# Analyse des vulnérabilités de trois modes de vote à distance

Chantal Enguehard
Université de Nantes
Laboratoire d'Informatique Nantes Atlantique
2, rue de la Houssinière
BP 92208
44322 Nantes Cedex 03
France
avec le support du European Computer and Communication Security Institute
Bruxelles, Belgique

**Résumé**
Cet article analyse trois modes de vote à distance dans un environnement non contrôlé : vote par correspondance postale, vote par correspondance hybride et vote par internet. Il décompose les procédures de vote en différentes étapes dont il compare les vulnérabilités en ce qui concerne le respect des critères d'un vote démocratique (confidentialité, anonymat, transparence, unicité, sincérité). Qu'il s'agisse de sûreté ou de fiabilité, chaque vulnérabilité est quantifiée par trois paramètres : ampleur, difficulté et visibilité.

L'étude constate que l'automatisation des traitements combinée à la dématérialisation des objets du vote tend à substituer des vulnérabilités visibles et d'ampleur réduite par des vulnérabilités invisibles et de grande ampleur.

**Mots-clef :** vote par internet, vote à distance, vote par correspondance postale, vote par correspondance hybride, démocratie, transparence, fraude, anonymat, sincérité, unicité, visibilité, ampleur, virus, vers

## Introduction

Les procédures de vote à distance ont été renouvelées ces dernières années avec l'introduction de scanners optiques pour dépouiller automatiquement les bulletins de vote ou la dématérialisation des objets du vote dans le cadre de votes par internet. Cet article situe trois modalités de vote à distance (vote par correspondance postale, vote par correspondance hybride et vote par internet), en rappelle les détails et en établit les différentes phases. Les failles techniques du vote par internet sont exposées dans la troisième partie tandis que la quatrième partie réalise une comparaison des vulnérabilités de chacun des modes de vote.

## I. Le vote à distance

### I.1 - Définition

Selon les pays, le vote à distance peut désigner deux notions distinctes :

— vote hors de son lieu de vote habituel mais dans un lieu sous surveillance (comme les locaux d'une ambassade) ;

— vote dans un environnement non contrôlé et en l'absence de tout agent électoral.

Nous nous intéressons ici au vote à distance échappant au contrôle d'un agent électoral (deuxième

acceptation) sous les trois formes suivantes : vote par internet, vote postal et vote hybride.

Le périmètre d'une étude portant sur les élections peut aller jusqu'à englober la préparation des listes électorales, la campagne des candidats ou encore la proclamation des résultats. Nous nous concentrons ici sur les bulletins de vote[1] que nous observerons depuis la communication du matériel de vote aux électeurs jusqu'au comptage des voix.

Nous ne présenterons ici ni les questions liées au rituel du vote qui ont déjà été largement traitées (voir par exemple [7] et [15]), ni les aspects concernant la fracture numérique ou l'accessibilité (voir [3], [14]).

## I.2 - Trois modes de vote à distance dans un environnement non contrôlé

Pour chacun des modes de vote à distance nous nous sommes attachés à définir un modèle incarné par une application réelle utilisée à grande échelle et qui peut être considérée comme représentative des pratiques du domaine.

— vote par internet : procédure de vote par internet utilisée dans le canton de Genève en 2007 [10].

— vote par correspondance postale : procédure de « vote par correspondance généralisé ou facilité » utilisée dans le canton de Genève en 2007 [31].

— vote par correspondance hybride : procédure de vote hybride utilisée lors des élections du Comité National de la Recherche Scientifique en 2008.

### Vote par internet

Le vote par internet (i-vote) fait partie d'un ensemble plus large appelé vote électronique (e-vote). Sous ce dernier terme sont regroupées toutes les formes de vote faisant intervenir un dispositif électronique (ordinateurs de vote, vote par kiosque, etc.).

Il existe des ébauches de standards et des normes internationales mais ceux-ci manquent de précision dans leur définition des nécessaires modèles organisationnels, légaux et technologiques, aussi le vote par internet connaît de nombreuses variantes. Voici cependant le schéma général qui est suivi dans ses grandes lignes par les procédures usuelles de vote par internet dites sécurisées. Les informations utiles à l'authentification sont communiquées aux électeurs par courrier postal. Les électeurs se connectent sur un site officiel de vote depuis n'importe quel ordinateur relié au réseau internet et comportant un navigateur compatible avec l'application de vote s'exécutant sur le site officiel. Ils doivent alors s'identifier (donner leur identité) et s'authentifier (prouver leur identité) avant d'exprimer leur choix. Celui-ci est crypté puis envoyé vers le serveur abritant le site officiel de vote qui recueille les votes**,** les stocke jusqu'à la clôture du scrutin. Il produit les résultats du vote à la clôture du scrutin.

Comme tous les électeurs ne disposent pas d'un ordinateur connecté à internet, ce mode de vote est toujours mis en place en supplément d'une procédures de vote par correspondance postale[2].

### Vote par correspondance postale

Chaque électeur reçoit le matériel de vote par la poste. Il comprend une "carte de vote"[3] portant l'identité de l'électeur, le bulletin de vote, une enveloppe anonyme et une enveloppe de correspondance. Pour voter, l'électeur met le bulletin de son choix dans l'enveloppe anonyme qu'il scelle, puis il glisse cette enveloppe, ainsi que la carte de vote qu'il date et signe, dans l'enveloppe de correspondance. Cette enveloppe est alors envoyée, par la poste, au bureau centralisateur des élections.

---

1 Ce terme est employé ici dans un sens générique puisque, pour le vote par internet, les bulletins de vote sont dématérialisés.

2 À l'exception notable de la France où le décret n°2007-554 du 13 avril 2007 relatif aux modalités d'élection par voie électronique des conseils de l'ordre des infirmiers dispose « Le vote électronique exclut toute autre modalité de vote. »

3 Le terme "carte de vote" est polysème. Ici il s'agit d'une carte en papier portant le nom est l'adresse du votant.

Le bureau des élections collecte les enveloppes au fur et à mesure de leur réception. Le dépouillement se déroule en deux phases. Le registre d'émargement est mis à jour puis les enveloppes de correspondance sont ouvertes afin de collecter les enveloppes anonymes. Ensuite les enveloppes anonymes sont brassées afin de ne pas conserver de lien entre celles-ci et les enveloppes de correspondance, elles sont alors ouvertes. Les voix portées par les bulletins qu'elles contiennent sont dénombrées afin d'établir l'issue du vote.

**Vote par correspondance hybride : voie postale et dépouillement informatique**

La procédure hybride de vote par correspondance est un aménagement de la procédure de vote par correspondance postale afin d'automatiser le dépouillement par l'usage d'outils informatiques. Les électeurs reçoivent le matériel de vote par la poste : une "carte de vote" et une unique enveloppe. Chaque carte de vote porte une marque (code barre ou numéro) permettant d'identifier l'électeur et une série de cases placées en face des alternatives proposées et que l'électeur noircit pour signifier son choix. Le jour du dépouillement les bulletins sont extraits des enveloppes puis scannés par un lecteur optique qui met à jour le registre d'émargements et le nombre de voix obtenues par chaque candidat.

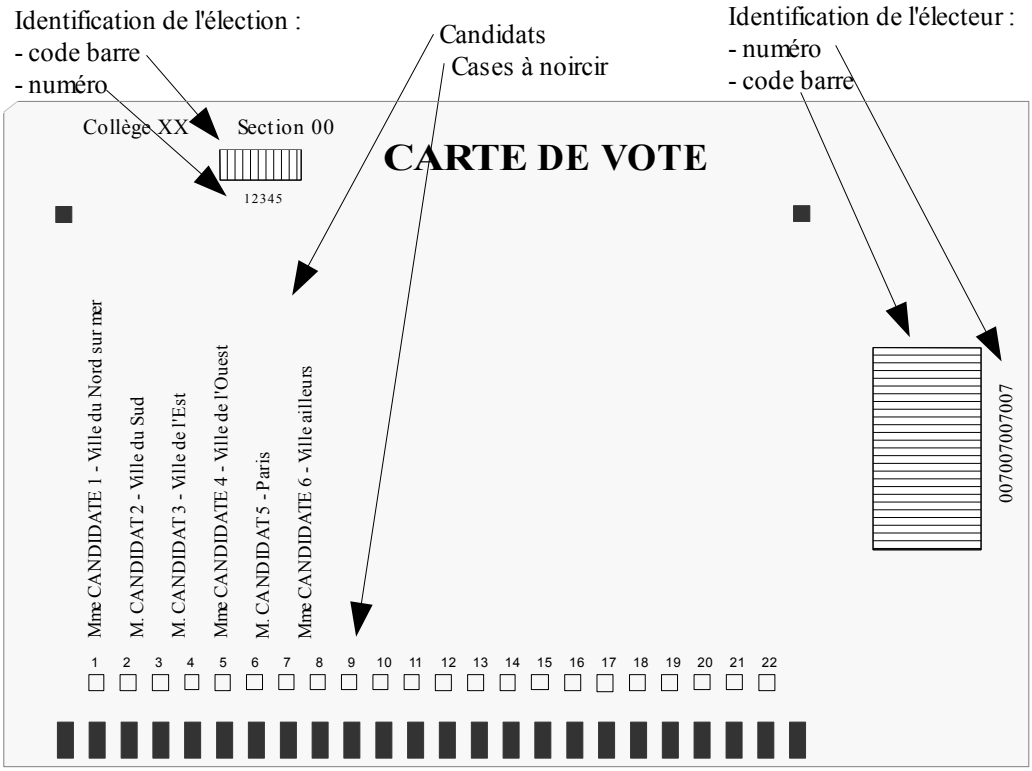


*figure 1 : carte de vote par correspondance hybride*

## I.3 - Phases du vote à distance dans un environnement non contrôlé

Le vote par correspondance dans un environnement non contrôlé suit un parcours que l'on peut découper en plusieurs phases abstraites, communes aux trois mode de vote, mais qui s'incarnent différemment selon la modalité (cf. table 1) : les organisateurs du vote préparent le matériel de vote (B1), et sa transmission (B2). Le matériel de vote voyage dans le canal de transmission (C1) et parvient à l'électeur (E1). L'électeur exprime son choix (E2) puis prépare l'envoi de son vote (E3). Le vote est transmis (C2). Le bureau de vote reçoit les votes (B3) puis effectue les comptages nécessaires (B4). Cette présentation ne reflète pas la totalité des communications ; par exemple, lors d'un vote par internet il existe des échanges entre l'électeur et le système de vote lors de l'expression du choix.

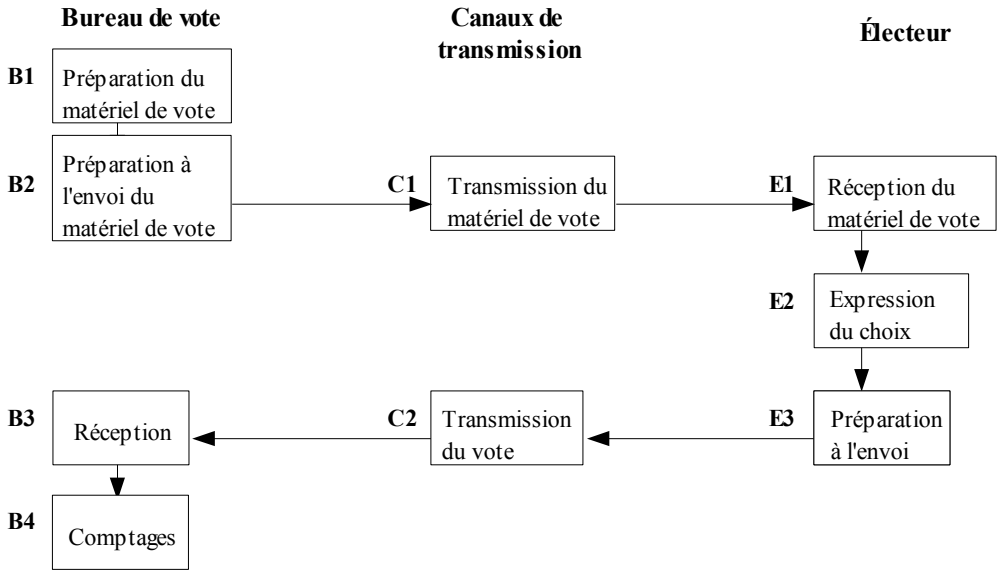


*figure 2 : Les phases du vote à distance dans un environnement non contrôlé*

| | Vote par internet | Vote par correspondance postale | Vote par correspondance hybride |
|---|---|---|---|
| **B1*** Préparation du matériel de vote | Élaboration des listes d'identifiants et de mots de passe, impression du matériel de vote | Impression du matériel de vote | Impression du matériel de vote |
| **B2*** Préparation à l'envoi du matériel de vote | Mise sous pli et transfert à la poste | | |
| **C1*** Transmission du matériel de vote | Les identifiants de connexion sont acheminés (courrier postal) | Les deux enveloppes et les bulletins sont acheminés (courrier postal) | L'enveloppe et le bulletin sont acheminés (courrier postal) |
| **E1** Réception du matériel de vote | Le matériel de vote est reçu par l'électeur | | |
| **E2** Expression du choix | L'électeur se connecte au site de vote, s'identifie, s'authentifie, fait son choix et le valide | L'électeur exprime son choix à l'aide du bulletin de vote | L'électeur exprime son choix à l'aide du bulletin de vote |
| **E3** Préparation à l'envoi | Le bulletin virtuel est crypté | L'électeur met son bulletin de vote dans l'enveloppe anonyme, et celle-ci dans l'enveloppe de correspondance | L'électeur met son bulletin de vote dans l'enveloppe de correspondance |
| **C2** Transmission du vote | Le bulletin de vote voyage sur le réseau jusqu'au bureau de vote | L'enveloppe est transmise jusqu'au bureau de vote | |
| **B3** Réception | Le bureau de vote mémorise les votes reçus, met à jour la liste d'émargements et renvoie des accusés de réception aux électeurs | Le bureau de vote reçoit et stocke les enveloppes de votes | |
| **B4** Comptages | Le logiciel décrypte les votes et décompte les voix | La liste d'émargement est mise à jour, les enveloppes de vote sont ouvertes et les voix sont comptées | Les enveloppes sont ouvertes, le lecteur optique lit les bulletins, le logiciel met à jour la liste d'émargements et décompte les voix |

* Cette étape peut être inexistante lorsque les électeurs se connectent à l'aide d'une carte de connexion comportant une piste magnétique, comme en Estonie.

*table 1 : Phases du vote à distance pour trois modes de vote dans un environnement non contrôlé*

# II. Choix méthodologiques

## II.1 - Démarche comparativiste

Tous les systèmes de vote présentent des vulnérabilités, il n'existe pas de système de vote idéal garantissant le strict respect des principes d'un scrutin démocratique et donnant des résultats parfaitement justes. Notre analyse veillera à comparer plusieurs modèles de vote à distance en fonction de critères exprimés par différentes organisations internationales : Déclaration Universelle des droits de l'Homme de 1948 (article 21) [23], code de bonne conduite en matière électorale de la Commission de Venise [8], manuel d'observation des élections de l'Organisation pour la Sécurité et la Coopération en Europe (OSCE)[27]. Ces critères peuvent être caractéristiques de tout vote démocratique ou être spécifiques au vote par correspondance [9].

Il s'agit de quantifier les conséquences des faiblesses majeures selon trois paramètres : ampleur, difficulté et visibilité.

— L'ampleur dépend du nombre de votes potentiellement affectés par une fraude ou un dysfonctionnement. Ce paramètre peut prendre les valeurs petite (quelques votes), moyenne (nombre de votes suffisant pour changer l'issue des élections), grande (potentiellement la quasi-totalité des votes).

— La difficulté est une estimation floue de la probabilité d'occurrences des conditions nécessaires à l'exploitation de la vulnérabilité. Dans le cas d'un problème de fiabilité technique, il s'agit d'estimer si la panne est courante ou rare. Pour une fraude il faut mesurer la complexité de sa mise en œuvre avec succès (nombre de personnes impliquées, connaissances techniques nécessaires, discrétion, etc.). Ce paramètre peut prendre les trois valeurs petite, moyenne et grande.

— La visibilité détermine si les conséquences des vulnérabilités sont perceptibles. Elle peut prendre les trois valeurs : nulle (conséquences invisibles), moyenne (conséquences visibles mais ne pouvant être prouvées) ou grande (conséquences visibles susceptibles de faire annuler l'élection).

Le pire des cas correspond à une grande ampleur tandis que la visibilité est nulle et la difficulté petite. Ces trois critères ne sont pas indépendants : difficulté et visibilité ne seront estimées que pour un incident d'ampleur grande ou moyenne.

## II.2 – Vote démocratique à distance

### Vote démocratique

Le vote à distance s'inscrit dans les procédures de gouvernance sur lesquelles reposent les démocraties. Les critères énoncés par les organismes internationaux visent le respect des qualités essentielles des élections démocratiques :

— unicité : un vote par électeur[4] ;

— confidentialité : chaque électeur peut effectuer son choix en secret ;

— anonymat : il est impossible de relier un bulletin à l'électeur qui l'a choisi[5] ;

— sincérité : les résultats du scrutin reflètent fidèlement la volonté des électeurs ;

— transparence : « pour le vote par internet, la transparence du système doit être garantie, en ce sens que son fonctionnement correct doit pouvoir être vérifié » (Commission de Venise) [9].

4 C'est l'unicité qui donne au scrutin son caractère universel. Chaque personne en âge de voter (et non déchue de ses droits civiques) possède une et une seule voix. Il n'existe pas d'autres critères limitant le droit de vote comme cela pu être le cas en France avec le suffrage censitaire (un revenu minimum était exigé) ou le déni de droit de vote aux femmes, encore d'actualité dans quelques pays.

5 Confidentialité et anonymat traduisent les deux aspects du secret du vote.

**Vote à distance**

Ces critères génériques sont complétés par des critères spécifiques au vote à distance :

— sûreté : le système peut résister aux attaques délibérées ;

— fiabilité : le système fonctionne, quelles que soient les déficiences matérielles ou logicielles.

La principale difficulté est s'assurer que les votes ne sont ni déformés ni perdus entre le moment de leur expression par les électeurs et le dépouillement.

## III - Failles techniques du vote par internet

Le vote par internet est une procédure nouvelle caractérisée par la dématérialisation de tous les objets du vote (bulletins de vote, urne, cahier d'émargement). Nous détaillons quelques failles techniques susceptibles de modifier les entités virtuelles représentant les objets du vote. Ces failles peuvent relever de la sûreté ou de la fiabilité.

### III.1 - Sûreté

**Vers[6] et virus**

Le poste à partir duquel l'électeur vote est susceptible d'abriter des vers et des virus capables de déclencher des attaques ciblées visant l'expression du vote de l'électeur. Comme la plupart des antivirus ne peuvent détecter que les vers et virus déjà connus, les nouveaux virus ne sont pas identifiables avant de passer à l'action et les attaquants ont l'avantage de tester leurs créations à l'aide des anti-virus communément distribués et qu'utilisent leurs victimes potentielles. Les vers les plus récents sont capables de passer les firewalls et autres défenses, et sont difficiles à analyser [22] [30]. Les attaquants peuvent créer de nouveaux virus, ou modifier des virus qui existent déjà (il existe sur internet des kits de construction de virus). Un virus peut donc facilement infecter un grand nombre d'ordinateurs sans être détecté et rester dormant jusqu'au jour du vote. Il est susceptible de réaliser différents types d'actions, à l'insu de l'électeur, comme capturer les informations nécessaires à la connexion avant qu'elles ne soient transmises au serveur et les communiquer à un tiers, modifier le vote de l'électeur avant cryptage, espionner le vote de l'électeur et le divulguer à un tiers.

**Pharming**

L'électeur est victime d'un détournement de session alors qu'il a saisi l'adresse URL[7] du site officiel et qu'il navigue à l'aide du protocole de sécurisation des communications SSL[8]. Il croit donc voter sur le site officiel alors qu'en fait il est en train d'interagir avec un site qui se contente d'imiter le site officiel y compris en envoyant une confirmation de la réception du vote. Cette usurpation peut être démasquée si l'électeur vérifie que le certificat de sécurité est connu et valide.

Mais un certificat de sécurité falsifié peut avoir été accepté sur le même ordinateur lors d'une connexion précédente sur un site dit sécurisé, provoquant l'affichage d'une alerte de sécurité (voir figure 3). Dans ce cas, de nombreux utilisateurs choisissent de continuer, sans avoir conscience qu'ils autorisent ainsi un certificat de sécurité potentiellement falsifié à rejoindre les certificats de sécurité dûment approuvé par les autorités de certification. Lors d'une connexion ultérieure au site de vote falsifié, il n'y aura aucune alerte de sécurité.

6 Un vers est un virus qui a la capacité de se propager seul en utilisant le réseau.

7 URL : Uniform Ressource Locator.

8 SSL : Secured Socket Layer.

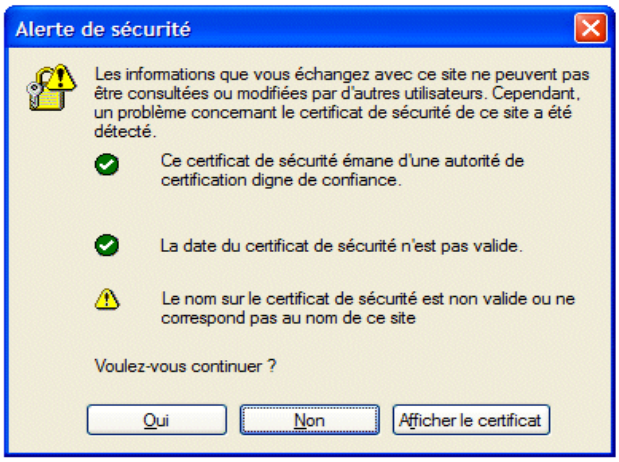


*figure 3 : Fenêtre d'alerte de sécurité*

### Homme-du-milieu

Les interventions du type homme-du-milieu (man-in-the-middle) consistent à se faire passer pour le serveur vis-à-vis de l'ordinateur de l'électeur, et à se faire passer pour l'électeur vis-à-vis du serveur, le fraudeur peut ainsi modifier le vote qui a été émis. Le cryptage du vote offre une bonne protection contre cette attaque si la clef publique de chiffrement envoyée à l'électeur n'a pas été interceptée par le fraudeur. Celle-ci doit donc lui être envoyée dans un courrier sécurisé. En revanche il n'est pas nécessaire de connaître la clef de chiffrement pour capturer le bulletin et le détruire, privant l'électeur de l'exercice de son droit de vote, et renvoyer un message sur le poste de l'électeur afin de lui faire croire que son vote a été bien enregistré.

### Déni de service

Le déni de service (denial of service) consiste à bombarder le serveur de demandes de vote afin d'empêcher les électeurs légitimes de voter. Le serveur, saturé, ne peut répondre à toutes les demandes et est même susceptible de tomber en panne.

## III.2 - Fiabilité

### a - Erreurs matérielles

Un ordinateur peut connaître des pannes ou des dysfonctionnements. Il peut y avoir des défauts dans le matériel, notamment dans les cartes électroniques (soudures défaillantes), ou même dans les microprocesseurs. Les ordinateurs doivent donc intégrer des mécanismes de détection d'erreurs, ce qui n'est pas réalisé systématiquement sur les ordinateurs détenus par des particuliers.

### b - Erreurs logicielles

Il peut y avoir des erreurs dans les programmes qui équipent un ordinateur. Ces erreurs peuvent intervenir à tous les niveaux : système, logiciels, compilateurs, failles de sécurité, etc., y compris dans un système de vote informatisé. C'est pourquoi l'institut national nord-américain des standards et technologies recommande que la vérification ou le contrôle des résultats d'un système de vote ne soit pas confié à des logiciels qui, eux aussi, peuvent connaître des dysfonctionnements [24]. Ces résultats ont été confirmés par de nombreuses études universitaires portant sur le vote dématérialisé [12] [18] [21] [33], la commission indépendante irlandaise sur le vote électronique [4] [5] ou encore des institutions internationales [26].

Plusieurs pistes ont été explorées afin de détecter et éliminer les erreurs d'une application de vote par internet : les tests, le développement formel de programmes, l'expertise, le suivi des opérations

électorales et la vérification cryptographique des résultats.

***Tests***

Tester une application informatique avec succès ne permet pas de prédire avec certitude son comportement lors des utilisations futures, ou même de connaître sa conduite lors d'utilisations passées. Il n'est pas possible de simuler ou reproduire le déroulement d'une vraie élection impliquant des milliers de personnes, avec tous les aléas qui peuvent subvenir. La démarche de tests, inadéquate d'une manière générale pour prouver la correction d'un programme informatique, l'est encore plus en ce qui concerne une application de vote où des dysfonctionnements peuvent passer inaperçus du fait de l'anonymat.

***Développement formel***

En l'état de la science informatique, pour être certain qu'un programme n'abrite pas d'erreurs, il faut au moins imposer l'utilisation de méthodes formelles de développement. Ces méthodes restent très onéreuses et limitées à des composants logiciels. Au-delà d'une certaine complexité, il n'existe pas encore de méthodes de développement sûres[9].

***Contrôle expert***

Il peut exister des autorités de certification mais elles n'ont pas la capacité de vérifier les programmes avec suffisamment de moyens et d'attention pour détecter toutes les erreurs et failles de sécurité. Enfin, même si un tel examen était réalisé, même si l'on disposait de méthodes de développement permettant d'éviter les erreurs humaines, il subsisterait un problème non résolu à ce jour : s'assurer que les programmes en service sont exactement ceux qui ont été certifiés ou qu'ils s'exécutent sans modification contrainte par l'environnement (détournement d'exécution par du code malveillant présent dans des logiciels périphériques ou du microcode pilotant des composants actifs). Dans tous les cas, le serveur utilise un système d'exploitation, éventuellement un compilateur ou un interpréteur de code qu'il faudrait également examiner, etc. Cette démarche devient rapidement titanesque et donc impraticable[10].

***Suivi des opérations électorales***

Pour tracer le fonctionnement d'une application informatique il faut observer son déroulement pas à pas. Or, introduire des sondes logicielles dans des programmes pour en surveiller l'exécution pose la question de l'objectivité et de la neutralité de ces sondes et des programmes chargés d'analyser les données d'observation. Dans le cadre d'une application de vote, un tel suivi implique la tenue d'un journal de bord dans lequel sont notés et horodatés tous les événements : arrivée d'un bulletin, émargement du votant, dépouillement, etc. Le problème est que la lecture de ce journal permettrait de connaître le vote de chacun, ce qui constitue une violation du secret du vote. Si les informations du journal ne sont pas complètes (pour protéger le secret du vote), le procédé devient alors vain puisqu'il ne permet plus de suivre complètement le traitement des informations reçues et qu'un dysfonctionnement (ou une fraude), même majeur, peut passer inaperçu. Nous constatons ici qu'une mesure efficace dans le cadre des utilisations habituelles d'internet (comme les transactions bancaires) ne peut être mise en œuvre avec succès du fait des caractéristiques très particulières des scrutins démocratiques anonymes.

***Vérification des résultats a posteriori***

Le vote par internet est l'objet d'intenses recherche dans le domaine de la cryptographie afin de fournir des modèles permettant à tout électeur de vérifier que son vote est bien pris en compte et

9 « We don't have a theory that can guarantee system reliability, that can tell us how to build systems that are correct by construction. We only have some recipes about how to write good programs and how to design good harware. We're learning by a trial-and-error-process » [32].

10 « les experts ne contrôlent que ce qu'ils veulent, ou ce qu'ils peuvent. » A. Auer [2]

que le total de l'ensemble des votes est juste. L'électeur doit également être en mesure d'apporter des preuves de ses constatations. Quelques systèmes expérimentaux ont été implémentés comme RIES [16] ou VoteBox [29]. Ces systèmes présentent un haut degré de complexité, ce qui est un facteur de vulnérabilité : comme il a été constaté dans le domaine bancaire, un protocole cryptographique bien conçu peut présenter des erreurs d'implantations et se révéler vulnérable aux fraudes [17], [28]. De plus, avec ces systèmes, même si l'électeur constate une déformation de son vote il n'a aucune possibilité d'en apporter la preuve. Enfin, le respect de la confidentialité est conditionné par la destruction de fichiers intermédiaires[11].

# IV. Évaluation

Différentes approches sont envisageables pour structurer cette évaluation car l'analyse doit tenir compte de plusieurs dimensions : le respect des critères qui caractérisent un vote démocratique, les caractéristiques technique de chaque mode de vote, ou encore le déroulement spatio-temporel des atteintes à une élection. C'est ce dernier fil conducteur que nous privilégions en abordant d'abord les aspects communs aux trois modes de vote pour ensuite les traiter individuellement.

## IV.1 Aspects communs aux trois modes de vote

### Préparation et transmission du matériel de vote

Un incident ou une malversation peut amener à ne pas imprimer (B1) ou ne pas transmettre (B2) à une partie des électeurs le matériel de vote nécessaire pour voter, les courriers contenant le matériel de vote peuvent être égarés, retardés ou détournés lors de leur transmission (C1). Les électeurs sont alors privés de leur droit de vote.

Cette atteinte à l'unicité et à la sincérité du vote peut être d'ampleur moyenne, tout en étant de difficulté réduite pour une personne impliquée dans l'organisation. Elle présente une visibilité moyenne car, les courriers n'étant pas envoyés en recommandé pour des raisons de coût, il n'existe aucun contrôle de leur délivrance, les électeurs peu vigilants sont peu susceptibles de noter cette absence et encore moins de le signaler officiellement. Un contrôle strict du nombre de courriers effectivement envoyés est indispensable.

### Réception du matériel de vote (E1)

Lorsque le courrier est parvenu à destination, il peut être intercepté, plusieurs personnes habitant souvent le même domicile. Cette fraude est susceptible d'être commise par une personne de l'entourage de l'électeur qui connaît généralement les informations additionnelles à fournir pour être autorisé à voter (généralement la date de naissance), mais elle est de portée limitée : un fraudeur ne peut détourner que quelques votes.

Les processus biométriques sont parfois envisagés pour éviter l'usurpation d'identité dans le cadre du vote par internet. Cette approche rencontre différents obstacles. Tout d'abord, elle contredit plusieurs principes de sécurité comme le fait qu'un mot de passe doit toujours être stocké dans un fichier unique et de manière cryptée, qu'il doit être possible d'en changer et que les étapes d'identification et d'authentification doivent être distinctes. Lorsque des procédés biométriques sont mis en œuvre, on observe que ce sont les mêmes données qui servent à s'identifier et à s'authentifier, qu'il s'agisse de la paume de la main, de l'iris de l'œil, ou des empreintes digitales. Ces données ne sont pas secrètes et il est impossible d'en changer. De plus, il a été démontré à plusieurs reprises qu'il est facile de tromper les systèmes biométriques en usage [20][12]. Enfin, généraliser cette

11 Détruire des fichiers de telle manière qu'il soit impossible de les reconstruire n'est pas un problème trivial.

12 En France, ces faiblesses ont amené la direction de la protection et de la sécurité de l'État du Secrétariat Général de la Défense Nationale (SGDN) à formellement déconseiller l'usage de la biométrie en ce qui concerne la sécurisation des systèmes informatiques de l'État [36].

approche implique de relever et centraliser les données biométriques de tous les électeurs, ce qui pose des problèmes techniques, organisationnels et éthiques importants.

**Non-réception du matériel de vote (E1)**

Les enveloppes acheminant le matériel de vote et qui n'ont pu être distribuées sont retournées à l'envoyeur, c'est-à-dire au bureau organisateur. Il peut être tentant de les utiliser à l'insu des destinataires officiels.

La portée de cette fraude est limitée par le nombre d'enveloppes retournées au bureau de vote. La comptabilité de ces enveloppes sur les procès-verbaux officiels est une mesure permettant d'alerter en cas de détournement en nombre. L'ampleur de cette fraude est donc limitée.

**Expression du choix (E2)**

Le respect de la confidentialité implique que l'électeur vote seul et qu'il n'est soumis à aucune pression. Dans le cadre d'un vote à distance dans un environnement non contrôlé aucun des modes de vote par correspondance n'est en mesure de garantir que l'électeur exprime son choix seul et à l'abri des pressions.

Des aménagements visant à répondre aux problèmes de pression et donc à accroitre le respect de la confidentialité ont été mis en œuvre dans quelques systèmes de vote par internet : ils donnent la possibilité de voter plusieurs fois, seul le dernier vote étant finalement compté[13]. En supplément, les électeurs ont parfois la possibilité de voter à l'urne dans un bureau de vote pendant quelques jours avant le jour officiel des élections et d'annuler ainsi leur éventuel vote par internet. Ces tentatives présentent l'inconvénient de fragiliser le principe d'anonymat : pour pouvoir être annulés, les votes doivent être stockés sur le serveur en conservant le lien entre le vote et l'identifiant de la personne qui l'a envoyé. Introduire la possibilité de vote multiple pour éliminer une faiblesse visible (au moins par l'électeur concerné) d'ampleur mineure introduit donc une vulnérabilité invisible et d'ampleur majeure : le recueil et l'analyse des fichiers internes au serveur peut permettre de dévoiler les auteurs de tous les votes et les choix qu'ils ont exprimés.

## IV.2 Vote par correspondance postale

Le point faible du vote par correspondance postale est l'acheminement des votes (C2). Les enveloppes contenant les votes peuvent être détournées (elles sont facilement reconnaissables), ou simplement prendre du retard, leur non-réception par le bureau constituant une atteinte à la sincérité du vote.

Même si les services postaux sont censés respecter le secret des missives, les enveloppes peuvent être ouvertes et les votes dévoilés, au mépris de la confidentialité du vote. Il existe aussi des techniques pour connaître le contenu d'enveloppes sans même les ouvrir. Il serait théoriquement envisageable de sécuriser les services postaux en généralisant l'utilisation de courriers recommandés et d'enveloppes inviolables, mais, outre le coût démesuré de telles mesures, il semble illusoire de l'étendre à des pays où n'existe même pas la notion de courrier recommandé[14].

Des enveloppes peuvent être détruites ou remplacées après leur réception par le bureau de vote centralisateur (B3).

Ces atteintes à la sincérité et la confidentialité du vote sont de visibilité moyenne, celle-ci augmentant avec le nombre de courriers concernés. La difficulté de réalisation dépend également de l'ampleur : il est facile de faire disparaître une ou deux enveloppes, réitérer l'opération pour plusieurs centaines ou milliers exige l'implication de nombreuses personnes ce qui accroit sa

13 Curieusement, des études proposent que les électeurs aient la possibilité de signaler un vote comme ultime, alors que cette possibilité ruinerait les avantages apportés par le vote multiple puisque, en cas de pression, on forcerait évidemment la victime à déclarer qu'il s'agit de son dernier vote [35].

14 Cas des électeurs vivant à l'étranger.

visibilité. Ce mode de vote a d'ailleurs été interdit pour les élections politiques par loi n° 75-1329 du 31 décembre 1975 [19] à la suite de nombreux cas de fraude avérés.

## IV.3 Vote par correspondance hybride

Le vote par correspondance hybride connaît les même vulnérabilités que le vote par correspondance postale en ce qui concerne l'acheminement des votes par les services postaux (C2). De même les enveloppes de vote peuvent être subtilisées et détruites après leur réception (B3). Le remplacement des enveloppes de votes est plus complexe que pour le vote par correspondance car chaque carte de vote est unique. L'ampleur de cette fraude peut donc être limitée si le processus de fabrication des cartes de votes est hors de portée du bureau de vote centralisateur.

L'étape du comptage (B4) est automatisée. Les cartes de vote sur lesquelles figurent l'identifiant de chaque électeur et son choix sont dépouillées par un unique logiciel qui gère à la fois la mise à jour de la liste des émargements et le comptage des voix. La séparation entre les votes, les identifiants et les identités des électeurs n'est pas clairement établie. Le dévoilement du vote des électeurs est à la portée des personnes ayant accès au logiciel qui effectue les comptages ou aux données. Cette atteinte au secret du vote peut être le fait d'une unique personne et porter sur tous les votes tout en restant invisible.

## IV.4 Vote par internet

### Préparation et transmission du matériel de vote

Les identifiants et mots de passe sous forme électronique peuvent être copiés lors de leur génération, ou chez l'imprimeur chargé de la réalisation des courriers (B1). Cette manœuvre peut concerner l'ensemble des électeurs et ne pas présenter de grandes difficultés, tout en restant invisible. Toutefois, pour renforcer la sécurité, des informations supplémentaires, comme la date ou la commune de naissance, sont souvent demandées. La collecte de ces informations pour de nombreuses personnes peut s'avérer une tâche insurmontable, ce qui limite l'ampleur d'une copie des informations nécessaires pour voter.

Afin de faire disparaître cette étape, et donc les vulnérabilités qui l'accompagnent, il est possible d'équiper chaque électeur d'une carte électronique servant d'identifiant. Dans ce cas un risque se substitue à un autre : l'usage d'une unique carte d'identité électronique[15] pour effectuer différentes opérations (voter, payer ses impôts, etc.) rend les citoyens particulièrement vulnérables aux agissements abusifs d'un État qui pourrait être tenté de croiser ces données. Ce risque important ne doit pas être négligé, d'autant plus que l'État tenté par ces pratiques ne serait certainement pas le plus désireux d'en informer la population [11].

### De l'expression du choix (E2) à la réception du vote (B3)

Ces étapes donnent lieu à des interactions entre l'électeur et le serveur du site officiel de vote.

Un virus présent sur l'ordinateur utilisé pour voter peut intercepter le vote entre sa validation (E2) et son cryptage (E3) et le communiquer à des tiers, ou mettre en œuvre un détournement de session capturant les informations saisies par l'électeur. Ces informations peuvent ensuite être utilisées pour voter à l'insu de l'électeur légitime. Susceptibles d'affecter un grand nombre de votes, ces agissements peuvent rester quasi invisibles. Leur réalisation ne présentent pas de difficulté particulière pour un informaticien motivé.

En revanche, le déni de service qui a pour principe de perturber l'accès au site de vote, est immédiatement visible.

Par ailleurs de nombreuses personnes pourraient être tentées de voter à partir d'un ordinateur situé

15 Effective en Estonie.

sur leur lieu de travail, surtout s'il s'agit d'un vote professionnel, sans toujours se rendre compte que les entreprises exercent un contrôle de plus en plus serré sur l'utilisation du réseau internet [6] et qu'elles seraient donc en mesure d'espionner les votes de leurs employés.

**Réception (B3) et comptages (B4)**

Dans toute application de vote par internet, chaque bulletin voyage accompagné de l'identité du votant. Ces informations parviennent ensemble sur un premier serveur de vote. Ce point est particulièrement délicat et a fait l'objet de nombreuses publications montrant comment crypter les votes de manière à décoder l'identité du votant indépendamment de son vote ([13] par exemple), mais il reste possible de reconstituer les votes à partir des fichiers intermédiaires stockant les informations reçues par le serveur, même si celles-ci sont cryptées (disposer de données en quantité suffisante et de temps pour les étudier sont des facteurs facilitant ce type de fraude) ; on ne peut mettre en place des mesures techniques qui rendraient impossible la violation du secret du vote par une personne ayant des intentions malveillantes et bénéficiant d'accès aux serveurs.

Il existe des processus de fraude classiques comme l'introduction d'un cheval de Troie (Trojan Horse) ou d'une porte arrière (Back Door). Ces fraudes se résument à l'introduction de quelques lignes de programme qui peuvent facilement passer inaperçues au milieu de programmes comprenant plusieurs milliers de lignes [34]. Ces malversations peuvent être mises en place par une personne unique. Il peut s'agir d'un programmeur, d'un technicien chargé de la maintenance et des mises à jour, ou de toute personne ayant un accès physique ou logique aux serveurs. Le programme frauduleux peut modifier jusqu'à la totalité des votes reçus.

Enfin, la concomitance de l'automatisation de la mise à jour des registres d'émargement et de la dématérialisation des bulletins facilitent le bourrage d'urnes à grande échelle : un programme frauduleux peut générer les votes de nombreux électeurs abstentionnistes dans les derniers instants de la période de vote. Ce risque ne peut être maîtrisé par une surveillance du taux de participation (on a observé que les sites de vote connaissent des pics de fréquentation dans les derniers instants pendant lesquels le vote est ouvert). Il ne peut être jugulé par un contrôle des électeurs : même si des électeurs découvrent qu'un vote a été enregistré à leur nom, alors qu'ils n'ont pas voté, il leur sera impossible d'en apporter la preuve.

# V. Bilan

## V.1 - Synthèse

Aucun des systèmes de vote par correspondance examiné ne peut être qualifié de sûr. Mais les vulnérabilités sont susceptibles de conséquences hétérogènes.

**Vote par correspondance**

Le vote par correspondance est vulnérable à la fraude et largement tributaire des services postaux, mais ces atteintes à la sincérité des élections ne peuvent passer inaperçues lorsqu'elles sont de grande ampleur.

**Vote par correspondance hybride**

Le vote par correspondance hybride, en confiant exclusivement les comptages des votes et des émargements à des procédures automatiques, empêche toute intervention extérieure sur cette étape déterminante d'un vote. La procédure de dépouillement peut être le siège d'un dysfonctionnement ou d'une fraude de grande ampleur qui garde intact le nombre total de votes décomptés mais porte atteinte à sa sincérité. L'établissement d'une telle fraude obligerait à dépouiller à la main l'ensemble des bulletins reçus, ce qui se révèle impossible s'il y a plusieurs milliers de bulletins du fait des difficultés pratiques (il faut garder les bulletins sous scellés, réunir suffisamment de personnes pour

effectuer des comptages, disposer du temps nécessaire et, surtout, pouvoir justifier de la nécessité d'une telle opération) et légale (si le recomptage n'est pas réalisé, il n'y a aucune preuve matérielle susceptible d'étayer les soupçons à présenter au juge de l'élection qualifié pour ordonner ce nouveau décompte).

Le logiciel de votes peut divulguer à des tiers les choix des électeurs sans que cette atteinte au secret du vote puisse être prouvée.

Cette procédure, apparue sans qu'il y ait une véritable réflexion au préalable, montre des vulnérabilités importantes et invisibles quant au respect de la sincérité et de la confidentialité.

**Vote par internet**

Le vote par internet présente de multiples vulnérabilités correspondant au pire des cas : elles sont invisibles et peuvent affecter un grand nombre de votes ; les fraudes peuvent être commises par un petit nombre de personnes et ne nécessitent pas de matériel coûteux.

Ces vulnérabilités apparaissent à différentes étapes de la procédure de vote : chez l'électeur, lors de l'acheminement des votes ou encore lors du dépouillement.

## V.2 - Analyse

Les vulnérabilités des modes de vote à distance examinés affectent des étapes du vote échappant à la surveillance directe des contrôleurs du vote, des scrutateurs, des délégués et des représentants des candidats. Ces étapes peuvent être corrompues à l'insu de tous.

Avec le vote par correspondance classique, les zones d'opacité sont limitées au moment du vote de l'électeur et à la transmission des courriers. Le comptage automatique du vote hybride étend les zones d'opacité en empêchant le décompte public des voix lors du dépouillement.

Le vote par internet radicalise cette démarche d'automatisation en ne manipulant que des objets dématérialisés. Le processus de vote est ainsi déplacé du monde réel, dont l'expérience est à la portée de la majorité des citoyens, vers un monde virtuel où les constats effectués directement au travers nos perceptions (la vue, le toucher, etc.) ne s'appliquent pas. Il est impossible de contrôler directement la procédure de vote et d'évaluer dans quelle mesure elle se déroule correctement. Il faut se contenter d'observer des processus qui sont censés refléter l'activité du système de vote, mais qui peuvent aussi en donner une vision déformée.

Les opérations de vote sont alors à la merci d'événements pouvant rester invisibles : agissements délictueux (d'autant plus faciles à commettre que la proximité avec l'équipe chargée d'organiser les élections est grande) ou encore simples dysfonctionnements.

Il apparaît finalement que l'informatique est démunie face à ce problème. Écrire un programme de taille importante ne comportant plus d'erreurs reste considéré comme un exploit. Or, garantir qu'un programme n'héberge aucune "erreur" volontairement dissimulée est une tâche bien plus complexe. Ni les tests[16], ni les expertises des programmes ne sont suffisants, comme nous le rappelle Ken Thompson, co-concepteur du système UNIX.

« You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. (...) As the level of program gets lower, these bugs will be harder and harder to detect. A well installed microcode bug will be almost impossible to detect. » [34]

16 « Il existe en outre un théorème fondamental de la théorie de l'informatique selon lequel il ne peut y avoir de test général pour décider si un système et ses logiciels hébergent ou non un code malveillant. » R. Oppliger [25]

## Conclusion

Cette étude a présenté les vulnérabilités de trois modes de vote par correspondance dans les domaines technique et démocratique. Elle a montré que l'usage d'outils informatiques s'accompagne, par nature, d'une densification et d'une complexification des procédures internes, ce qui peut rendre invisibles des atteintes massives à la sincérité des résultats ou au respect de la confidentialité.

Il apparaît que la dématérialisation et la conversion des informations inhérentes à tout traitement informatique plonge le processus de vote dans un univers nouveau où les règles de la physique ordinaire ne s'appliquent plus. L'impossible devient possible (modifier des milliers de vote en un instant) alors que le possible si quotidien se transforme en une trompeuse illusion. Par exemple, dans le monde réel le simple brassage des enveloppes du vote par correspondance tranche définitivement les liens entre votes et électeurs. Dans l'univers virtuel, il n'existe aucun moyen de toujours réaliser cette opération sans faillir : des fichiers peuvent avoir été copiés, des informations mal effacées, etc.

En France, la Commission Nationale Informatique et Liberté exige des gestions séparées des émargements et des votes mais semble ignorer que cette séparation n'est pas de nature à interdir les atteintes au secret du vote. De même, la Commission Européenne définit la transparence comme la possibilité de vérifier le fonctionnement correct du système de vote, ce qui reste une tâche impossible comme nous l'avons précédemment démontré. Ou encore elle recommande que l'électeur puisse obtenir confirmation de son vote et le corriger[17] alors que cette possibilité oblige à garder un lien entre vote et électeur, fragilisant ainsi le secret de l'anonymat. Ces tentatives balbutiantes de concilier anonymat, protection du vote et dématérialisation montrent bien que le passage au vote électronique pose des problèmes originaux, particuliers, révélant des contradictions et des résistances surprenantes.

> « The clear consensus of computer-science experts around the world who have studied these issues is that Internet elections cannot be trusted, for all the reasons that I have explained: the voters and political parties cannot audit the operation of the software and hardware that serves as the real *bureau de vote*. Therefore it is not clear to me how the *assesseurs* can sign anything but a surrealist image of a true *procès-verbal*. » [1]

## Bibliographie

[1] APPEL (A.W.) Ceci n'est pas une urne: On the Internet vote for the Assemblée des Français de l'étranger, (juin 2006).

[2] AUER (A.), VON ARX (N.) La légitimité des procédures de vote : les défis du e-voting, faculté de droit de l'Université de Genève, Suisse, (décembre 2001).

[3] BIRDSALL (S.) The democratic divide, first monday, peer-reviewed journal on the internet, (2005).

[4] CEV. Commission on Electronic Voting, Secrecy, Accuracy and Testing of the Chosen Electronic System", first report, (December 2004).

[5] CEV. Commission on Electronic voting. Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. second report, (July 2006).

[6] CNIL. La cybersurveillance des salariés. rapport de la Commission Nationale Informatique et Libertés, (2003).

[7] COLEMAN (S.) Internet voting and democratic politics in an age of crisis. in Trechsel A. (ed.) The European Union and E-Voting: Addressing The European Parliament's Internet Voting Challenge, Londres: Routledge, p.223-237, (2005)

[8] COMMISSION EUROPÉENNE POUR LA DÉMOCRATIE PAR LE DROIT (COMMISSION DE VENISE). Code de bonne conduite en matière électorale, (juillet 2002).

17 « En particulier, l'électeur doit pouvoir obtenir confirmation de son vote et le corriger, si nécessaire, dans le respect du secret du vote. » [9], article 8.

[9] COMMISSION EUROPÉENNE POUR LA DÉMOCRATIE PAR LE DROIT (COMMISSION DE VENISE). Rapport sur la compatibilité du vote à distance, et du vote électronique avec les standards, du Conseil de l'Europe, Adopté par la Commission de Venise, lors de sa 58e session plénière, (Venise, 12-13 mars 2004), (18 mars 2004).

[10] ÉTAT DE GENÈVE. E-Voting - Cahier des charges. www.ge.ch/evoting/cahier_charges.asp

[11] DESWARTE (Y.), MALCHOR (C. A.) Current and future privacy enhancing technologies for the Internet. Ann. Télécommun., 61, n°3-4, p.399-417, (2005).

[12] DILL (D.), DOHERTY (W.) Electronic Voting Systems. Report for the National Research Council, (November 22, 2004).

[13] GÓMEZ OLIVA (A.), SÁNCHEZ GARCIA (S.), PÉREZ BELLEBONI (E.) Contributions to traditional electronic systems in order to reinforce citizen confidence. Electronic Voting 2006, 2nd International Workshop, GI-Edition, Lecture Notes in Informatics, Robert Krimmer (Ed.), p.39-49, Bregenz, Austria, (August, 2nd-4th 2006).

[14] HERRNSON (P. S.), NIEMI (R. G.), HANMER (M. J.), BEDERSON (B. B.), CONRAD (F. G.), TRAUGOTT (M.) The Importance of Usability Testing of Voting Systems. Electronic Voting Technology Workshop, Vancouver B.C., Canada, August 1, 2006.

[15] HOFF (J.) Towards a theory of Democracy for the information age. Discussion paper for the Democracy Platform UK-Nordic Meeting, (16-17 septembre 1999).

[16] HUBBERS (E.), JACOBS (B.), PIETERS (W.) RIES - Internet Voting in Action. In R. Bilof, Proceedings of the 29th Annual International Computer Software and Applications Conference, COMPSAC'05, pages 417-424. IEEE Computer Society, (July 26-28, 2005).

[17] JANVIER (R.) Lien entre modèles symboliques et computationnels pour les protocoles cryptographiques utilisant des hachages. Thèse de doctorat de l'université Joseph Fourier, Grenoble, (2006).

[18] JEFFERSON (D.R.), RUBIN (A.D.), SIMON (B.), WAGNER (D.) Analyzing Internet Voting Security. Communications of the ACM, vol.47, n°10, p.59-64, (October 2004).

[19] LOI n°75-1329 du 31 décembre 1975. codifiée sous l'article L72-1 du code électoral, (1975).

[20] MATSUMOTO (T.), MATSUMOTO (H.), K. YAMADA (K.), HOSHINO (S.) Impact of artificial "gummy" fingers on fingerprint systems, Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol.4677, (2002).

[21] MERCURI (R.) A Better Ballot Box?. IEEE Spectrum Online, (October 2002).

[22] MOORE (D.), PAXSON (V.), SAVAGE (S.), SHANNON (C.), STANIFORD (S.), WEAVER (N.) Inside the Slammer worm. IEEE Security and Privacy, (2003).

[23] NATIONS UNIES. Déclaration universelle des droits de l'homme, (1948).

[24] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC, (November 2006) Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission, (August 31, 2007).

[25] OPPLIGER (R.) Traitement du problème de la sécurité des plates-formes pour le vote par Internet à Genève, (3 mai 2002).

[26] OSCE/ODIHR. USA 2 November 2004 Elections - OSCE/ODIHR Needs Assement Mission Report. 7-10 September 2004, Warsaw, (28 September 2004).

[27] OSCE. Manuel d'observation des élections, cinquième édition, ISBN 83-60190-02-X, (2005).

[28] RYAN (P.Y.A.), PEACOK (T.) Prêt à Voter: Systems Perspective, (September 20, 2005).

[29] SANDLER (D.), DERR (K.), WALLACH (D. S.) VoteBox: a tamper-evident, verifiable electronic voting system. Proceedings of the 17th USENIX Security Symposium (USENIX Security '08), (2008).

[30] SCHNEIER (B.) The Trojan Horse Race. Inside Risks 111, Communications of the ACM, vol.42, n°9, (September 1999).

[31] SERVICE CANTONAL DES VOTATIONS ET ÉLECTIONS. Je vote ! - élections communales, Election du Conseil municipal du 25 mars 2007. Canton de Genève, (2007).

[32] SIFAKIS (J.) cited in "In Search of Dependable Design" by Leah Hoffman. Communications of the ACM, vol.51, n°7, p.14- 16, (July 2008).

[33] SIMONS (B.) Electronic Voting Systems: the Good, the Bad, and the Stupid. ACM Queue vol.2, no.7, (October 2004).

[34] THOMPSON (K.) Reflections on Trusting Trust. Communication of the ACM, vol.27, n°8, p.761-763, (August 1984).

[35] VOLKAMER (M.), GRIMM (R.) Multiple Casts in Online Voting: Analyzing Chances. Electronic Voting 2006, 2nd International Workshop, GI-Edition, Lecture Notes in Informatics, Robert Krimmer (Ed.), p.97-106, Bregenz, Austria, (August, 2nd-4th, 2006).

[36] WOLF (P.) de l'authentification biométrique", Sécurité Informatique, n° 46, p.1-6, (octobre 2003).