Association Moratoire sur le vote électronique

Consultation sur la réintroduction de l'opération expérimentale de vote électronique

De René Droz

Contenu

Inhalt

1. Introduction 2
1.1. Auteur 2
1.2. Situation initiale avec le vote électronique 2
1.3. La confiance perdue 3
2. Conditions pour un essai de vote électronique sécurisé 5
3. Sélection et fonction des experts indépendants et compétents 6
4. Risques et contre-mesures 6
4.2. Objets d'essai minimum dans l'opération d'essai 8
5. Les problèmes non résolus 9
6. Objectifs de l'opération d'essai 10
7. Remarques finales 10

Évaluation globale

Le dialogue avec la communauté scientifique a permis de porter la question à un niveau scientifique approprié. Cette complexité trouve une expression appropriée dans le règlement et son annexe. **On ne reconnaît pas les conséquences politiques d'une telle complexité. Les cantons, qui ne peuvent jamais fournir toutes les ressources nécessaires pour le faire, sont chargés d'examiner toutes les mesures très complexes qui devraient s'ensuivre. Leur gestion des risques aboutira donc à des compromis inacceptables en matière de sécurité. Cela ne permettra pas de gagner la confiance dans le vote électronique.**

Les lacunes restantes du vote électronique en détail

[1] Des fuites ou des vols de codes d'accès au vote peuvent être commis par des utilisateurs du monde entier. Ces attaques sont difficiles à détecter et ne peuvent être efficacement prévenues avec la solution actuelle. Le droit du non-votant de faire vérifier l'utilisation de son vote, éventuellement faussement exprimé, n'est pas réalisable dans ce contexte.
[2] Les conséquences des terminaux non sécurisés sont supportées non seulement par l'utilisateur lui-même, mais aussi par la collectivité des citoyens votants. Il s'agit notamment du secret du vote.
[3] L'ampleur de la manipulation ne pourra jamais être déterminée. Il en résulte un énorme potentiel d'incertitude en cas d'irrégularités. Il y a donc lieu de se méfier des prestataires et des autorités en matière de transparence.
[4] La fonction d'une commission électorale au sens actuel ne peut plus avoir lieu. Seuls des experts en informatique et des mathématiciens hautement qualifiés peuvent se prononcer sur la validité du processus de vote. Leur compétence et leur probité ne sont soumises à aucune légitimité démocratique.
[5] La fenêtre de temps pour les clarifications en cas de rapports sur d'éventuelles manipulations sera toujours trop petite pour communiquer la validité des élections et des votes à temps dans tous les cas.
[6] Un essai fonctionnera avec un fort déficit pendant des années, tant pour les fournisseurs que pour les utilisateurs. Si l'introduction définitif doit être basée sur une bonne sécurité du système, la fin de l'opération d'essai est difficilement prévisible. Le bénéfice et l'effort sont dans un rapport dramatiquement mauvais.

(V1.5-4)

1. Introduction

Nous sommes heureux d'accepter l'invitation à commenter à nouveau la reprise prévue de l'essai du vote électronique.

1.1. Auteur

L'auteur René Droz[1] a été responsable de la mise en place et de la gestion de la cyberdéfense opérationnelle dans l'armée (milCERT) entre 2005 et 2015. Il est impliqué dans le vote électronique depuis 5 ans et a été membre du comité d'initiative "Pour une démocratie sûre et fiable". Au nom du comité d'initiative, il a également rédigé la "Consultation sur la nouvelle loi sur les droits politiques".

1.2. Situation initiale avec le vote électronique

Le fait que la démocratie directe soit l'une des réalisations les plus importantes de la Confédération suisse n'est guère contesté dans ce pays. L'introduction du vote électronique doit donc être accompagnée de toutes les précautions imaginables. On parle beaucoup des cyberdangers, mais l'ampleur des menaces possibles n'est reconnue que par les meilleurs experts.

Fondamentalement, l'informatique ne peut pas être entièrement sécurisée aujourd'hui parce qu'il est impossible de se passer des composants principaux qui ne sont pas sous contrôle. Il faudrait réinventer toute l'informatique pour vraiment maîtriser tous les processus afin de garantir la sécurité. Ce n'est pas réaliste. Aujourd'hui, l'informatique n'est exploitée avec succès et avec une sécurité généralement suffisante que parce qu'il existe des résultats contrôlables dans presque tous les domaines. Cela limite le risque et le rend statistiquement visible et gérable.

Ce n'est pas le cas du vote électronique - qui est, pour ainsi dire, le seul domaine public présentant ce critère de manque de contrôlabilité. En raison du caractère secret du scrutin, le contrôle public n'est pas possible. Même si certains experts tentent de tracer ce contrôle par voie électronique, il échappe de **toute façon** au contrôle démocratique du public. La fonction de commission électorale ne s'exerce plus sous la forme initialement prévue.

Essayer de sécuriser le vote électronique, c'est comme résoudre la quadrature du cercle. Vous pouvez toujours vous rapprocher, mais vous n'y arriverez jamais. Puisqu'il n'existe pas d'informatique sûre en soi, on peut essayer de sécuriser tous les processus connexes avec beaucoup de compétence et de gagner la confiance avec beaucoup de transparence. Il faut se défaire de l'idée qu'à un moment donné, quelqu'un va mettre au point un "système informatique sécurisé" et que cela résoudra le problème. Le "système" comprend toujours tous les processus de mise en service et d'exploitation, et ceux-ci doivent être envisagés de manière dynamique, contrôlés par des personnes et inclure un grand nombre de nouvelles interventions techniques, chacune pouvant avoir des conséquences fatales. Comme ce fait est largement méconnu du public en raison de la communication unilatérale des administrations (Confédération + cantons), les conséquences inévitables ne sont reconnues que par une minorité. Si l'on veut éviter toutes ces conséquences, cela se traduit par des procédures de révision longues et élaborées dont la complexité est difficilement surpassable.

[1] www.Noevoting.ch

Afin d'identifier ces problèmes et de les rendre accessibles au grand public, la ferme expérimentale pourrait devenir un vaisseau approprié.

1.3. La confiance perdue

Les promesses et les assurances que le vote électronique serait beaucoup plus sûr que ce que nous avons aujourd'hui, nous les avons entendues de la part de la partie fédérale engagée et des défenseurs cantonaux pendant de nombreuses années. C'est notamment pour cette raison que le vote électronique a bénéficié d'un bon taux d'approbation pendant longtemps. En attendant, cela semble beaucoup plus douteux. On ne peut nier la capacité d'apprentissage de la Chancellerie fédérale. Mais comment l'électorat peut-il, après toutes ces années, faire confiance aux mêmes personnes qui postulent encore aujourd'hui pour un système de demain que personne ne connaît encore ? "Les *expériences avec les systèmes précédents ont été utiles"*, disent-ils. Le bénéfice effectif est la prise de conscience que l'on ne peut pas faire aveuglément confiance aux assurances, même du côté fédéral. Le fait de réaliser qu'il existe des entreprises qui développent des systèmes qu'elles ne comprennent pas suffisamment et d'autres qui délivrent des certificats par-dessus le marché apporte le sens de la réalité nécessaire à la discussion.

1.4. L'ancienne et la nouvelle ferme expérimentale

D'une part, il était et il est toujours insatisfaisant que l'opération expérimentale précédente ait été introduite sans base constitutionnelle pour le nouveau canal de vote et donc également sans référendum. On peut admettre que, sans opération expérimentale, il serait difficile de définir et de mettre en œuvre tous les besoins en matière de sauvegarde de la sécurité avec toute la profondeur nécessaire, c'est-à-dire uniquement sur la base de résultats théoriques et scientifiquement connus. L'ancienne opération d'essai était manifestement destinée à contribuer de manière significative à l'instauration de la confiance. Le fait que cela ait clairement mal tourné en 2019 est, à notre avis, dû aux raisons suivantes.

- Sur la perception erronée des cyberdangers
- La surestimation des organismes de certification
- Manque de transparence vis-à-vis des parties intéressées
- L'absence de base scientifique dans l'élaboration des fondements techniques
- La composition des experts

D'autre part, l'opposition à l'exploitation expérimentale en tant que telle était également justifiée par la part beaucoup trop importante du tarif électrique, qui ne serait pas utilisée pour des essais dans aucun secteur de l'économie. Ce nombre a été réduit, ce qui est bienvenu.

Les erreurs prévisibles à venir dans l'opération de jugement ne doivent en aucun cas permettre de douter de l'authenticité des résultats globaux du scrutin. Il n'est **donc pas réjouissant que les Suisses de l'étranger ne soient apparemment pas inclus dans la part de 10%.** A notre avis, cela augmente à nouveau trop fortement le risque de manipulation dans un système qui ne doit pas encore répondre aux exigences minimales qui seront définies une fois.

1.5. Points en suspens dans le nouveau système de vote électronique

Avec son catalogue de mesures, la Confédération a[2] créé des récipients qui doivent permettre de minimiser les risques du vote électronique. Les nouvelles exigences semblent consister essentiellement en les innovations suivantes :

1. *Transparence : il est exigé que toutes les parties d'un système de vote électronique (c'est-à-dire les composants logiciels) soient visibles et accessibles au public, afin que chacun puisse se convaincre de leur innocuité.*
2. *Contrôle et test permanents des systèmes : Le système ne doit pas passer un test unique, mais peut être testé à nouveau et réévalué à tout moment.*
3. *Un groupe de scientifiques indépendants suit l'évolution de la situation et conseille la Chancellerie fédérale sur les questions de sécurité.*
4. *L'objectif des efforts de sécurité n'est pas l'exactitude absolue des résultats, mais la "vérifiabilité complète".*
5. *Les groupes intéressés peuvent rechercher des bogues à tout moment et recevoir de l'argent s'ils en trouvent ("programme de primes aux bogues").*

Les points 1 à 3 font partie des normes industrielles de sécurité informatique et sont bien sûr les bienvenus.

Dans la pratique, le point 4 est extrêmement difficile à réaliser (voir 4.1.4). Le terme utilisé trompe le public en lui faisant croire que l'électeur lui-même et l'autorité pourraient découvrir des manipulations du comptage correct des votes. Jusqu'à présent, cela n'était même pas possible pour leurs propres votes. Seule la manipulation dans *la création et la transmission des* données - aurait pu être théoriquement découverte par soi-même. Il s'agirait de manipulations découvrables avec le téléphone portable ou l'ordinateur personnel. Pour une vérifiabilité individuelle, il faudrait en outre disposer au moins d'une liste publique des codes de vote ("tableau de vote public") pour le vote ou l'élection en question. Puisque chacun ne connaît que son propre code de vote, chacun peut vérifier le décompte par lui-même sans mettre en danger le secret du vote dans une mesure pertinente. Mais la vérifiabilité "complète" n'est toujours pas possible, tant qu'il n'est pas garanti que tous les votes comptés peuvent être attribués à des électeurs authentiques - qui ont réellement voté - et que chacun n'a qu'un seul vote. Mais la "vérifiabilité complète" ne rétablit pas non plus la confiance si (a) la majorité ne comprend pas et ne règle pas ce qui doit se passer en cas de vérification négative (notamment au niveau du "Public Voting Board") et (b) si, même après coup, il n'est pas possible de déterminer l'ampleur d'une éventuelle manipulation. Pour les deux, malheureusement, aucune approche raisonnable vers une solution n'est reconnaissable. Au contraire : la seule chose qui est certaine dans ces cas est le fait que de telles conclusions entraîneraient la plus grande incertitude possible parmi l'électorat. La conséquence supplémentaire de ceci est que la dissimulation des problèmes est opportune pour tout fournisseur et aussi pour les autorités de l'Etat. Et cela favorise à son tour toute méfiance à l'égard du système global de "vote électronique".

Le point 5 - s'il est compris de la même manière que dans l'annonce du dernier concours de hackers - n'apportera aucune contribution et sert manifestement davantage à rassurer le public. Pour les experts externes, cela semble plutôt contre-productif et indique quelque peu l'impuissance à traiter

[2] 64680.pdf (admin.ch)

le sujet, si le dépannage public n'est (toujours) pas étendu aux vulnérabilités vraiment importantes (ingénierie sociale, sécurité opérationnelle à tous les endroits de l'évaluation).

De plus, on ne gagne rien à définir ces principes ; il faudrait aussi les mettre en œuvre de manière cohérente. Cela pourrait être très, très cher. On peut donc douter que, dans le cadre de cette évolution, les exigences de sécurité bénéficient à tout moment d'une priorité absolue.

2. Conditions pour un essai de vote électronique sécurisé

Les conditions d'une exploitation sûre ont été décrites dans le document "Dialogue de la science". En principe, le caractère scientifique des approches y est reconnaissable. En plus de cela, il faudrait dire:

- La divulgation et la vérification absolues de tous les codes sources des composants concernés par les fournisseurs, en particulier de toutes les routines de test, sont obligatoires.
- Des experts indépendants et compétents dignes de confiance sont indispensables. Ceux-ci doivent répondre aux conditions du chapitre 3.
- L'examen détaillé des mécanismes de test par les experts, avec la possibilité permanente d'introduire des tests supplémentaires, est obligatoire.
- La supervision de la mise en œuvre du test d'évaluation est effectuée en détail par les experts dans chaque cas d'opération à l'urne.
- La compensation pour les efforts généraux et en particulier pour ces opérations spéciales pour tous les bulletins de vote est indispensable et doit être appropriée. Ils seront inclus dans le coût total de l'opération de vote électronique.
- Il est urgent de définir des critères d'alarme qui entraînent une intervention immédiate, ainsi que des critères permettant d'arrêter un scrutin.
- Les critères d'alarme doivent également pouvoir être définis et établis par les experts.
- Un catalogue de mesures doit être convenu avec les experts et fourni de manière transparente.

L'examen public ne peut logiquement avoir lieu qu'avec un certain décalage, une fois que les experts ont effectué toutes les analyses et fourni les documents sous une forme compréhensible. Il en résulte une fenêtre temporelle dans laquelle les éventuelles irrégularités peuvent être identifiées et évaluées. Nous recommandons une procédure en deux étapes pour commencer:

- Détermination de la procédure présumée correcte dans les 3 heures.
- Détermination de la procédure certainement correcte dans un délai de 4 jours

Elle peut entraîner une perte de confiance si, par exemple, les problèmes détectés a posteriori, qui peuvent être le signe d'une manipulation, se révèlent plus graves qu'on ne le pensait au départ. Cela ne devrait pas conduire à une réduction de la transparence, mais plutôt à une répétition du scrutin, voire à la suspension ou à l'abandon général du système actuel de vote électronique.

3. Sélection et fonction des experts indépendants et compétents

Pour instaurer la confiance, la sélection d'experts indépendants et compétents est d'une importance capitale. Normalement, les experts informatiques compétents se trouvent du côté du fournisseur ou du prestataire, car ils s'occupent à plein temps des circonstances de leur système. Cependant, ils sont basés sur des intérêts, on ne peut donc pas s'attendre à ce qu'ils poursuivent toutes les irrégularités avec le plus grand sérieux et compromettent au mieux leur propre système. D'un autre côté, il existe des experts qui enquêteront sur les irrégularités avec tout le sérieux voulu, mais ils peuvent avoir un niveau de connaissance plus approfondi du produit actuellement utilisé. Il est donc nécessaire de leur donner le temps d'enquêter sur les questions et de mettre en doute et vérifier les informations privilégiées. Cela peut entraîner des discussions animées, des retards et des doutes dans la salle. Mais cela fait partie d'une culture de l'erreur, qui est absolument nécessaire, surtout dans le domaine du vote électronique.

La sélection et la fonction des experts doivent donc respecter les principes suivants :

- Ils ne doivent pas être impliqués dans des organisations qui s'alignent sur les intérêts du prestataire, du fabricant ou du fournisseur.
- La moitié au moins des experts doit avoir une attitude critique vis-à-vis du vote électronique et ne doit pas appartenir à l'administration.
- En ce sens, les organisations Digitale Gesellschaft, Chaos Computer Club et Piratenpartei sont considérées comme dignes de confiance pour l'expertise.
- Les noms des experts seront publiés.
- Les experts ont le droit de rendre leurs opinions publiques. Les opinions majoritaires et minoritaires sont publiées et marquées comme telles.

4. Risques et contre-mesures

Certains risques et contre-mesures ont été reconnus ou identifiés en principe dans le dialogue avec la communauté scientifique. Les autres doivent également être pris en compte dans une mesure appropriée.

4.1. Trop peu d'attention accordée aux risques de la cyberguerre

4.1.1. fuite de codes : les codes créés dans les centres d'impression, qui sont censés garantir la sécurité de la transmission, peuvent fuir de ces centres de diverses manières, tout comme les mots de passe sont volés à grande échelle dans le monde entier dans des centres informatiques hautement compétents. Ce fait montre qu'il est apparemment très difficile de protéger les centres informatiques en général contre les fuites de données. Ainsi, il est possible de produire des bulletins de vote globalement valides, que l'on tente ensuite de placer dans le système peu avant la date de clôture du vote électronique. Seuls les codes de vote qui ont déjà été utilisés par le propriétaire authentique entraîneraient un échec. Avec un taux de non-votants de, disons, 55%, il en résulte un potentiel de manipulation important.

La prévention de ces fuites de données devrait être assurée par des exigences opérationnelles et ces mesures devraient être compréhensibles pour les experts et vérifiables à tout moment, ainsi que

communiquées de manière crédible au public par ces experts. Le test 4.2.1 pourrait éventuellement être utilisé pour identifier des indications de fuite de code.

Le droit du non-votant de vérifier son vote, qui peut être faux, est une mesure juridiquement efficace, mais il ne convient pas pour détecter les manipulations pertinentes, car il n'est probablement perçu que dans les cas les plus rares. Pourquoi une personne politiquement désintéressée devrait-elle s'intéresser à la question de savoir si son vote a été émis illégalement ?

4.1.2. Manipulation par des initiés : les personnes ayant des privilèges sur les systèmes peuvent effectuer des interventions qu'elles ne doivent pas nécessairement comprendre et qu'elles ne doivent même pas avoir l'intention de faire. Les manipulateurs peuvent, sous n'importe quel prétexte, inciter les initiés, ou au mieux les faire chanter, à effectuer des interventions qui ont des effets complètement différents de ceux communiqués.

Ces manipulateurs peuvent être des sociétés d'approvisionnement infiltrées, des services secrets, des organisations mafieuses ainsi que des individus (à l'intérieur et à l'extérieur de l'entreprise du fournisseur), comme l'ont montré divers événements dans le passé. La détection et l'analyse de ces manipulations nécessitent un contrôle rigoureux et élaboré de l'accès à tous les systèmes concernés (sécurité opérationnelle). Cela devrait également être effectué par un prestataire de services indépendant du fournisseur (par exemple, le gouvernement fédéral/l'armée).

4.1.3. Vulnérabilités cachées dans le système central : Afin d'effectuer des manipulations au-delà des dispositifs de sécurité, une vulnérabilité est nécessaire dans un premier temps. Outre les 10 000 nouvelles vulnérabilités découvertes et enregistrées chaque année, il faut également s'attendre à un certain nombre de vulnérabilités découvertes mais non enregistrées qui facilitent ces interventions manipulatrices ou les rendent possibles en premier lieu. Celles-ci changent avec chaque mise à jour qui élimine les anciennes vulnérabilités et/ou en introduit de nouvelles. Comme le potentiel des attaquants augmente massivement si les vulnérabilités connues restent ouvertes plus longtemps, il n'y a pas d'alternative aux mises à jour permanentes des fournisseurs, qui éliminent néanmoins toujours certaines des plus importantes vulnérabilités connues. Toutefois, à chaque mise à jour, une nouvelle vulnérabilité est à nouveau possible.

Si l'opposition est une agence gouvernementale, le risque lié à une nouvelle mise à jour peut être plus important que de laisser un état testé en place à court terme. Cependant, il n'existe pas de méthode sûre et concluante. Ces dangers ont été évoqués en passant, mais des contre-mesures complètes et efficaces ne sont pas encore apparues.

4.1.4. terminaux non sécurisés : la manipulation éventuelle d'un terminal (téléphone mobile, ordinateur) est censée être détectable avec la solution cryptologique du vote électronique ("vérifiabilité individuelle"). Bien que cela soit formellement correct, cela ne fonctionnera pas dans la pratique. Un terminal manipulé peut retenir le code de confirmation dans le cas d'un "mauvais vote" et laisser l'électeur croire qu'il a voté. Ils ne verront pas le code de finalisation, mais 90 % des votants se contenteront sûrement d'un "Vote OK" ou d'un message similaire sur l'écran. De cette façon, le scrutin peut être manipulé massivement et seules quelques personnes seront surprises par l'absence du code de finalisation. Étant donné que dans un tel cas, seule la décision de l'électeur de se rendre aux urnes demeure, on peut s'attendre à ce que de tels cas passent largement inaperçus. Ce qu'il convient de faire avec les rapports qui nous parviennent reste totalement inconnu, car le nombre de cas non signalés ne peut même pas être estimé. En outre, les contrôles de ces rapports

prennent tellement de temps qu'au mieux, il serait possible d'analyser quelques exemples au bout de quelques jours. Si l'on intervenait rigoureusement avec seulement quelques rapports, on pourrait aussi tomber dans le piège d'une fausse manipulation. Aucun des mécanismes de défense possibles n'est donc digne de confiance.

Comme pour la pandémie, il ne suffit pas que les individus se protègent (contre la manipulation des votes), ils doivent aussi contribuer à protéger la société dans son ensemble. Toute personne qui ne le fait pas est un maillon faible et contribue à une éventuelle manipulation. Par conséquent, si l'ensemble ne peut être contrôlé, il est impossible d'obtenir un résultat sûr et digne de confiance. Jusqu'à présent, ce danger n'a pas été mentionné, même par les scientifiques concernés.

4.1.5 Négociation avec les codes de vote : Étant donné que nous devons encore compter avec environ 40 à 50 % de votants abstinents, il existe un potentiel d'échange de non-votes grâce aux codes d'échange faciles à utiliser. L'offre et la demande sur le darknet sont largement protégées de la justice. Un modèle économique approprié serait tout à fait concevable.

Jusqu'à présent, il n'existe aucune précaution contre ces dangers. Dans ce cas, l'utilisateur peut agir illégalement, mais le contrôle n'est guère possible.

4.1.6 Compromettre le secret du vote : En piratant un téléphone portable, par exemple, les données relatives au vote peuvent facilement être transmises à une base de données qui s'intéresse au comportement électoral des personnes. Une application qui simplifie par exemple le processus compliqué de vérification manuelle aurait non seulement la possibilité de manipuler le vote mais aussi de le transmettre à des tiers.

Jusqu'à présent, il ne semble y avoir aucune précaution contre ces dangers. Il semble que le risque soit simplement laissé à l'utilisateur, puisque personne n'est obligé d'utiliser le vote électronique. Ce que l'on oublie, cependant, c'est que dans une grande partie de la population, il existe une demande pour que l'État fasse quelque chose contre ces dangers.

4.2. Objets d'essai minimum dans l'opération d'essai

Le passage de la "vérifiabilité individuelle" - insuffisamment protégée - à la "vérifiabilité complète" consiste en une série de contrôles qui, au moment de l'évaluation, doivent garantir au minimum ce qui suit :

#	Essais	Description	Contre-mesures pour
1	Que tous les bulletins de vote soient marqués d'un code de vote unique, valide et à jour.	Seuls les bulletins avec des codes de vote valides seront comptés. Les tentatives de duplication invalides avec le même code de vote sont listées avec l'IP d'origine. Des codes de vote inexistants conduisent à une alarme Il convient de consulter les données comparatives fiables à ce sujet.	4.1.2,4.1.3 4.1.1. partielle
2	Que tous les codes de vote représentent un électeur valide	Les données de comparaison sécurisées (codes de vote) doivent être utilisées à cette fin. Le nom de l'électeur n'est pas nécessaire.	4.1.2,4.1.3

3	Que les bons moyens soient utilisés pour tester (Test conjoint d'une ou plusieurs routines de test préparées par les experts)	Le prestataire et les experts examinent la routine de test, qui doit vérifier les routines d'évaluation	4.1.2,4.1.3
4	Que les résultats correspondent aux bulletins de vote existants (Authenticité des routines d'évaluation 1-2)	Le contenu des routines d'évaluation est vérifié par les experts. Cela peut être fait avec une routine de test développée par les experts. Les routines d'évaluation ne doivent pas avoir été modifiées depuis la dernière (vérification du code source, y compris la traduction du code machine). La routine d'évaluation doit avoir été correctement appliquée pour la détermination des résultats de l'inspection.	4.1.2,4.1.3
5	Que les résultats ne dépendent pas de la plateforme (Authenticité des plateformes)	Les évaluations sont réalisées sur 4 plates-formes différentes qui n'ont pas d'action commune	4.1.2,4.1.3

5. Les problèmes non résolus

Il ressort clairement de ce qui précède qu'il n'est pas encore possible de définir des contre-mesures efficaces pour toutes les cybermenaces. C'est évidemment la raison pour laquelle le cadre de la durée de la nouvelle opération d'essai est estimé à 15 ans supplémentaires.

Parmi les risques individuels mentionnés (section 4.1), qui ne font pas l'objet de contre-mesures suffisantes, les suivants sont des priorités absolues et doivent être traités immédiatement :

- Flux de code pour les autorisations et l'authentification (4.1.1)
- Terminaux utilisateurs non sécurisés et conséquences mentionnées (4.1.4)
- Compromission du secret du vote par la cybercriminalité "normale" (c'est-à-dire également sans l'hypothèse d'un adversaire étatique) (4.1.6)

Nous constatons également les points critiques suivants :

- La **fenêtre de temps pour** tous les contrôles est trop courte. La complexité de la détection d'éventuelles cyberattaques et manipulations est telle qu'en aucun cas on ne peut s'attendre à disposer d'une évaluation finale en quelques heures si des résultats partiels douteux sont disponibles aux stations d'audit. Ce sera politiquement extrêmement sensible si l'on arrive à la conclusion, après des jours, voire des semaines, que l'élection a pu être compromise. Là encore, l'évaluation de l'ampleur de ce phénomène pourrait constituer un défi majeur.
- **La fonction réelle de la commission électorale** est assurée par des experts en informatique qui n'ont aucune légitimité politique. Ce fait pourrait ne pas être politiquement acceptable s'il était clairement perçu par le public.
- **Le fournisseur** veut réussir commercialement avec son produit. Il est difficilement concevable que cet objectif soit déjà atteint dans le cadre d'une opération expérimentale, les cantons n'ayant aucune idée du prix qu'ils devront payer pour cela. La seule chose qui est certaine, c'est qu'il y a beaucoup d'incertitude quant aux développements futurs et qu'aucune garantie d'achat ne peut être donnée avant longtemps. Une communication

transparente de ce fait limiterait probablement l'enthousiasme dans certains cantons et auprès du seul prestataire visible pour le moment.

6. Objectifs de l'opération d'essai

Selon nous, les cibles pour l'exploitation expérimentale doivent répondre aux exigences minimales suivantes :

- **Transparence pour le public de tous les domaines problématiques découverts par les experts**. C'est le seul moyen de gagner la confiance, si elle est justifiée.
- Les **approches visant à résoudre les autres problèmes non résolus mentionnés ci-dessus sont définies**. C'est le seul moyen de désamorcer la situation sécuritaire désolante.
- **Définition des critères d'annulation d'une élection ou d'un vote**. Ce n'est que de cette manière que l'on peut rendre crédible le fait que le processus de vote est également sous contrôle dans le cas électronique.
- **Estimation des coûts et du temps nécessaires pour toutes les mesures de sécurité**. C'est la seule façon d'établir un accord entre le fournisseur et l'acheteur dans un avenir prévisible.
- **Publication des besoins en ressources**. C'est le seul moyen de convaincre le public du bien-fondé de ce projet.

7. Remarques finales

Lors de la conférence de presse du 21.12.2020, il est apparu pour la première fois que le vote électronique ne vise pas à augmenter la participation électorale, c'est-à-dire à améliorer la participation politique de la population (plus). Trop souvent, la preuve de l'absence de lien à cet égard a été apportée. Il ne reste donc que des avantages pour les malvoyants et quelques milliers de Suisses de l'étranger qui ont effectivement un problème avec la distribution postale. Pour ces derniers, il y aurait des mesures largement compensatoires[3].

En tant qu'électeur, je peux avoir l'attitude que le vote électronique doit être possible. En tant que professionnel, je dois admettre qu'avec le vote électronique, nous mettons tous, en tant qu'électeurs, la garantie de résultats corrects entre les mains de quelques spécialistes inconnus de nous, et nous ne pouvons pas non plus réellement évaluer le risque de manipulation. Même si l'on peut en remarquer un, il n'y a aucune garantie. Et si tel était le cas, l'ampleur de la manipulation serait inconnue et les conséquences seraient arbitraires. Ce que cela signifie pour la confiance dans nos institutions démocratiques, personne ne peut le deviner. Ce que j'attends des hommes politiques, c'est qu'ils prennent note de tous ces faits ou qu'ils les divulguent, ***puis qu'ils*** expriment une opinion sur les raisons pour lesquelles le vote électronique devrait ou ne devrait pas être introduit.

En tout cas, en tant qu'électeur, je préférerais ne pas avoir recours au vote électronique dans ces circonstances, même avec une attitude correspondante de droit.

[3] Courrier de vote retardé : La solution réside dans une répartition plus précoce - SWI swissinfo.ch