositifs ne sont donc pas connues des autres équipes, tant pour des raisons de secret industriel que par la quantité considérable d'informations que cela supposerait de maîtriser. L'effet des particularités de conception internes d'un dispositif sur les autres ne peut donc être évalué *a priori*. Ainsi, bien que chacune de ces équipes ait à cœur de sécuriser le dispositif qu'elle conçoit, l'intégration de dispositifs d'origines diverses induit de nombreuses potentialités de failles.

32 Or, en termes de sécurité, les protections ne s'additionnent souvent pas : le niveau de sécurité d'un système est celui de son maillon le plus faible. La présence d'un seul dispositif faiblement sécurisé, au sein d'un système réputé sûr, peut compromettre l'ensemble de sa sécurité.

4.1.1 Diversité des niveaux d'attaque

33 Pour réduire la portée de la défaillance d'un sous-système, une méthode classique, inspirée de l'architecture militaire, consiste à construire un système à l'image d'un ensemble d'enceintes concentriques, afin que la compromission d'une enceinte soit limitée par l'enceinte suivante. Cependant, tout comme dans le monde physique, ces ouvrages de défense peuvent être globalement contournés. De la même façon que des sapeurs peuvent progresser sous les édifices successifs pour déboucher au cœur des forteresses, des « sapes numériques » peuvent offrir l'accès au cœur d'un système, en contournant l'ensemble de son dispositif de défense, en s'attaquant pour cela au substrat du système plutôt qu'au système lui-même.

34 C'est par exemple le cas avec les cartes réseau des ordinateurs. Ces cartes servent d'interface entre l'ordinateur et les réseaux auxquels elles sont connectées, et permettent l'échange d'informations avec des équipements distants. Du fait de la généralisation des attaques à distance, majoritairement au moyen de virus informatiques, les systèmes d'exploitation ont été équipés de multiples dispositifs logiciels permettant de réduire la portée de ces attaques : filtres de connexion (aussi appelés « pare-feux ») pour limiter les tentatives de connexions depuis l'extérieur, en n'acceptant que les connexions provenant de certains émetteurs ou mettant en œuvre certains protocoles de communication [17] ; logiciels de reconnaissance de signatures de virus au sein des flux de données et des messages, pour empêcher l'exécution de logiciels malveillants ; séparation des rôles d'administrateur système et d'utilisateur, afin que l'exécution d'un logiciel malveillant

17. Par exemple, on fera en sorte qu'un serveur web d'entreprise n'accepte de l'extérieur que les tentatives de connexion selon le protocole HTTP, correspondant à des demandes de pages web, et réserve les connexions selon le protocole SSH, pour l'administration à distance de ce serveur, aux seules machines identifiées comme appartenant au service informatique de l'entreprise.

au nom d'un utilisateur ne permette pas à ce logiciel d'effectuer des actions au nom de l'administrateur, telles que celles lui permettant d'accéder aux informations possédées par d'autres utilisateurs.

Cependant, toutes les protections ci-dessus relèvent du niveau du système d'exploitation, et 35
peuvent être contournées en s'attaquant directement à la carte réseau elle-même. Ces cartes sont en fait des ordinateurs à part entière : elles disposent de leur propre processeur dédié, piloté par un logiciel embarqué appelé génériquement « *firmware*[18] ». Elles peuvent de surcroît accéder directement à la mémoire vive de l'ordinateur. Ces caractéristiques leur permettent de prendre en charge de façon autonome les transferts de données avec le monde extérieur, tout en laissant le processeur de l'ordinateur libre d'effectuer d'autres tâches. Il suffit pour cela que ce dernier leur indique l'endroit de la mémoire vive où se trouvent les données prêtes à l'envoi, ainsi que l'identifiant[19] de l'équipement distant au sein du réseau. La capacité de la carte réseau à accéder à l'ensemble de la mémoire vive de l'ordinateur, avantageuse en termes d'efficacité des transferts, constitue cependant une faille majeure. Elle permet à tout attaquant prenant le contrôle de la carte réseau de « siphonner » l'intégralité de la mémoire vive de l'ordinateur ciblé, lui donnant ainsi accès à l'intégralité des données en cours de traitement, quel que soit l'utilisateur auquel elles appartiennent. Ce siphonnage étant mis en œuvre au niveau du matériel, le système d'exploitation n'a aucun moyen de le détecter, puisque les messages échangés entre l'attaquant et la carte réseau ne lui seront bien évidemment pas répercutés par cette dernière. La carte réseau peut également écrire à sa guise dans la mémoire vive, et modifier au vol le fonctionnement des programmes et du système d'exploitation.

Ce type d'attaque illustre l'intérêt, pour un service secret ou un groupe malveillant, de placer 36
des « portes dérobées » (« *backdoor* », en anglais) dans certains matériels considérés comme « peu nobles », mais d'une importance pratique considérable [2]. L'installation de portes dérobées au sein des logiciels embarqués de pilotage des cartes réseau est un moyen remarquablement efficace pour accéder à une quantité considérable d'informations, sans que l'administrateur de l'ordinateur puisse s'y opposer d'une quelconque manière. La parade consiste alors, pour le responsable de la sécurité du système, à filtrer en amont les connexions entre ses ordinateurs et le monde extérieur, au moyen d'équipements dédiés (routeurs, ponts d'échange, etc.). Ces matériels sont donc eux aussi des cibles privilégiées pour l'implantation de portes dérobées permettant, entre autres, de désactiver ce filtrage [27].

Il peut arriver que des portes dérobées soient installées de façon délibérée par les concepteurs 37
du logiciel eux-mêmes, sans intention malicieuse. Il s'agit souvent d'accès destinés à faciliter le débogage du logiciel en usine, voire à permettre la réutilisation de fonctionnalités déjà présentes au sein d'un logiciel sécurisé, sans avoir à les dupliquer au sein d'un autre logiciel [30]. Dans tous les cas, il s'agit de très mauvais choix techniques, dont l'évidence n'apparaît malheureusement qu'une fois que ces portes dérobées sont découvertes et exploitées par des personnes malveillantes. Par exemple, la présence de portes dérobées au sein de nombreuses versions de BIOS[20] est maintenant de notoriété publique. Elles permettent à quiconque de circonvenir les mots de passe mis en place par les usagers légitimes de l'ordinateur, et de modifier la configuration de ce dernier [43].

18. Parce qu'il est bien moins coûteux de développer du logiciel que du matériel, à fonctionnalités égales, les concepteurs de périphériques s'attachent à réduire leur part matérielle à ce qui est strictement nécessaire à l'interaction du périphérique avec le monde extérieur. Le pilotage de cette partie matérielle est dévolu à un processeur dédié, associé à un logiciel spécifique. Ce logiciel est habituellement développé par l'entreprise (« *firm* », en anglais) qui a conçu le matériel, d'où le terme de « *firmware* ». Un ordinateur est donc constitué de multiples matériels, mais aussi de multiples logiciels, tous susceptibles de failles [31].

19. Ce pourra par exemple être l'« adresse IP » (pour « Internet Protocol ») de l'équipement distant au sein d'Internet.

20. Voir *infra*.

Dans certains cas également, il a pu arriver qu'un fabricant de matériel réseau, une fois informé par un expert de la présence d'une faille présentant toutes les caractéristiques d'une porte dérobée, prétende par la suite l'avoir corrigée alors qu'il s'est juste efforcé de mieux la cacher [26].

38 Ces exemples conduisent à postuler que, en termes d'équipements informatiques, la présence de portes dérobées n'est pas l'exception mais plutôt la norme. De fait, l'usage de tout composant et / ou périphérique tiers au sein de systèmes destinés au « vote électronique » laisse planer un soupçon sérieux quant à la possibilité d'en altérer le processus de façon totalement invisible [21]. Nous illustrerons cet aspect en évoquant la diversité des attaques pouvant être conduites contre un système informatique.

4.1.2 Diversité des vecteurs d'attaque

39 Parce que les cartes réseau et autres périphériques considérés comme sensibles représentent des vecteurs d'attaques idéaux, ils font parfois l'objet d'audits de la part d'experts en sécurité. Ces audits ciblés sont néanmoins inopérants, car il est possible d'installer des portes dérobées à partir de n'importe quel matériel, y compris le plus anodin, comme par exemple une banale carte audio. Nous l'illustrerons en décrivant un schéma d'attaque possible [7].

40 Lorsqu'un ordinateur démarre, le processeur commence par exécuter un logiciel rudimentaire pré-installé en usine, le BIOS [22]. Le rôle de ce dernier est de charger en mémoire vive le système d'exploitation stocké sur le disque dur, puis de lui transférer le contrôle de l'ordinateur. Le système informatique est alors pleinement opérationnel.

L'une des tâches du BIOS, avant de donner la main au système d'exploitation, est de détecter le matériel présent au sein de l'ordinateur et de le préparer à être utilisé par le système. Comme le BIOS est un logiciel pré-installé qui ne peut connaitre tous les matériels à venir, il possède en son sein un mécanisme d'extension, par lequel il permet à un matériel de lui fournir lui-même les fragments de programme permettant de le piloter. La faille est donc béante : un attaquant peut faire en sorte que ces fragments, subtilement altérés, perturbent le chargement ultérieur du système d'exploitation. L'un des moyens pour cela consiste à substituer à la volée, au code original du système en train d'être lu à partir du disque dur, une version modifiée de celui-ci. C'est donc à un système d'exploitation perverti, embarquant un logiciel malveillant ou les indications pour l'exécuter, que sera donné le contrôle de l'ordinateur.

41 L'élégance de cette attaque réside dans le fait que tout audit du code du système d'exploitation résidant sur le disque dur de l'ordinateur ne peut qu'être infructueux, la version altérée n'étant présente que dans la mémoire vive de l'ordinateur. Pour mettre en évidence l'attaque, il faudrait effectuer une sauvegarde à la volée de l'intégralité de la mémoire vive. Comme, habituellement, ceci se fait en ayant recours aux services du BIOS, un attaquant prévoyant peut également couvrir ses traces par ce biais. Seule une lecture directe de la mémoire vive permettrait d'en connaître le contenu réel.

42 Parce que le logiciel malveillant réside en mémoire vive, il peut s'auto-modifier pour ne pas laisser de traces. Dans le cas qui nous intéresse, on peut imaginer que ce logiciel a été conçu pour ne s'activer que le jour donné d'une élection, connu à l'avance. Avant cette date, à chaque allumage, le logiciel malveillant s'auto-supprimera de la mémoire vive, le dispositif d'armement restant cependant présent au sein du matériel. En revanche, lors de l'allumage de l'ordinateur le jour dit, le logiciel malveillant réalisera ce pour quoi il aura été conçu, avant de s'effacer de la

21. Nous rappellerons à ce titre que la majorité des dispositifs de « vote électronique » utilisés jusqu'à maintenant sont basés sur une architecture de type PC contenant un tel BIOS, de même que la majorité des ordinateurs utilisés par les électeurs dans le cadre du « vote à distance ».

22. Pour « *Basic Input/Output System* ».

mémoire du matériel lui ayant servi de vecteur d'entrée, par réécriture de son *firmware*. Toute audit ultérieur, y compris de l'ensemble du système, sera donc infructueux.

On pourrait penser que de tels logiciels malveillants sont rares et difficiles à mettre en œuvre. 43
En fait, c'est tout le contraire : ils sont installés d'origine par nombre de constructeurs informatiques. Récemment, des ingénieurs en sécurité ont montré que le logiciel CompuTrace / LoJack, dont la fonction prétendue consiste à tracer les ordinateurs volés, est installé et activé par défaut sur beaucoup d'ordinateurs neufs, à l'insu de leurs propriétaires. Or ce logiciel, qui se connecte de façon régulière et silencieuse sur les serveurs de l'entreprise étatsunienne qui le commercialise, permet le téléchargement et l'exécution de fragments de logiciel arbitraires, susceptibles de subvertir le fonctionnement de l'ordinateur [9]. Initialement considéré comme un logiciel malveillant, sa signature est maintenant enregistrée sur les « listes blanches » de la plupart des logiciels antivirus, qui sont donc actuellement configurés pour ignorer sa présence. Les utilisateurs des ordinateurs qui le possèdent ne sont donc plus à même d'être informés qu'ils en sont munis.

Tout concepteur de matériel ou de logiciel est investi par son client du rôle de tiers de 44
confiance : on attend de lui qu'il travaille loyalement à fournir un dispositif rendant exclusivement le service attendu. Or, la complexification des systèmes informatiques accroît grandement le nombre de ces tiers, et la généralisation des composants et logiciels dotés de portes dérobées conduit à une dégradation notable de la sécurité des systèmes d'information.

4.1.3 Les illusions de la cryptographie

Afin d'empêcher des attaques *ab initio* telles que celle décrite ci-dessus, un nouveau logiciel 45
de démarrage a été conçu en remplacement du BIOS, jugé trop peu sûr : le logiciel UEFI (pour « *Unified Extensible Firmware Interface* »). Afin de n'exécuter que des fragments de logiciel considérés comme intègres, UEFI peut mettre en œuvre une fonctionnalité appelée « *Secure boot* », basée sur une méthode d'authentification par chiffrement à clé publique [23]. Le logiciel UEFI contient une clé de déchiffrement maîtresse publique, dont la clé maîtresse privée correspondante est entre les mains du consortium qui promeut l'UEFI.

Tout fabricant de périphérique qui souhaite que son *firmware* ou son système d'exploitation puissent interagir avec le logiciel UEFI doit calculer un condensat [24] du logiciel considéré, puis le soumettre au consortium UEFI, qui chiffrera ce condensat avec sa clé maîtresse privée. Seul le consortium est en mesure d'effectuer ce chiffrement, puisqu'il est le seul à disposer de la clé maîtresse privée. Le condensat chiffré sera alors joint, sur le disque dur, au logiciel en question. Lors du chargement du logiciel par le *Secure boot* de l'UEFI, celui-ci calculera le condensat du logiciel qu'il est en train de charger en mémoire, et déchiffrera la valeur certifiée du condensat du logiciel original grâce à sa clé maîtresse publique. Si les deux condensats sont différents, le logiciel ne sera pas exécuté mais au contraire supprimé de la mémoire vive, puisqu'il diffère de la version certifiée.

Si l'usage de la cryptographie, technique parée des vertus de la robustesse, peut sembler ras- 46
surante de prime abord, il n'augmente pas significativement le niveau de sécurité des ordinateurs qui mettent en œuvre le *Secure boot*. En effet, la certification du logiciel par le consortium UEFI

23. Voir supra section 3.2.

24. Un condensat, ou « *hash* » en anglais, est la valeur calculée par une « fonction de hachage » à partir d'un fichier de données, tel qu'un texte ou un programme. La fonction de hachage est définie de telle sorte que deux fichiers quelconques ont une probabilité extrêmement faible de posséder la même valeur de condensat. Ainsi, si le condensat d'un fichier est connu, il est facile de savoir si ce fichier a été altéré par la suite. Il suffit pour cela de calculer à nouveau son condensat. Si celui-ci est différent de l'ancien, le fichier a été altéré avec certitude. Si les condensats sont identiques, la probabilité que le fichier ait pu être altéré est infinitésimale, et l'on supposera donc que le fichier n'a pas été altéré.

n'est somme toute que purement administrative. Son seul but est de garantir, avec toute la robustesse qu'offre la cryptographie, que le logiciel qui s'exécute est bien celui dont le condensat a été fourni par le fabricant au consortium UEFI. En revanche, ceci n'implique aucunement que ledit logiciel soit exempt de bogues ou de failles. C'est ainsi que n'importe quel auteur de logiciel est susceptible d'obtenir une telle certification, s'il en fait la demande, à charge pour lui de faire passer pour un bogue la faille de sécurité qu'il souhaiterait vouloir activer par la suite [40]. Un moyen encore moins traçable consiste à tirer parti des failles de sécurité existant au sein de pilotes de périphériques produits par des tiers, qui sont courantes du fait de la piètre qualité logicielle de nombre de ces pilotes [40], ou des portes dérobées mises en place par les différents fournisseurs de périphériques.

4.2 La difficulté de détecter les failles

47 La possibilité d'attaquer un système, et la diversité de ces attaques, amène naturellement à s'interroger sur leur détection. En effet, il peut être économiquement justifié de déléguer un traitement à un système informatique, même faillible, dans la mesure où sa subversion serait facile à mettre en évidence et sa compromission n'emporterait pas de conséquences trop dommageables au regard du bénéfice apporté.

48 Une fois leur présence suspectée, les défauts logiciels, pris individuellement, sont relativement simples à mettre en évidence. En effet, le logiciel contient la description exhaustive des traitements qu'il met en œuvre. De plus, il est très souvent facile d'en extraire une copie, à fin d'analyse [25], depuis son support originel. Celui-ci est en général facilement accessible, ne serait-ce que pour pouvoir mettre à jour le logiciel.

49 Il en va tout autrement lorsque les fonctions logiques en cause sont mises en œuvre au sein de composants électroniques dédiés, tels que les processeurs. Si ces composants électroniques numériques ne sont somme toute que du « logiciel pétrifié [26] », leur étude, incluant l'analyse de leurs bogues et failles éventuels, est bien plus coûteuse que pour le logiciel.

4.2.1 Étude en boîte noire

50 Un premier angle d'étude, dit de la « boîte noire », valable tant pour les logiciels que pour les matériels, consiste à inférer le fonctionnement d'un système par le biais de son interaction avec son environnement. En analysant les corrélations entre les données fournies à un composant et les résultats que celui-ci produit en sortie, il est possible, à force d'intuition, de logique et d'opiniâtreté, de déterminer le fonctionnement interne dudit composant.

C'est de cette façon qu'a été étudié le bogue dit « de la division du processeur Pentium™ ». Après que l'on se fut aperçu que l'instruction FDIV [27] du processeur Pentium™ d'Intel renvoyait un résultat dont certaines décimales pouvaient parfois être fausses [36], l'étude des conditions dans lesquelles ces erreurs apparaissaient a permis de comprendre la cause première de ce bogue : la présence de quelques valeurs erronées au sein d'une table de valeurs auxiliaires utilisée par la méthode de calcul de la division [18]. Ces erreurs résultaient d'un bogue dans le programme utilisé pour pré-calculer les valeurs de la table, lors de la phase de conception du processeur.

51 Du fait que les fonctions logiques sont gravées sur silicium, il est impossible de corriger ces bogues matériels. Dans le cas du bogue de l'instruction FDIV, Intel proposa aux utilisateurs mécontents de remplacer leur processeur par une nouvelle version dans laquelle le bogue avait

25. Nous ne débattrons pas ici des conditions juridiques dans lesquelles cette analyse peut être effectuée de façon licite ; nous renvoyons pour cela à notre ouvrage « Droit des logiciels - Logiciels privatifs et logiciels libres » [37].

26. La preuve en étant que le comportement d'un processeur peut être émulé par le biais d'un logiciel reproduisant fidèlement le comportement dudit processeur.

27. Pour « *floating point division* », c'est-à-dire « division de nombres à virgule flottante ».

été corrigé [12], provisionnant à ce titre plus de 400 millions de dollars dans son exercice fiscal. Lorsqu'il n'est pas possible de remplacer le composant défectueux, il faut mettre en place des mécanismes de contournement. Par exemple, dans le cas du Pentium™, il était possible de substituer, à l'utilisation de l'instruction FDIV erronée, l'appel à un sous-programme simulant le résultat de cette instruction de façon logicielle. Il était alors nécessaire de modifier les programmes utilisant l'instruction, pour qu'ils appellent ce sous-programme à la place, l'exécution de ce dernier étant bien plus lente que celle de l'instruction originelle.

4.2.2 Étude du câblage des composants électroniques

Lorsque les fonctions logiques que l'on souhaite étudier sont gravées, sous forme d'assemblage 52
de transistors, au sein d'un composant électronique, la détermination de leur schéma de câblage nécessite le recours à des moyens issus eux aussi au domaine de la physique.

La principale technique utilisée est la radiographie. Les circuits électroniques étant gravés 53
sur leur substrat de silicium au moyen de différents procédés, qui conduisent à des retraits ou à des ajouts de matière, le motif de ces circuits transparaît naturellement sur les clichés du fait des différences d'épaisseur ou de densité qui en résultent. Une fois le cliché obtenu, il revient à l'homme de l'art d'analyser le schéma de câblage mis au jour, afin d'en déduire le fonctionnement et les failles éventuelles du composant [28].

Cette technique est cependant fort coûteuse car, au delà même du matériel nécessaire à l'ob- 54
tention de ces clichés, la compréhension fine du fonctionnement d'un processeur comprenant jusqu'à plus d'un milliard de transistors est une tâche titanesque. C'est ainsi que même un technicien chevronné peut considérer comme une simple originalité de conception certains particularismes dans la mise en œuvre d'une fonction logique, alors que ces particularismes peuvent être exploités de façon malveillante par les personnes qui en sont à l'origine. Les exemples en sont fort rares, car les séquences d'actions conduisant à leur déclenchement sont très inhabituelles. On pourra citer à titre d'illustration le bogue dit « du registre TR4 du processeur i486 » [20], pour lequel une séquence d'instructions très peu courante conduit à ce que le processeur déroute son exécution à une adresse donnée, alors qu'aucune instruction de branchement n'a pourtant été invoquée.

Il est fort probable que ce comportement erroné soit un simple bogue. La complexité de la structure des processeurs fait que, comme pour leurs homologues logiciels « non pétrifiés », ils ne peuvent être *a priori* exempts d'erreurs [21]. Néanmoins, cet exemple illustre parfaitement comment pourrait être construite une porte dérobée au sein d'un processeur moderne : activée par une séquence d'instructions rare et s'appuyant sur l'architecture interne du processeur, elle permettrait d'exécuter un code localisé à une adresse arbitraire, en plaçant le processeur en « mode privilégié [29] ».

La méthode d'analyse par radiographie, qui peut sembler imparable, a cependant pu être 55
mise en défaut par une méthode d'attaque récemment publiée [10].

Lors de la fabrication d'un circuit intégré, le substrat de silicium, qui est nativement un isolant électrique, est enrichi (on dit « dopé ») par l'ajout en très faible quantités d'atomes d'éléments chimiques possédant un surcroît ou un défaut d'électrons, qui le rendent partiellement conducteur. C'est la localisation précise de ces zones de « dopage » qui définit le fonctionnement

28. C'est par ce moyen qu'avait été mise en évidence, il y a plusieurs années, une porte dérobée au sein d'un composant de chiffrement livré par une entreprise étrangère à un intégrateur national en charge de fournir des téléphones chiffrés à notre gouvernement.

29. Le passage en mode privilégié permet au processeur d'accéder à l'intégralité des ressources de l'ordinateur, sans aucune limitation. C'est ce dernier effet qui manque à la séquence décrite pour en faire une porte dérobée imparable.

des transistors, ceux-ci étant construits par juxtaposition de zones de dopages différents. En modifiant l'emplacement de ces zones, il est ainsi possible de perturber le fonctionnement ultérieur des transistors, ceux-ci ne jouant plus leur rôle de commutateur mais restant bloqués dans un état donné (toujours activés ou toujours désactivés).

Les concepteurs de la méthode ont ainsi montré comment, en modifiant l'état de quelques centaines de transistors, il était possible de pervertir le fonctionnement d'un circuit cryptographique, pour en affaiblir le niveau de sécurité [30].

Cette méthode d'attaque est pratiquement indétectable. S'il est possible par radiographie de déterminer la localisation des transistors et leur agencement, il est impossible de savoir, à l'échelle atomique, si le dopage de tel ou tel transistor a été effectué de façon conforme. Seule l'analyse du fonctionnement du circuit peut mettre en évidence un comportement anormal ; encore faut-il pour cela qu'elle soit suffisamment exhaustive.

56 La conséquence la plus remarquable de ce type d'attaque est qu'elle dégrade profondément le niveau de confiance pouvant exister entre le concepteur d'un circuit intégré et le sous-traitant chargé de sa fabrication. Jusqu'à présent, un sous-traitant mal intentionné pouvait toujours implanter des portes dérobées au sein des composants qu'il fabriquait, mais le commanditaire pouvait toujours, par microscopie électronique et / ou radiographie, vérifier la conformité du circuit réalisé avec les plans (appelés « masques ») qu'il avait fournis. Dans le cas présent, ce contrôle devient inopérant.

Du fait que cette attaque ne permet que de modifier le comportement de transistors existants, les possibilités offertes aux attaquants sont limitées, mais gageons que ceux-ci sauraient faire preuve de créativité.

4.2.3 Les erreurs transitoires

57 Les erreurs de conception et les actes de malveillance ne sont pas les seules causes de dysfonctionnement des systèmes informatiques. L'environnement extérieur peut également influer sur eux, en interagissant avec le substrat physique des équipements.

Tel est le cas des rayons cosmiques. Ces particules [31] de très haute énergie, issues d'événements cataclysmiques au sein du soleil ou du cosmos, traversent en permanence la matière [32] qui nous environne, ainsi que la nôtre d'ailleurs. Cependant, il arrive parfois que l'une de ces particules entre en collision avec les particules qui constituent la matière, y déposant alors son énergie. C'est ainsi que l'impact d'un rayon cosmique au sein d'un composant électronique peut conduire à la modification d'une ou plusieurs valeurs binaires stockées au sein de ce composant [50].

58 Ce phénomène, appelé « *bit flip* » en anglais, est devenu problématique avec la généralisation et la miniaturisation des ordinateurs. Dans les grands centres de données, des volumes considérables sont occupés par les mémoires des serveurs informatiques, augmentant d'autant la probabilité de collision avec un rayon cosmique. La miniaturisation, quant à elle, en réduisant la quantité d'énergie utilisée pour la représentation d'une valeur binaire, augmente la probabilité qu'un faible apport d'énergie puisse conduire à la modification de cette valeur. Des études conduites par IBM dans les années 1990 indiquent que les mémoires vives des ordinateurs étaient sujettes à une erreur par 256 mégaoctets et par mois, dues aux rayons cosmiques [50].

30. La technique consistant à créer des transistors non fonctionnels n'est pas nouvelle. Elle est déjà utilisée par les concepteurs de circuits intégrés, dans un but d'obfuscation. Il s'agit de compliquer le travail des personnes souhaitant comprendre le fonctionnement du circuit, en lui ajoutant des ensembles de transistors non fonctionnels, qui complexifient son schéma de câblage sans modifier son fonctionnement.

31. Nous utiliserons, pour décrire le phénomène, la représentation corpusculaire de ces « rayons », en vertu de la dualité onde-particule.

32. Celle-ci étant, en fait, majoritairement constituée de vide, tant entre les atomes qu'entre les noyaux atomiques et les électrons.

Afin de lutter contre ce phénomène, les constructeurs de mémoires informatiques ont développé des systèmes redondants, basés sur des codages particuliers de l'information, dits « codes auto-correcteurs ». En s'appuyant sur certaines propriétés mathématiques, il est possible, sans trop augmenter le niveau de redondance et donc le coût de la mémoire, de pouvoir détecter et corriger une erreur unique se produisant sur une valeur binaire, et détecter deux erreurs sans pouvoir les corriger [33]. En testant et en corrigeant régulièrement les erreurs éventuelles, le risque de « triple erreur », c'est-à-dire d'erreur non détectable, est jugé suffisamment faible pour les logiciels non critiques.

Pour autant, certaines parties des ordinateurs ne sont pas protégées. C'est le cas des processeurs eux-mêmes, dont la surface a été jugée suffisamment petite, en comparaison des mémoires, pour considérer que leur probabilité d'être touchée était négligeable. Leur protection n'est de toute façon pas possible dans tous les cas, car certains calculs ne peuvent être menés autrement qu'en manipulant les valeurs binaires originales, et non leur codage sous forme redondante. Pour minimiser ce type de problèmes, il faut alors maintenir plusieurs copies distinctes de l'information en mémoire, et mener plusieurs calculs redondants sur chacune de ces copies, puis vérifier ensuite que ces calculs ont donné le même résultat.

Parce que les *bit flips* pourraient avoir des conséquences extrêmement graves au sein de systèmes critiques tels que les logiciels équipant les centrales nucléaires, les avions ou les voitures, des normes industrielles très strictes ont été mises en place au sein de ces industries, voir *infra*.

Des erreurs transitoires peuvent également être causées par le vieillissement des équipements. 59
C'est le cas des court-circuits causés par l'altération des soudures qui, avec le temps, développent des filaments (appelés « vibrisses », ou « *whiskers* », en anglais), qui peuvent à la longue créer des ponts électriques entre soudures voisines. C'est aussi le cas de l'électro-migration des atomes au sein des circuits intégrés : tout comme les galets sont roulés par le courant du ruisseau, les atomes sont déplacés par le flot d'électrons, conduisant parfois à rompre les connexions au sein de ces circuits.

Si nous l'avons mentionné dans un but d'exhaustivité, nous ne considérerons pas plus avant ce type d'erreurs transitoires, qui peut être évité par un renouvellement régulier des matériels. Ce renouvellement renchérit cependant d'autant la mise en œuvre du « vote électronique ».

5 Portée de la certification

Bien évidemment, en dehors de la tentation ou de l'obligation légale qui peut lui être faite 60
d'installer des portes dérobées, le concepteur d'un système informatique a tout intérêt à ce que celui-ci fonctionne parfaitement. Les conséquences d'une défaillance logicielle peuvent en effet être très graves, et mettre en danger non seulement la vie de ses clients et de la population, mais également celle de son activité économique. Ceci a conduit au développement de méthodologies et d'outils destinés à garantir la plus grande qualité logicielle possible. Cependant, aucune des techniques disponibles ne peut garantir la bonne exécution d'un logiciel et, par conséquent, la sincérité d'un processus électoral dématérialisé.

33. L'idée consiste à représenter une séquence de valeurs binaires, ou « mot », par un mot de plus grande taille (d'où le surcoût en mémoire), de telle sorte que toute modification d'une unique valeur binaire de ce nouveau mot plus long conduise à une configuration non valide, et donc détectée comme erronée. Par exemple, dans la langue française, « POMME » est une configuration de lettres valide. Si une lettre est changée par erreur, on peut obtenir des configurations telles que « PIMME » ou « POSME », reconnues comme invalides, et que l'on pourra corriger. Si deux lettres sont changées, on pourra tomber sur « PISME », également reconnue comme invalide, et si trois lettres sont changées, on pourra tomber sur « PISTE », qui ne sera pas reconnue comme une erreur. Pour plus de précisions, voir par exemple [45].

5.1 Normes et contrôles de qualité

61 Une première catégorie de méthodes vise à accompagner les équipes de développement dans l'écriture de leur code informatique. Elles se fondent sur l'adoption de référentiels de bonnes pratiques de développement, conçus de façon empirique, que les programmeurs doivent respecter. C'est par exemple le cas des normes MISRA dans le domaine de l'industrie automobile [35]. En renfort de ces normes ont été créés des outils logiciels qui permettent de vérifier de façon automatique, lorsque c'est techniquement possible, leur respect au sein du logiciel produit.

Malheureusement, dans nombre de domaines, ces normes ne sont qu'indicatives. Faute de contrôle réglementaire, les industriels peuvent très bien décider de n'appliquer que leurs propres règles en matière de qualité, et rien ne garantit qu'il les respectent. C'est par exemple le cas dans le secteur automobile, comme l'a mis en lumière le procès opposant à un constructeur automobile les proches d'une victime dont la voiture avait accéléré au lieu de freiner sur une bretelle d'autoroute. L'analyse du logiciel embarqué du véhicule a mis en évidence plus de 80.000 violations des normes MISRA-C, ainsi que des violations des règles internes du constructeur, pourtant bien plus souples. Les causes en étaient nombreuses : absence de tout contrôle de qualité, absence de formation des personnels et des sous-traitants aux méthodologies de qualité logicielle requises, et impossibilité d'évaluer le logiciel fourni par les sous-traitants, pour cause de secret industriel. Il en a résulté un ensemble de logiciels présentant de nombreux bogues et une très faible tolérance aux pannes. L'absence de redondance des dispositifs matériels et logiciels rendait l'ensemble des systèmes de régulation du véhicule vulnérables à une erreur unique (« *single point of failure* », en anglais) : un seul *bit flip* pouvait conduire à l'accélération incontrôlée dont la survenue était l'objet du procès [5, 6]. Ce cas illustre magistralement qu'en l'absence d'obligation réglementaire, la tentation de faire des économies en temps et en ressources pénalisera toujours la qualité des logiciels.

62 Pourtant, dans bien des pays dont la France, les dispositions réglementaires portant sur l'agrément des « machines à voter » n'imposent aucunement la mise en œuvre par le fabricant de processus normalisés de développement logiciel, ni de certification de la qualité de ce dernier selon des normes industrielles. La raison en est triviale : soumettre à de telles contraintes le processus de développement de ces logiciels en renchérirait le coût d'une façon telle que très peu de municipalités pourraient les acquérir.

63 L'absence de normes de développement strictes ne peut que conduire à la survenue de nombreux bogues. Certains peuvent sembler bénins et non susceptibles d'influer sur le déroulement de l'élection. Ainsi, avec le système mis en œuvre pour l'élection de 2006 à l'Assemblée des Français de l'étranger, a-t-il été constaté que, lorsqu'on recherchait un électeur par son nom et son prénom, le système de gestion de la liste d'émargement indiquait que cet électeur n'existait pas, alors que lorsqu'on effectuait cette recherche uniquement sur le nom, l'électeur était bien trouvé [38]. D'autres sont bien plus graves. C'est ainsi qu'en Belgique, lors des élections régionales de 2014, dans plusieurs cantons, les décomptes des voix de préférence aux candidats des listes en présence n'ont pu être donnés [23]. Aux États-Unis, il est arrivé que certains systèmes totalisent des nombres de voix négatifs [25].

64 En Belgique encore, en 2003, il a été constaté au bureau de Schaerbeek une surcroît de 4096 voix [34] au profit d'un membre d'une liste, par rapport au nombre de suffrages recueillis par la liste elle-même. Après analyse du système, et aucune cause directe n'ayant pu être mise en évidence, la conclusion de la commission d'enquête a été que cette erreur « *pouvait probablement être attribuée à une inversion spontanée d'une position binaire dans la mémoire vive du PC* » [42].

34. Le nombre 4096 est très parlant pour un informaticien. Il s'agit d'une puissance de deux, c'est à dire un nombre qui s'écrit en binaire au moyen d'un unique bit à 1, tous les autres étant égaux à 0. De fait, une différence de 4096 entre deux nombres signifie qu'ils ne diffèrent dans leur écriture que d'un seul bit.

Cet événement appelle plusieurs commentaires. Premièrement, si l'explication du *bit flip* est la bonne[35], il illustre de façon exemplaire que la miniaturisation de l'information, désirable en termes de performance, la rend plus fragile. Alors qu'un rayon cosmique est suffisant pour changer le résultat d'un scrutin de 4096 voix[36], la probabilité d'occurrence des transmutations atomiques ou sauts quantiques nécessaires au changement du nom porté par un bulletin papier est incommensurablement plus faible, car la disparition d'une molécule d'encre ne rendra pas le bulletin illisible. Deuxièmement, si ce scrutin n'avait pas comptabilisé séparément suffrages de liste et suffrages de préférence individuels, ou encore si le nombre des voix indûment apportées au candidat n'avait pas dépassé le nombre de voix recueillies par sa liste, il n'aurait pas été possible de détecter l'erreur, ni de corriger le scrutin a posteriori. En fait, rien ne dit que, dans des conditions similaires, des scrutins faussés n'ont pas été validés. Troisièmement, il fournit un exemple supplémentaire de la méconnaissance des normes industrielles destinées à protéger les systèmes critiques contre les *bit flips*. Le niveau de qualité des logiciels mis en œuvre au sein des « ordinateurs de vote » n'est pas meilleur que celui de jeux vidéo, voire souvent moindre[37]. Quatrièmement, si l'explication du *bit flip* n'est en fait pas la bonne, cet exemple démontre que le degré de complexité du système mis en œuvre dépasse la compétence des personnes les plus à même de le comprendre, ce qui n'est pas moins inquiétant.

5.2 Certification formelle

Les normes et contrôles de qualité, s'ils permettent de réduire les risques de bogues, ne 65
peuvent en garantir l'absence. Face à ce problème et aux enjeux de sécurité que cela représente pour les systèmes critiques, de nombreuses équipes de recherche se sont attachées à développer des méthodes visant à prouver mathématiquement la correction des programmes informatiques. Ces méthodes mathématiques, dites de « vérification formelle », visent à garantir que les propriétés que le logiciel étudié est censé posséder ne sont pas violées au cours de son exécution [49]. Par exemple, on attendra d'un logiciel de contrôle de sas d'entrée qu'il ne permette pas que les deux portes dudit sas soient déverrouillées en même temps, quelles que soient les manipulations effectuées par les usagers sur les commandes d'ouverture.

Pour ce faire, on modélisera mathématiquement la propriété en question, sous la forme d'une expression logique mathématique[38]. On s'attachera alors à vérifier que, quel que soit le chemin que prendra le déroulement du programme, cette expression soit toujours vérifiée. Le nombre de chemins d'exécution possible étant très important, la tâche de vérification est dévolue à des logiciels dédiés, conçus par les équipes de recherche elles-mêmes, et qui prennent comme donnée le logiciel à vérifier. Même dans ce cas, le nombre de chemins à tester peut être l'objet d'une « explosion combinatoire », du fait que les chemins peuvent boucler sur eux-mêmes et doivent donc être parcourus de nombreuses fois selon des séquences différentes. Il en découle que les logiciels de preuve de programmes ne peuvent explorer l'ensemble des chemins en un temps raisonnable, et ne peuvent par conséquent garantir l'absence de chemin conduisant à une violation des propriétés testées. L'usage de ces logiciels est donc limité à de petits programmes, écrits dans des langages de programmation peu complexes[39].

Plusieurs équipes de recherche, désireuses de montrer l'utilité pratique de leurs travaux, ont 66
pris le « vote électronique » comme application de leurs méthodes de preuve de programmes, avec

35. En effet, l'hypothèse d'une malveillance, bien que moins probable, ne peut aucunement être écartée.
36. Ou de n'importe quelle autre puissance de deux, d'ailleurs, même les plus grandes.
37. Les jeux vidéo faisant l'objet de nombreuses heures de test par des personnels dédiés, les « bêta-testeurs ».
38. Par exemple, dans le cas précité, « ouvert(porteA) et ouvert(porteB) = Faux », puisque jamais les deux portes A et B du sas ne doivent être ouvertes en même temps.
39. Par exemple, un sous-ensemble du langage C excluant l'usage des pointeurs, les alias entre pointeurs étant une cause d'explosion combinatoire.

comme objectif affiché de le « sécuriser ». Du fait de la complexité des systèmes informatiques considérés, ces derniers ne peuvent cependant pas être étudiés dans leur globalité. Les travaux de certification ne s'appliquent donc qu'à certains éléments du système, ou bien à la modélisation de son fonctionnement général, sans aborder les détails de mise en œuvre.

67 C'est ainsi qu'une équipe de recherche a pu prouver que le code source d'un module logiciel d'urne chiffrée était conforme à sa spécification, tant que la mémoire à écriture unique destinée à stocker les suffrages n'autorise effectivement pas la réécriture d'informations [13]. Une autre a affirmé pour sa part que la méthode de vote qu'elle proposait garantissait simultanément le secret et la sincérité du scrutin [3]. Ce deuxième résultat a de quoi surprendre le lecteur non averti : le Graal du « vote électronique » serait-il à portée de main ? Au risque de décevoir le lecteur, la réponse est négative. La rédaction de l'article en question illustre en revanche magistralement en quoi même les annonces de scientifiques doivent être prises avec beaucoup de réserves, lorsqu'elles sont extraites de leur contexte.

L'article décrit successivement trois variantes d'un processus de vote, dont nous n'allons présenter que la troisième, puisque c'est celle que les auteurs considèrent comme la plus fiable. Elle consiste, pour chaque électeur, à choisir secrètement un nombre, puis à le communiquer au système de vote en même temps que son suffrage. L'ensemble des suffrages est alors affiché sur un écran, chaque nombre étant mis en regard du suffrage correspondant. Chaque électeur est donc à même de vérifier individuellement sur l'écran que son choix a bien été pris en compte en lisant le suffrage exprimé en regard du nombre qu'il a choisi, et tous peuvent vérifier collectivement le résultat de l'élection en recomptant l'ensemble des suffrages exprimés pour chaque candidat. De plus, aucun électeur ne peut, en consultant l'écran, savoir qui a voté pour qui. Le seul risque est que plusieurs personnes choisissent le même nombre, ce qui empêcherait ces personnes d'affirmer que leur vote a bien été pris en compte, si tous ne votaient pas de la même manière. Cependant, ce cas de « collision » est rare si les nombres choisis comportent suffisamment de chiffres.

Le problème de cette étude est qu'elle ne considère pas la question de la coercition. Puisque l'électeur a toute liberté pour choisir son nombre, il peut tout à fait avoir été contraint de fournir un nombre communiqué à l'avance par un tiers qui le menace ou le soudoie. Ce dernier, en regardant l'écran, peut alors savoir avec certitude si l'électeur a voté conformément à ses instructions, l'absence dudit nombre à l'écran indiquant que l'électeur a désobéi. Le dispositif présenté, s'il garantit le secret vis-à-vis des autres électeurs, ne garantit pas la liberté du vote. La cause en est que toute information publique liant l'électeur à son suffrage peut être mise à profit par un tiers malveillant.

68 D'autres travaux théoriques s'attachent à déterminer sous quelles conditions un dispositif de « vote électronique » peut vérifier simultanément plusieurs propriétés voulues, telles que le secret du scrutin, sa vérifiabilité *a posteriori* par les électeurs, ou encore la garantie d'absence de traces dont un tiers pourrait tirer parti pour connaître le suffrage des électeurs. C'est ainsi qu'il est possible de prouver qu'un système de vote ne peut offrir simultanément la vérifiabilité par les électeurs et le secret, à moins que tous les électeurs enregistrés ne votent [16].

Cependant, les résultats énoncés ne sont ici encore que théoriques. Ils concernent des systèmes abstraits, éventuellement conçus pour résister à des attaques de types variés, telles que la volonté de l'autorité organisatrice de modifier le résultat du scrutin. Cependant, lesdites attaques ne peuvent être contrées qu'à l'intérieur d'un environnement strictement contrôlé, au sein duquel le logiciel est censé fonctionner loyalement. Or, comme nous allons le voir, il ne peut exister aucune garantie à ce sujet.

5.3 Périmètre de la certification

Nous avons déjà exposé en quoi la complexité des systèmes informatiques rend impossible 69
l'audit empirique de l'ensemble d'un tel système. En pratique, seuls sont réalisés des audits des logiciels de « vote électronique » proprement dits [17, 29, 32], laissant dans l'ombre l'ensemble des matériels et des logiciels qui les environnent.

Il en va de même des certifications théoriques que l'on peut vouloir mettre en œuvre : la majorité d'entre elles portent sur le logiciel de « vote électronique » en tant que tel, seuls quelques auteurs s'intéressant aux logiciels auxiliaires contribuant à la construction du programme qui sera réellement exécuté [33]. L'étude du système d'exploitation est, pour sa part, actuellement hors de portée de ces outils d'analyse.

La limitation intrinsèque du périmètre de l'audit et / ou de la certification permet à un at- 70
taquant de s'intercaler de façon transparente entre l'usager et la partie certifiée du système, en marge de ce périmètre, afin d'intercepter les informations entrant et sortant de celui-ci. Une démonstration très élégante d'une telle « encapsulation » silencieuse d'un logiciel au sein d'un environnement destiné à le contrôler, a été faite par la technique d'attaque appelée « BluePill » [40]. Cette attaque s'appuie sur le mécanisme de « virtualisation », présent au sein des processeurs modernes, qui permet de faire croire à un système d'exploitation complet qu'il s'exécute nativement sur le processeur de l'ordinateur, alors qu'il est encapsulé dans une « machine virtuelle » qui permet son analyse depuis l'extérieur de cette « bulle ».

Cette technique d'encapsulation permet de violer de façon invisible les propriétés revendiquées 71
du logiciel de « vote électronique ». Par exemple, en encapsulant le logiciel de saisie du choix de l'électeur au sein d'une machine virtuelle, il est possible d'intercepter au vol les choix entrés par l'électeur, et de fournir un choix altéré au logiciel. De même, lorsque ce dernier voudra rendre compte à l'électeur de son choix, en affichant le nom du candidat sélectionné par malice, cette information sera interceptée et le nom qui apparaîtra à l'écran sera celui que l'électeur avait initialement saisi.

Dans le cas où l'ensemble des suffrages est affiché sur un dispositif situé hors du périmètre de falsification de la machine virtuelle, il ne sera pas possible d'user de cette technique pour falsifier le suffrage de l'électeur, puisque celui-ci pourrait s'en rendre compte en consultant ledit dispositif d'affichage. En revanche, le choix de l'électeur aura bien été intercepté, à la manière d'un « *keylogger*[40] », ce qui viole la propriété du secret du scrutin. De plus, comme nous l'avons vu dans la section précédente, de tels modes de scrutin permettent la coercition, ce qui les disqualifie d'origine.

6 Chaînes de confiance

La robustesse du processus démocratique repose sur la capacité des citoyens à pouvoir en 72
contrôler eux-mêmes la régularité. Cependant, lorsque le corps électoral est important, aucune personne ne peut à elle seule assister à l'ensemble des opérations, du simple fait qu'elle ne peut

40. On appelle ainsi, dans le jargon technique anglophone, un logiciel qui enregistre secrètement les frappes de l'usager. Les plus évolués enregistrent également les déplacements de la souris et effectuent des captures d'écran à chaque clic. De tels logiciels malveillants, le plus souvent installés par le biais de virus informatiques, servent à capturer les mots de passe des usagers et / ou leurs informations bancaires, au moment où ils se connectent sur des sites d'intérêt.

être présente simultanément dans deux bureaux de vote[41, 42]. La confiance de chaque électeur en la sincérité du processus électoral ne peut alors être acquise que de façon collective, au moyen d'un processus de certification distribué.

6.1 Assesseurs et délégués

73 Tout électeur ne pouvant assister à l'intégralité du processus de vote doit forger son opinion sur la base d'informations collectées par des tiers. Se pose alors la question du degré de confiance que l'on peut accorder à ceux-ci. La solution utilisée dans bien des activités humaines consiste à s'appuyer sur des réseaux de confiance : on aura plus tendance à croire une personne qui nous a été recommandée par une connaissance dont on a pu estimer la sûreté de jugement, ou avec laquelle on partage ouvertement des valeurs communes.

Ces pratiques ont été reprises avec profit dans le Code électoral. Celui-ci définit le rôle des assesseurs, désignés par les candidats, et des délégués, nommés par les partis politiques. Chacun des assesseurs et des délégués a pour mission de défendre les intérêts du candidat au nom duquel il a été investi, en veillant à ce que ceux-ci ne soient pas lésés pendant le déroulement de l'élection. Grâce au contrôle réciproque qu'ils exercent les uns sur les autres, aucun d'entre eux ne peut agir de façon nuisible aux intérêts des autres candidats. Il en résulte l'instauration d'un équilibre entre toutes les parties, qui concourt au bon fonctionnement du bureau de vote.

Tout électeur peut donc supposer, avec une très forte probabilité, que dans chaque bureau de vote il se trouvera une ou plusieurs personnes ayant les mêmes intérêts que lui, qui veilleront sur le bon déroulement du processus électoral. Ces personnes, une fois le scrutin clos, surveilleront le décompte des suffrages, et retransmettront les résultats de chaque bureau au candidat ou à ses représentants au niveau des sections, fédérations, et autres instances des partis, qui les totaliseront de façon indépendante des services officiels en charge de la proclamation des résultats. Il existe donc, depuis l'électeur jusqu'à la personne totalisant l'ensemble des résultats pour son candidat, une chaîne de confiance qui réduit considérablement le risque qu'une de ces personnes agisse de façon contraire aux intérêts de l'électeur.

74 Du fait de l'existence de chaînes de confiance au bénéfice de chacun des candidats, le système électoral est caractérisé par une très forte redondance. De multiples acteurs participent en parallèle à la surveillance du processus de vote et à la totalisation des résultats, ce qui minimise le risque d'erreur ou de malveillance. Les principes mis en œuvre dans ce cadre sont les mêmes que ceux présidant à la conception des systèmes informatiques critiques.

75 C'est également au moyen de chaînes de confiance que se règle le cas des électeurs ne pouvant se rendre au bureau de vote. Le mécanisme de la procuration permet à un électeur de déléguer son suffrage à un tiers de confiance. Celle-ci peut être un proche, qui respectera le souhait de l'électeur par loyauté même s'il ne vote pas comme lui. Ce peut également être l'un des militants du candidat choisi par l'électeur, désigné par le parti auquel il s'est adressé pour l'aider à établir sa procuration. Dans ce cas, l'électeur peut avoir une certitude encore plus grande sur le fait que son mandataire votera pour le candidat qu'il a choisi, mais au prix du secret de son suffrage.

6.2 Conséquences de la dématérialisation du processus électoral

76 Dans le cas du vote traditionnel, tant les électeurs que les assesseurs et les délégués peuvent constater le bon fonctionnement du processus électoral grâce à leurs propres sens et sans aucun

41. Ceci ne vaut bien sûr que pour le vote en bureau. Dans le cas du « vote électronique » à distance, l'ordinateur totalisateur est bien localisé en un seul lieu, mais l'observation de son fonctionnement est impossible, pour les raisons évoquées plus haut.

42. Et encore, sur l'Agora, l'introduction de dispositifs techniques comme le *klérotérion* pouvait-il conduire à cacher aux yeux des électeurs le processus de sélection des candidats, voir [41].

intermédiaire. La simplicité de ce processus est un élément essentiel de la confiance que les citoyens peuvent y apporter. *A contrario*, plus le nombre d'intermédiaires est important entre la personne constatant la réalité d'une opération et celle qui en est informée, et moins l'information peut être considérée comme fiable, à moins que ces personnes ne soient liées par une communauté d'intérêts. C'est le même désir de voir leur candidat gagner qui lie l'électeur et les personnels travaillant au nom de ce candidat.

Or, la dématérialisation, ne serait-ce que partielle, du processus électoral conduit à rompre 77
l'ensemble des chaînes de confiance propres à chaque candidat. En effet, elle conduit à insérer, en chacune d'elles, un maillon technique conçu par des tiers absolus n'appartenant à aucun réseau de confiance des parties en présence.

Comme nous l'avons vu plus haut, la complexité d'un système informatique est telle que son étude exhaustive, dans le but d'en certifier le bon fonctionnement, est impossible à mener sans disposer de ressources considérables en termes de temps et de moyens techniques et humains. Qui plus est, cette étude devrait être menée sur chacun des systèmes effectivement mis en place dans chaque bureau. Rien ne dit en effet que l'exemplaire du système utilisé par les électeurs au sein d'un bureau de vote est bien strictement identique à celui qui a été mis à la disposition des experts auditeurs de l'administration concernée.

C'est pour ces mêmes raisons que la mise à disposition des codes sources du logiciel de « vote électronique » à l'ensemble des électeurs n'offre strictement aucune protection. Rien ne dit que le logiciel qui s'exécute au sein des machines est bien celui dont le code source a été fourni, et qu'il ne sera pas perverti à l'exécution par l'injection de code malicieux, comme décrit en section 4.1.2.

Un inconvénient supplémentaire des systèmes de « vote électronique » est que leur défaillance 78
met en danger l'ensemble du processus électoral pour lequel ils sont utilisés, si les données qu'ils contiennent ne peuvent être récupérées. Ils constituent, de ce point de vue, une vulnérabilité à une erreur unique (« *single point of failure* »), d'un niveau de complexité bien plus élevé que le mécanisme du volet obturateur de l'urne, par exemple. Ainsi, en plus d'empêcher toute vérification du processus électoral, ces systèmes en affaiblissent la robustesse.

6.3 Sur le rôle des assesseurs

Comme nous l'avons vu, le rôle des assesseurs est de témoigner en personne du bon déroulement 79
du scrutin et du respect des principes fondamentaux auquel celui-ci doit répondre. Le « vote électronique » ne leur permet aucunement de tenir ce rôle.

La destruction de la fonction d'assesseur est encore plus évidente dans le cas de scrutins organisés à distance. C'est ainsi que, pour le vote par correspondance électronique mis en place dans le cadre des élections de 2006 à l'Assemblée des Français de l'étranger, les assesseurs ne se trouvaient même pas dans les locaux du prestataire de services informatiques en charge de l'exploitation du système centralisé de totalisation des votes. Ils étaient hébergés dans un bureau situé à plus de 700 kilomètres de là, dans lequel l'exploitant avait installé les équipements censés leur permettre d'accomplir leur mission. Il s'agissait, d'une part, d'un écran de télévision montrant quelques ordinateurs ronronnant dans une salle informatique et, d'autre part, d'une console permettant d'interroger la liste d'émargement du système [38].

La dématérialisation de l'information place l'ensemble des participants au processus de vote 80
dans la situation de la caverne de Platon : personne ne peut plus faire confiance à ses sens pour attester de la réalité d'actions immatérielles, se produisant au sein d'équipements informatiques dont seule l'existence physique peut être attestée, et dont les effets ne sont perceptibles qu'à travers d'autres dispositifs techniques. Les assesseurs n'ont en fait plus accès qu'à l'ombre de l'ombre, les logiciels d'interrogation du système de « vote électronique » étant eux-mêmes

faillibles [43].

7 Portée de la fraude

81 Nul dispositif technique ou procédé ne peut prétendre à l'infaillibilité. Le choix de recourir ou non à son usage est donc guidé par un ensemble de critères, pondérés de façon plus ou moins importante selon le contexte. En dehors du coût, les deux principaux critères habituellement considérés sont la robustesse et le risque encouru en cas de dysfonctionnement, que celui-ci résulte d'une panne ou d'une action malveillante. Dans le cas du processus électoral, ce dernier critère peut être évalué en considérant la portée de la fraude qu'un dispositif autorise. Nous désignons par ce terme la capacité de nuisance d'une personne malveillante souhaitant subvertir le processus électoral.

82 La portée de la fraude est le principal critère restrictif considéré dans la définition du processus électoral. Nul doute que c'est lui qui a guidé le législateur dans la limitation du nombre de procurations donc un électeur peut être porteur. Ainsi, le mandataire qui vote en France ne peut détenir qu'une seule procuration établie en France. Il peut en recevoir deux si au moins l'une de ces procurations a été établie à l'étranger, et trois procurations s'il participe au scrutin dans un centre de vote ouvert à l'étranger. Cette latitude supplémentaire laissée aux mandataires votant à l'étranger ou recevant des procurations issues de résidents à l'étranger est destinée à faciliter l'expression du suffrage d'électeurs ne pouvant se rendre facilement à leur bureau de vote. Elle est cependant fortement contrainte, afin qu'un mandataire indélicat ne puisse fausser le scrutin de façon importante en se livrant à des manœuvres illicites destinées à obtenir le plus grand nombre possible de procurations.

83 Nombreux sont les cas rapportés de personnes ayant entrepris de fausser le résultat d'une élection traditionnelle [44]. Bien des techniques ont été utilisées, allant des bulletins cachés dans la chaussette au doigt encré pour annuler certains bulletins, jusqu'à la substitution d'urnes une fois le scrutin clos. Cependant, dans tous les cas, la fraude est circonscrite au périmètre physique que peut couvrir le fraudeur, qui est limité par la capacité de déplacement de ce dernier.

84 Il en va tout autrement des scrutins dématérialisés. Du fait que ceux-ci font usage de logiciel, la capacité de frauder bénéficie de la facilité de copie associé à celui-ci. Un unique fraudeur peut alors concevoir, de chez lui, un logiciel de fraude qui pourra être copié en autant d'exemplaires que nécessaire. C'est le cas par exemple des failles implantées au sein des *firmwares* et des systèmes d'exploitation, qui deviennent exploitables dès que l'industriel a mis à jour ceux-ci sur les ordinateurs qu'il va livrer.

85 Ce risque est encore plus évident dans le cas des scrutins à distance, pour lesquels l'usager télécharge sur son propre ordinateur, généralement très peu sécurisé, le logiciel qui recueillera son suffrage. Lors du « vote » par Internet mis en place pour les Français de l'étranger lors des élections législatives de 2012, des informaticiens soucieux de la démocratie ont démontré par la pratique comment reprogrammer ledit logiciel de recueil afin d'en altérer le fonctionnement [22, 39]. Il suffit donc d'infecter sur grande échelle les machines des électeurs, au moyen de virus adaptés, afin que le logiciel de recueil qui sera exécuté soit le logiciel falsifié, pour altérer massivement, et de façon totalement invisible, le résultat d'une telle élection. Peut-être cela a-t-il même déjà été fait ; nous ne pouvons pas le savoir.

43. Dans l'exemple pré-cité, lorsque les assesseurs effectuaient, sur le système d'interrogation à leur disposition, la recherche d'un électeur par son nom et son prénom, le système indiquait que l'électeur n'était pas présent sur la liste d'émargement, alors que lorsqu'ils effectuaient cette recherche uniquement sur le nom, l'électeur était bien trouvé.

44. Qui n'incluent évidemment pas les cas de ceux ayant réussi à ne pas se faire prendre.

L'usage de systèmes dématérialisés pour les scrutins à distance n'apporte donc aucun avantage par rapport au vote par correspondance, déjà autorisé. En effet, la portée de la fraude est considérablement plus faible dans le cas du scrutin sur support papier, pour lequel un attaquant devrait tracer l'ensemble des flux de courrier arrivant du monde entier. 86

8 Conclusion

La fiabilité d'un système est celle de son maillon le plus faible. Remplacer un processus simple, robuste et perceptible par un processus plus complexe, plus fragile, et imperceptible n'a de sens que si les avantages qu'on en retire sont supérieurs aux inconvénients. Or, la simplicité, la robustesse et la perceptibilité sont justement les principes essentiels qui doivent caractériser un processus électoral, et qui ne peuvent être négociés. 87

Il n'est donc guère surprenant que, dans nombre de pays, il ait été mis un terme aux diverses expérimentations de « vote électronique » [1]. Dès le début de l'année 2004, le FVAP (« *Federal Voting Assistance Program* »), l'agence étatsunienne en charge du vote des personnels militaires et des citoyens résidant à l'étranger, avait commandé un rapport d'audit sur le système de « vote électronique » SERVE qui allait bientôt être déployé [32]. Sur la base de ce rapport très détaillé, le FVAP a définitivement arrêté son programme. Ici encore, il ne s'agissait pas d'une question de moyens (les États-Unis n'en manquent assurément pas) ou de faiblesse cryptographique, mais bien de principe. 88

Les décisions d'arrêt du « vote électronique » ont parfois été hâtées par les tribunaux. C'est ainsi que la Cour constitutionnelle fédérale d'Allemagne a décidé en mars 2009 que l'usage de dispositifs numériques pour les élections était inconstitutionnel pour les dix années à venir [11, 41]. 89

En France, le Conseil constitutionnel s'est toujours prononcé en faveur de la validation de élections menées au moyen de ces dispositifs, en dépit des multiples irrégularités constatées, y compris celles contraires au Code électoral quant à la possibilité de rattacher l'électeur à son suffrage. Le Tribunal d'instance de Brest a cependant déjà annulé en 2012 les résultats d'un « vote électronique » mis en œuvre dans le cas d'élections professionnelles [15]. Face à la récurrence des problèmes rencontrés, le législateur s'est saisi de la question, mais de façon encore timide. Dans un récent rapport sur la question, les sénateurs recommandent la suppression de toute subvention à l'acquisition et à l'entretien de ces systèmes, ainsi que le maintien du moratoire sur l'équipement de nouvelles communes, afin d'éteindre peu à peu les foyers d'utilisation du « vote électronique » au sein des bureaux de vote. Ils avalisent cependant l'usage du « vote » par Internet, dont nous avons pourtant montré que c'est celui qui offre le moins de garanties [1].

À la lumière de nos précédents travaux, il nous était apparu que le seul avantage du « vote électronique » était de pouvoir donner rapidement un résultat totalement dénué de fiabilité. Les récentes péripéties électorales ayant eu lieu en Belgique [23] nous conduisent à modifier cette conclusion, afin d'en supprimer le bénéfice de la vitesse. Il ne nous semble donc pas opportun de retirer les guillemets du terme « vote électronique », mais plutôt de retirer de la circulation les systèmes qui prétendent le mettre en œuvre, tant qu'une avancée significative de la science[45] ne sera pas de nature à permettre au législateur de reconsidérer cette interdiction. 90

Références

[1] A. Anziani et A. Lefèvre, Rapport d'information sur le vote électronique, fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement

45. Et non de la seule technique.

et d'administration générale, n° 445, enregistré à la Présidence du Sénat le 9 avril 2014. http://www.senat.fr/rap/r13-445/r13-4451.pdf .

[2] J. Appelbaum, J. Horchert et C. Stöcker, Shopping for Spy Gear : Catalog Advertises NSA Toolbox, Spiegel Online, 29 décembre 2013. http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html .

[3] M. Arnaud, V. Cortier, C. Wiedling, Analysis of an Electronic Boardroom Voting System, actes de E-Voting and Identify, LNCS 7985, Springer-Verlag, 2013, p. 109-126, DOI 10.1007/978-3-642-39185-9_7. Version préliminaire de l'article disponible sous : http://www.loria.fr/∼cortier/Papiers/ACW-voteCNRS-VoteID2013.pdf .

[4] J. Ball, J. Borger et G. Greenwald, Revealed : how US and UK spy agencies defeat internet privacy and security, The Guardian, 6 septembre 2013. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security .

[5] M. Barr, déposition devant la cour, affaire Bookout & Schwarz c/ Toyota, CJ-2008-7969, District Court of Oklahoma County, 14 octobre 2013. http://www.safetyresearch.net/Library/Bookout_v_Toyota_Barr_REDACTED.pdf .

[6] M. Barr, diapositives utilisées pendant la déposition devant la cour, affaire Bookout & Schwarz c/ Toyota, CJ-2008-7969, District Court of Oklahoma County, 14 octobre 2013. http://www.safetyresearch.net/Library/BarrSlides_FINAL_SCRUBBED.pdf .

[7] R. W. Barton, Hosting Backdoors in Hardware, blog Ksplice d'Oracle, 26 octobre 2010. https://blogs.oracle.com/ksplice/entry/hosting_backdoors_in_hardware .

[8] BBC News, Mafia turns to 3G video phones, 16 mai 2003. http://news.bbc.co.uk/2/hi/technology/3033551.stm .

[9] S. Belov et V. Kamluk, Absolute Computrace Revisited, 12 février 2014, consulté le 29 mai 2014. http://www.securelist.com/en/analysis/204792325/Absolute_Computrace_Revisited .

[10] G. T. Becker, F. Regazzoni, C. Paar et W. P. Burleson, Stealthy Dopant-Level Hardware Trojans. In *Actes de Cryptographic Hardware and Embedded Systems – CHES 2013*, LNCS 8086, Springer-Verlag, p. 197-214, DOI 10.1007/978-3-642-40349-1_12. Version préliminaire de l'article disponible sous : http://people.umass.edu/gbecker/BeckerChes13.pdf .

[11] Bundesverfassungsgericht, Leitsätze zum Urteil des Zweiten Senats vom 3. März 2009, 2 BvC 3/07, 2 BvC 4/07. https://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html . Communiqué de presse en anglais disponible sous : https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-019en.html .

[12] Business Wire, Intel adopts upon-request replacement policy on Pentium processors with floating point flaw ; Will take Q4 charge against earnings, 20 décembre 1994. http://www.thefreelibrary.com/Intel+adopts+upon-request+replacement+policy+on+Pentium+processors...-a015939945 .

[13] D. Cansell, J. P. Gibson et D. Méry, Formal verification of tamper-evident storage for e-voting, Fifth International Conference on Software Engineering and Formal Methods (SEFM), september 2007, IEEE, p. 329-338. DOI 10.1109/SEFM.2007.21. Version préliminaire de l'article disponible sous : http://hal.inria.fr/docs/00/18/48/33/PDF/mery-e-voting.pdf .

[14] G. Champeau, Le vote électronique sanctionné par la justice, Numérama, 15 juin 2012. http ://www.numerama.com/magazine/22899-le-vote-electronique-sanctionne-par-la-justice.html .

[15] G. Champeau, Vote électronique : anomalie détectée, une candidate UMP conteste l'élection !, Numérama, 18 juin 2012. http://www.numerama.com/magazine/22913-vote-electronique-anomalie-detectee-une-candidate-ump-conteste-l-election.html .

[16] B. Chevallier-Mames, P.-A. Fouque, D. Pointcheval, J. Stern, J. Traoré, On Some Incompatible Properties of Voting Schemes, in Towards Trustworthy Elections, LNCS 6000, Springer, p. 191-199. DOI 10.1007/978-3-642-12980-3_11. http://dx.doi.org/10.1007/978-3-642-12980-3_11 .

[17] M. Clarkson, B. Hay, M. Inge, A. Shelat, D. Wagner et A. Yasinsac, Software Review and Security Analysis of Scytl Remote Voting Software, 19 septembre 2008. http://www.eecs.berkeley.edu/∼daw/papers/scytl-odbp.pdf .

[18] T. Coe *et al.*, FDIV model, 28 novembre 1994. http://www.khd-research.net/Tech/Computer/PBug/pbug_coe.txt .

[19] Constitution du 4 octobre 1958. http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/la-constitution/la-constitution-du-4-octobre-1958/texte-integral-de-la-constitution-du-4-octobre-1958-en-vigueur.5074.html .

[20] R. R. Collins, Intel486 TR4 Register Anomaly, blog personnel. http://www.rcollins.org/secrets/TR4Bug.html .

[21] R. R. Collins, Intel Secrets, Bugs and Undocumented Opcodes, blog personnel. http://www.rcollins.org/secrets/ .

[22] P. Da Silva, Le vote par Internet, c'est pire au second tour !, blog personnel, 10 juin 2012, consulté le 13 juin 2014. http://www.paulds.fr/2012/06/vote-internet-legislatives-fraude/ .

[23] P.-A. D. et J. M. T. (avec Belga), Énormes bugs informatiques dans le dépouillement des élections, la Libre Belgique, 25 mai 2014. http://www.lalibre.be/actu/politique-belge/enormes-bugs-informatiques-dans-le-depouillement-des-elections-53821daf3570102383d0d88c .

[24] C. Enguehard, Les dispositifs de vote électronique dits vérifiables, in G. J. Guglielmi et O. Ihl, dirs, Le vote électronique, Lextenso, Paris, 2014, à paraître.

[25] B. Fitrakis et H. Wasserman, Diebold's Political Machine, Mother Jones, 5 mai 2004. http://www.motherjones.com/politics/2004/03/diebolds-political-machine .

[26] S. Gallagher, Easter egg : DSL router patch merely hides backdoor instead of closing it, Ars Technica, 21 avril 2014. http://arstechnica.com/security/2014/04/easter-egg-dsl-router-patch-merely-hides-backdoor-instead-of-closing-it/ .

[27] G. Greenwald, How the NSA tampers with US-made internet routers, The Guardian, 12 mai 2014. http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden .

[28] L. Grégoire, Comment mon ordinateur a voté à ma place (et à mon insu), 27 mai 2012. http://www.scribd.com/doc/94990325/Comment-mon-ordinateur-a-vote-a-ma-place-et-a-mon-insu .

[29] J. A. Halderman, H. Hursti, J. Kitcat, M. MacAlpine, T. Finkenauer et D. Springall, Security Analysis of the Estonian Internet Voting System. https://estoniaevoting.org/wp-content/uploads/2014/05/IVotingReport.pdf . Le contexte du processus d'audit est décrit sous : https://estoniaevoting.org .

[30] C. Heffner, Reverse Engineering a D-Link Backdoor, blog « /dev/ttyS0 », octobre 2013. http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/ .

[31] C. Heffner, Finding and Reversing Backdoors in Consumer Firmware, atelier Black Hat Embedded Security Summit organisé dans le cadre de la conférence Electronics Engineering Live ! (EE—Live !), avril 2014. Diapositives disponibles sous : http://www.devttys0.com/wp-content/uploads/2014/04/FindingAndReversingBackdoors.pdf .

[32] D. Jefferson, A. D. Rubin, B. Simons et D. Wagner, A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), 20 janvier 2004. http://www.servesecurityreport.org/ . Une traduction française est disponible sous : http://www.servesecurityreport.org/French.pdf .

[33] X. Leroy, Formal verification of a realistic compiler, Communications of the ACM, vol. 52(7), p. 107-115, 2009. Copie disponible sous : http://gallium.inria.fr/∼xleroy/publi/compcert-CACM.pdf .

[34] J. McCormally, Paperless Ballots, Election Legitimacy and Voter Confidence : Problems and Solutions, Cyberlaw Seminar, University of Iowa College of Law, 2006. http://www.uiowa.edu/∼cyberlaw/cls06/papers/jmfinfin.htm .

[35] Motor Industry Software Reliability Association, Development Guidelines for Vehicle Based Software, ISO/TR 15497, ISBN 0 9524156 0 7, novembre 1994. Voir : http://www.misra.org.uk/Publications/tabid/57/Default.aspx#label-dvg .

[36] T. R. Nicely, Pentium FDIV flaw FAQ, blog personnel, 19 août 2011. http://www.trnicely.net/pentbug/pentbug.html .

[37] F. Pellegrini et S. Canevet, Droit des logiciels - Logiciels privatifs et logiciels libres, Puf, Paris, novembre 2013.

[38] F. Pellegrini, Rapport d'observations afin d'auditer le déroulement du vote par correspondance électronique des électeurs inscrits sur les listes électorales consulaires des circonscriptions électorales d'Europe et d'Asie et Levant pour les élections de 2006 à l'Assemblée des Français de l'Étranger. Rapport d'expertise commandé par l'association représentative Association démocratique des Français de l'Étranger – Français du monde (ADFE-FM), juin 2006. http://www.pellegrini.cc/works/rapport_ADFE-FdM_6anon.pdf .

[39] M. Rees, Un bulletin litigieux, grain de sable du vote électronique au Benelux, PCInpact / NextINpact, 18 juin 2012. http://www.nextinpact.com/news/71719-vote-electronique-bug-benelux.htm .

[40] J. Rutkowska et A. Tereshkin, IsGameOver() Anyone ?, tutoriel de formation, conférence Black Hat USA, janvier 2007. http://www.invisiblethingslab.com/resources/bh07/IsGameOver.pdf .

[41] F. Segond, Myxomatos - ou de la démocratie et de la technè, in G. J. Guglielmi et O. Ihl, dirs, Le vote électronique, Lextenso, Paris, 2014, à paraître.

[42] Sénat et Chambre des représentants de Belgique, Rapport concernant les élections du 18 mai 2003, présenté à en Session extraordinaire par le Collège d'experts chargés du contrôle des systèmes de vote et de dépouillement automatisés, 5 juin 2003. http://www.senate.be/www/?MIval=/publications/viewPubDoc&TID=50332887&LANG=fr#3-7/1_38 .

[43] W. Spencer, How to Reset a BIOS Password, Tech-FAQ, novembre 2012, consulté le 29 mai 2014. http://www.tech-faq.com/reset-bios-password.html .

[44] T. Stoppard, Jumpers, acte I, Grove Press, 1971.

[45] Wikipedia, Code correcteur, consulté le 22 juin 2014. http://fr.wikipedia.org/wiki/Code_correcteur .

[46] Wikipedia, Cryptographie asymétrique, consulté le 8 mai 2014. http://fr.wikipedia.org/wiki/Cryptographie_asymétrique .

[47] Wikipedia, Fonction de hachage, consulté le 8 mai 2014. http://fr.wikipedia.org/wiki/Fonction_de_hachage .

[48] Wikipedia, Heartbleed, consulté le 27 mai 2014. http://en.wikipedia.org/wiki/Heartbleed .

[49] Wikipedia, Méthode formelle (informatique), consulté le 29 mai 2014. http://fr.wikipedia.org/wiki/Méthode_formelle_(informatique) .

[50] J. F. Ziegler *et al.*, IBM experiments in soft fails in computer electronics (1978 - 1994), IBM Journal of Research and Development, n° 40(1), janvier 1996, p. 3-18, DOI 10.1147/rd.401.0003. Voir par exemple : http://www.pld.ttu.ee/IAF0030/curtis.pdf .

RESEARCH CENTRE
BORDEAUX – SUD-OUEST

351, Cours de la Libération
Bâtiment A 29
33405 Talence Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399