DeepL

Abonnez-vous à DeepL Pro pour éditer ce document.
Visitez www.DeepL.com/pro pour en savoir plus.

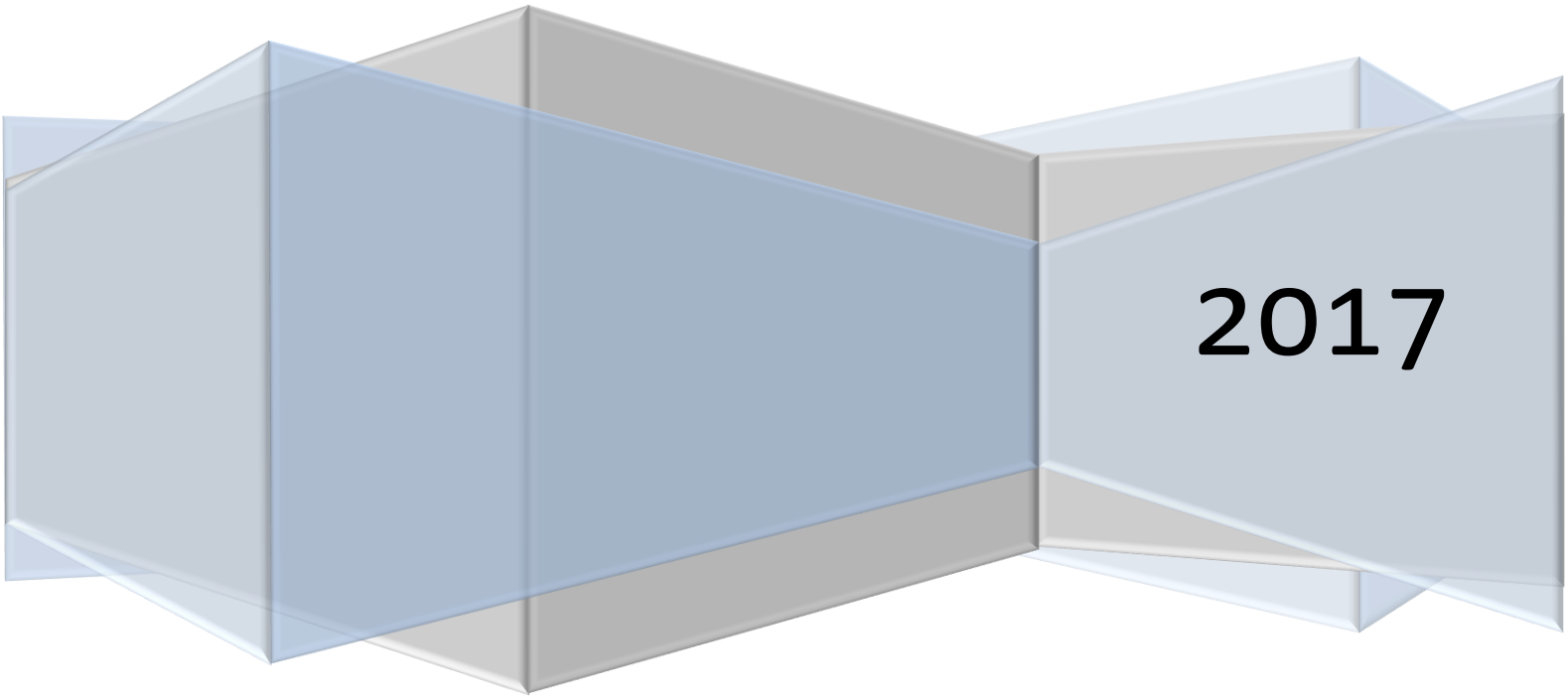
René Droz

E-Voting

Das Ende der Demokratie

Jetzt legen wir uns ein Kuckucksei ins Netz

2018/01.3.0



E-Voting Suisse - La fin de la démocratie

Préface

La Chancellerie fédérale souhaite moderniser et simplifier le contact entre les citoyens et l'État grâce à la cyberadministration. L'e-voting, qui fait partie de la cyberadministration, doit également permettre aux électeurs de voter encore plus facilement que le vote par correspondance, mais l'efficacité du travail de dépouillement a probablement aussi été au centre des préoccupations des autorités.

Les associations de Suisses de l'étranger se plaignent régulièrement d'être gênées, selon le pays d'émigration, par les mauvaises conditions postales lors du vote par correspondance. Elles servent ainsi de faire-valoir pratique à la nécessité du projet, qui ne présente par ailleurs que peu d'impératifs.

Les milieux progressistes pensent que si la politique se rapproche des nouvelles technologies, elle sera mieux acceptée par les jeunes. On vise sans doute un élargissement de son propre potentiel électoral.

Des voix critiques s'élèvent déjà, mais tant que le processus politique est correctement respecté, les arguments de fond sur les risques et les coûts se heurtent à la réalité de l'ordonnance 161.116[1], qui ne dispose pas encore de base concrète au niveau législatif. Le Conseil fédéral est maintenant en train d'élaborer un projet de loi qui devra ensuite être approuvé par le Parlement. Il faut espérer que le Parlement enterrera le projet de loi ou qu'il y aura au moins un référendum. Le risque n'est pas acceptable.

Je me penche de manière approfondie sur la question de savoir pourquoi cette impossible construction erronée d'un cheval de Troie, qui remet en question les fondements de notre système politique, n'est pas confrontée à davantage d'opposition. Dans cette brochure, j'essaie également d'apporter quelques réponses à cette question.

Certes, je ne m'intéresse pas en premier lieu aux coûts qui sont dépensés ici depuis des années. Mais comme pour tous les projets informatiques scandaleux de la Confédération, les coûts et la couverture des frais n'ont pas été rendus transparents. On peut donc supposer que c'est le contribuable, et non le client (= le citoyen), qui paiera la note, et encore moins le commanditaire du système.

[1] https://www.admin.ch/opc/de/classified-compilation/20132343/index.html

Contenu

Préface 1
1 L'histoire du e-voting CH 3
1.1 Motivation pour le vote électronique 3
1.2 Chronique 3
1.3 Compétences 3
1.4 Documents de vote 3
1.5 E-référendums ? 3
2 Le risque 4
2.1 Le risque de l'individu 4
2.2 Comment les risques sociaux sont-ils évalués ? 4
2.3 Qui détermine les risques que nous voulons prendre en tant que société ? 5
2.4 La relativisation des risques dans la vie 5
2.5 Et le cyber-risque du vote électronique ? 6
2.6 Qui sont les pirates informatiques ? 9
2.7 La cybercriminalité 9
3 Les conséquences de l'introduction du vote électronique 16
3.1 Comment faut-il se représenter une manipulation ? 16
3.2 La perte de confiance dans la politique 17
3.3 Le site économique 17
3.4 Le trou financier sans fin 17
3.5 La mondialisation signifie-t-elle l'abolition de son propre espace juridique ? 18
4 Les causes de l'absence de protestation 18
4.1 Le ventre et la tête 18
4.2 La confiance dans les autorités 18
4.3 La complexité et l'ignorance 19
4.4 Le plaisir de la nouveauté et la foi inébranlable en la technique 19
4.5 Les lobbies en lice ..... **Fehler! Textmarke nicht definiert.**
4.6 Le manque de conscience de la sécurité 20
4.7 Quels sont les groupes de personnes qui soutiennent le vote électronique ? 20
5 Conclusion 22
6 L'appel 23

Contrôle des versions :
Nouveautés depuis 2017/09.01.1 au chap. 1.1, 2.5.1, 2.5.3, 2.5.5, 2.7.2, 2.7.6, 2.7.8, 3.4, 5

1 L'histoire du e-voting CH

Dans le cadre de la cyberadministration, la Chancellerie fédérale cherche à améliorer l'efficacité de la collaboration entre le peuple et les autorités. Il va de soi que ce principe peut être soutenu.

1.1 Motivation pour le vote électronique

Les raisons compréhensibles du vote électronique sont les suivantes :

- *Les Suisses de l'étranger qui ont de longs délais de distribution du courrier ont du mal à voter*
- *Les invalides peuvent aussi voter confortablement chez eux*
- *Temps de comptage plus court/économies économiques et écologiques*
- *Acceptation du processus politique par les jeunes*

1.2 Chronique jusqu'en 2017/4

La chronique suivante a été publiée à la Chancellerie fédérale (CF) :

2000	*Démarrer Vote électronique*
2004	*Genève : premiers essais lors de votations fédérales*
2005	*Neuchâtel : premiers essais lors de votations fédérales*
2005	*Zurich : premiers essais lors de votations fédérales*
2008	*Genève, Neuchâtel, Zurich : essais simultanés*
2008	*Neuchâtel : les Suisses de l'étranger admis pour la première fois*
2009-2011	*Contrats d'hébergement entre Genève et les cantons de Bâle-Ville, Lucerne et Berne pour les Suisses de l'étranger*
2009	*Création du consortium Vote électronique composé des cantons d'Argovie, de Fribourg, des Grisons, de Schaffhouse, de Saint-Gall, de Soleure et de Thurgovie.*
2010	*Premiers essais dans 12 cantons*
2011	*Premiers essais lors des élections au Conseil national dans les cantons de Bâle-Ville. Argovie, Grisons et Saint-Gall. Les essais se concentrent sur les Suisses de l'étranger.*
2012	*50% des Suisses de l'étranger peuvent utiliser le vote électronique pour les votations fédérales*
2013	*Troisième rapport sur le vote électronique du Conseil fédéral*
2014	*Entrée en vigueur des nouvelles bases juridiques*
2015	*Élections au Conseil national avec utilisation du vote électronique dans cinq cantons*
2015	*Dissolution du consortium Vote électronique*
2016	*Fribourg : première utilisation du système de la Poste suisse*

Le dernier message était le suivant :

Berne, 05.04.2017 - Lors de sa séance du 5 avril 2017, le Conseil fédéral a décidé des prochaines étapes de l'introduction du vote électronique à grande échelle. L'accent est mis sur des mesures dans le domaine de la transparence (publication du code source) et notamment sur le passage du vote électronique de la phase d'essai actuelle à l'exploitation ordinaire.

1.3 Compétences

- *La Chancellerie fédérale élabore l'ordonnance sur les conditions d'admission*
- *Les cantons exploitent l'installation et sont responsables de son utilisation*
- *Le citoyen doit "si possible" renoncer au vote par correspondance (élections et votations)*

1.4 Documents de vote

La Chancellerie fédérale renonce à l'envoi électronique des documents de vote. Elle connaît donc le risque de falsification et celui de faire croire à une falsification. Cela surchargerait très vite l'administration et la discréditerait.

1.5 E-référendums ?

Ils ne sont pas prévus. Cela entraînerait trop rapidement un trop grand nombre de référendums et surchargerait les administrations fédérales et cantonales.

2 Le risque

Un risque est en principe le produit de la probabilité qu'un incident se produise et de la gravité de ses conséquences s'il se produit.

2.1 Le risque de l'individu

La vie est risquée. Tout le monde prend des risques. Le matin, en traversant la rue, on peut être victime d'un accident mortel, lors d'un entretien d'embauche, on peut se vendre en dessous de sa valeur, lors d'une vente à domicile, on peut se faire arnaquer.

Les risques personnels sont gérés personnellement. Chacun décide lui-même de prendre ou non certains risques. Chacun a donc une certaine capacité d'évaluation des risques qu'il peut assumer ou non. Cela peut être totalement faux dans certains cas, car l'individu se fait une idée erronée des possibilités qui constituent le risque effectif. Mais comme l'individu assume lui-même le risque, cela ne pose pas de problème à la société dans son ensemble.

2.2 Comment les risques sociaux sont-ils évalués ?

Si je prends un risque dont les conséquences éventuelles doivent être supportées par la collectivité, il s'agit d'un risque social sur lequel la société devrait avoir une influence et, normalement, elle le veut. Chacun se fait par exemple assurer obligatoirement et l'assurance publique prend en charge les dommages. Mais qui peut estimer un tel risque pour que les primes couvrent les coûts ? L'Office fédéral de la statistique fournit des chiffres tirés du passé et, la plupart du temps, le peuple et les politiques s'accordent à dire que ces chiffres reflètent le risque de manière assez réaliste. Pour les risques nouveaux, on fait volontiers réaliser une étude, mais on constate toujours, notamment lors des votations, que ces connaissances scientifiques n'ont pas résisté à l'avenir réel. Les auteurs de l'étude indiquent généralement les conditions générales à partir desquelles il faut partir. Il n'est donc pas surprenant que de tels résultats aboutissent à ce que les commanditaires attendent. La question se pose alors de savoir qui vérifie le caractère scientifique du mandat d'étude ?

Malgré ces mauvaises expériences, la Chancellerie fédérale est compétente de par l'Etat pour évaluer de manière définitive les conséquences possibles des résultats des votations. Le "livret de votation", qui est toujours formellement très bien fait, laisse une si bonne impression à la plupart des gens qu'ils accordent du crédit aux affirmations numériques du gouvernement sur les conséquences des votations, qui sont souvent complètement à côté de la plaque, et qu'ils y fondent leurs réflexions sur les risques.

Heureusement, les opposants ont aussi leur mot à dire et leurs arguments sont parfois plus compréhensibles. Il y a des risques qui ne peuvent pas être décrits par des mesures du passé et chaque votant doit alors intégrer des réflexions de principe pour lesquelles sa tête et ses tripes doivent trouver une réponse appropriée. Le "bon sens" tient compte du comportement humain en cas de changement des conditions de base, indépendamment de l'existence de statistiques appropriées pour de telles situations.

Ce qui est particulièrement choquant, surtout pour les initiés de l'administration fédérale, c'est que souvent, même les services fédéraux internes pertinents, comme le service de renseignement, ne sont pas consultés sur les questions de risques sécuritaires. Apparemment, l'unité de l'opinion

gouvernementale est plus importante que le *débat contradictoire* sur le sujet. On peut également en déduire une méfiance générale entre les offices. Cela confirme au citoyen critique qu'il est nécessaire de réfléchir par lui-même. Les faits concernant les risques sont importants pour leur évaluation, mais ne donnent pas encore de réponse claire à cette évaluation. Pour cela, il faut disposer de son propre système de valeurs, qui est soumis à la libre formation de la volonté politique.

2.3 Qui détermine les risques que nous voulons prendre en tant que société ?

C'est là que nous voyons la différence essentielle qui distingue notre société suisse de presque toutes les autres. Alors que dans tous les autres pays, une élite est élue et décide du destin du pays et donc des risques sociaux, nous avons en Suisse la démocratie directe. Le peuple, le souverain, peut renverser les conclusions d'une élite si la majorité des gens n'a pas été convaincue par l'opinion du gouvernement. Une institution absolument centrale et très importante de la démocratie ! La majorité avant la vérité.

Il n'y a en effet que deux alternatives : La vérité avant la majorité ou la majorité avant la vérité. La question de la première est décrite ci-dessus : Qui détermine ce qui est vrai ? Si les risques ne sont pas correctement évalués, les réflexions sur l'équilibre entre les risques et les opportunités aboutiront à coup sûr à un résultat erroné. Pour la formation démocratique de la volonté, la "vérité" est donc tout à fait centrale, on ne peut certes jamais la revendiquer entièrement pour soi, mais on peut s'en approcher le plus possible en donnant de meilleures raisons. Il faut avant tout le vouloir. Il existe aujourd'hui suffisamment d'informations à ce sujet, il suffit de se donner la peine de toutes les enregistrer, de les trier et de les évaluer, même si l'individu peut faire des erreurs. Même si, ou justement parce que, le gouvernement est tenté de nous servir la bonne réponse sur un plateau. En effet, il commet aussi des erreurs, tant dans l'évaluation des faits que dans l'évaluation des risques !

La démocratie n'est pas à portée de clic, mais doit être acquise par un effort intellectuel. Cette constatation à elle seule aurait dû conduire à la conclusion que le vote électronique est un pas dans la mauvaise direction. Ce n'est pas la commodité de la décision qui apporte plus de démocratie, mais l'amélioration des clarifications et de la communication des faits et l'objectivation des débats.

2.4 La relativisation des risques dans la vie

Pour pouvoir évaluer de manière pertinente la capacité à supporter un risque particulier, l'homme intelligent compare ce risque à tous les autres qu'il est prêt à prendre. C'est sur ce point qu'il porte son attention. S'il s'agit d'un risque frappant, il le combattra (le réduira, le reportera, l'évitera), sinon il le supportera (l'acceptera, l'ignorera) comme tous les autres risques.

Il y a quelques risques pertinents que nous connaissons dans la vie.

- Le coup de foudre

La foudre est accidentelle, elle vous frappe vous-même, elle est extrêmement rare, mais lorsqu'elle se produit, elle est généralement mortelle. Comment l'homme réagit-il ? Il fait attention aux paramètres qui l'influencent et évite toutes les situations qui peuvent transformer le risque en problème : Ne pas chercher de champs ouverts ou d'arbres en cas d'orage. Schéma : le risque, c'est moi qui le prends, c'est pourquoi je me protège.

- La centrale nucléaire

Un accident nucléaire majeur est extrêmement rare, il dépend du strict respect des conditions de sécurité par les exploitants. Mais s'il se produit, il peut avoir des conséquences fatales pour des

régions entières, donc aussi pour d'autres que ceux qui déterminent le risque. C'est donc un risque pour la société. Comment celle-ci réagit-elle ? Elle veille scrupuleusement au respect des normes de sécurité, une haute autorité supervise la surveillance à cet effet. Mais l'accident ne dépend-il que de cela ? Les inquiétudes exprimées ces derniers temps concernant d'éventuels kamikazes qui pourraient provoquer l'incident de manière malveillante avec des avions ou des missiles n'ont pas encore été sérieusement prises en compte dans les réflexions sur la sécurité. Il n'y a encore eu qu'un seul incident comparable dans le monde (en 2001) et le risque correspondant est donc (encore) occulté. Schéma : le risque existe, mais il est supporté par la société. Comme les statistiques ne sont pas encore disponibles, il ne trouve pas sa place dans le livret de vote, c'est-à-dire dans la perception publique, et devient ainsi socialement acceptable.

2.5 Et le cyber-risque du vote électronique ?

Le cyber-risque - que les élections/votations soient manipulées lors du dépouillement - est apparemment extrêmement difficile à évaluer pour le citoyen lambda. Il faut considérer les risques individuels suivants et les additionner correctement d'un point de vue mathématique :

A. Le risque que les ordinateurs des électeurs soient manipulés par des outsiders
B. Le risque que les ordinateurs des électeurs soient manipulés par des initiés
C. Le risque que les ordinateurs de la centrale d'évaluation soient manipulés par des outsiders
D. Le risque que les ordinateurs de la centrale d'évaluation soient manipulés par des initiés

Le Service de renseignement de la Suisse estime que le cyber-risque est l'un des risques les plus importants pour la Suisse d'aujourd'hui. Même si le rapport sur la politique de sécurité ne mentionne pas directement le vote électronique, cela devrait conduire chaque autorité à faire les bons constats. Car en matière de cybercriminalité, la devise est la suivante : *tout ce qui est techniquement possible est fait.* Chaque astuce trouve tôt ou tard une application appropriée dans l'activité criminelle.

Alors que le potentiel de votes par correspondance mal comptés se situe à quelques voix par commune, car les différents décomptes sont méticuleusement vérifiés dans chaque commune selon le principe du double contrôle et peuvent être recomptés en cas de besoin, il faut rapidement s'attendre à des dizaines ou des centaines de milliers de votes manipulés sur Internet, qui ne peuvent pas être vérifiés ou recomptés de manière centralisée (c.-à-d. par les cantons) de quelque manière que ce soit (voir ci-dessous).

Si nous considérons le risque de vote électronique aujourd'hui en 2017, le *potentiel de votes*[2] *falsifiés n'*est "que" de quelques pourcents. Mais avec l'extension prévue de l'installation de vote électronique, la marge de manœuvre est déjà de 30% et le Conseil fédéral vise déjà la marque des 100%.

Pour mon système de valeurs, une valeur attendue de plus de 0,1 % de votes erronés n'est plus acceptable. Mais cette limite est bien sûr soumise au système de valeurs de chaque observateur. La question est maintenant de savoir ce qu'il en est du risque d'exploitation de ce potentiel. Il ne faut pas oublier que la manipulation de 10% des voix fait basculer presque toutes les votations. Dans le cas de l'initiative ME, cela aurait déjà représenté 0,1% des voix.

[2] Part de l'électorat utilisant le vote électronique

2.5.1 Risque A : manipulation de l'ordinateur par des outsiders Votants

Ce risque peut être résumé de manière simple comme suit. Les conditions suivantes doivent toutes être remplies : il faut (1) des personnes qui savent très bien pirater et qui connaissent bien le système à pirater, il faut (2) des personnes qui dépensent de l'argent pour organiser une manipulation, (3) un environnement qui permette aux personnes impliquées (1) et (2) de rester anonymes et (4) que la manipulation elle-même ne soit pas détectée ou du moins pas prouvée.

Pour évaluer le risque maintenant, il me suffit de savoir dans quelle mesure chacun des 4 éléments est rempli :

(1) L'**existence des pirates informatiques** ne peut pas être sérieusement mise en doute. Avec les 5 catégories de pirates informatiques, le DDPS distingue 5 niveaux de menace différents. Le système de vote électronique lui-même peut être acquis par tout citoyen suisse et son comportement analysé. Cela est nécessaire pour pouvoir manipuler avec succès les systèmes concernés.

(2) Le fait qu'il existe des personnes ou des organisations qui ont au moins la **volonté** de provoquer des décisions politiques pour de l'argent ne peut plus être sérieusement mis en doute aujourd'hui. De là à entrer dans la criminalité pour cela, il y a certainement un pas que tout le monde ne franchit pas. Mais la perspective d'un anonymat garanti pourrait très bien inciter l'un ou l'autre à tenter l'expérience...

(3) L'existence d'un **environnement permettant de faire des affaires de manière anonyme** a peut-être échappé au grand public. Les initiés savent toutefois qu'il est possible d'acheter illégalement des armes et de recruter des tueurs, par exemple en Russie, sur le "Dark Net". Dans ces cas, la remise de la marchandise et la réalisation de la commande comportent toujours un risque résiduel et sont donc aussi coûteuses que souhaité. En revanche, la manipulation de cyber-résultats sur n'importe quel ordinateur de citoyens ne comporte pratiquement aucun risque.

(4) La protection des données et sa mise en œuvre dans la solution de vote électronique font en sorte qu'une fois arrivé à la centrale, un résultat de vote ne peut **plus** être attribué au votant, c'est-à-dire comparé à sa volonté et donc **contrôlé** de manière centralisée. Grâce à ce que l'on appelle la vérifiabilité, qui apparemment n'est "pas (du tout) réalisable à court et moyen terme", même selon les constatations de la Chancellerie fédérale, l'électeur devrait reconnaître et annoncer lui-même la manipulation qu'il a constatée sur l'ordinateur. Un tel incident peut se produire. Mais qu'est-ce qui motive un électeur qui a recherché le vote électronique par commodité à se méfier de son ordinateur et à vérifier méticuleusement s'il ne contient pas de codes cryptés, conformément aux instructions détaillées, et à se débattre ensuite avec une déclaration aux autorités qui "ne sert de toute façon à rien" ? Peut-être serait-il classé comme un idiot qui ne sait pas se servir des moyens modernes, voire soupçonné lui-même de simuler des erreurs afin de saper la crédibilité du résultat de la votation. Ni les autorités cantonales ni la Chancellerie fédérale n'ont les ressources pour enquêter réellement sur de tels cas, et encore moins dans une mesure qui serait pertinente pour le résultat final. Il n'existe aucune indication sur l'ampleur du nombre de cas non recensés. Il semble que la Chancellerie fédérale envisage malgré tout, dans de tels cas, de ne pas faire compter les e-votes ou de les bloquer pendant le déroulement de la votation. Mais cela serait purement arbitraire et saperait également au plus haut point la confiance du

peuple dans les autorités. On ne sait pas non plus dans quelle mesure le public serait informé de tels processus.

On peut donc affirmer sans crainte que tous les éléments sont réunis pour que le risque A se réalise et que ce n'est donc qu'une question de temps avant qu'il ne se réalise, ou du moins que des doutes légitimes ne viennent saper de manière extrêmement dangereuse la confiance fondamentale dans l'État.

2.5.2 Risque B : manipulation des résultats des votations par des initiés sur l'ordinateur Votants

Le père d'une famille se connecte à l'ordinateur et vote immédiatement pour toutes les personnes de la famille, car il a ouvert le courrier des autorités. Mais cela peut aussi se produire lors d'un vote par correspondance, où il faudrait encore imiter la signature, ce qui ne constitue pas non plus un réel obstacle.

Le risque B ne doit plus être pris en compte par la suite, il ne constitue pas un risque supplémentaire par rapport au vote par correspondance et il est dominé par les risques A et D.

2.5.3 Risque C : Manipulation des résultats de vote par des personnes extérieures à l'ordinateur de dépouillement

Le piratage de la centrale d'évaluation par un outsider ne peut pas être négligé, mais il représente une contribution au risque plutôt faible par rapport à A) et D), si toutes les mesures de sécurité de l'installation ET de l'exploitation ont été prises de manière professionnelle et si l'on n'a pas lésiné sur les moyens. Mais la question de savoir si c'est le cas ici n'est soumise à aucun contrôle démocratique. Des négligences de la part d'initiés permettraient des manipulations de la part d'initiés, qui auraient des conséquences encore plus désastreuses, puisqu'elles toucheraient directement le résultat final. Une simple entrave au processus de vote devrait être assez simple, mais ne conduit pas nécessairement à une manipulation ciblée. Une telle manipulation serait certes théoriquement prouvable, mais qui peut garantir qu'elle serait suivie et publiée ? Quelles sont les exigences en matière de confiance ?

2.5.4 Risque D : Manipulation des résultats de vote par des initiés sur l'ordinateur de dépouillement

Il faut ici un administrateur corrompu pour que ce risque se réalise. Il ne faut pas s'attendre à ce qu'un audit indépendant par un fonctionnaire cantonal puisse avoir lieu sans le spécialiste de l'entreprise qui fournit l'installation. Même si l'on se chargeait de tout le travail d'un audit certifié par un tiers indépendant, il serait difficile de prouver sans l'ombre d'un doute une intervention secrète dans le code ou dans la sortie des données.

Ce risque renvoie à la dépendance à l'égard des individus. **Jamais auparavant l'intégrité d'un vote n'avait dépendu d'individus isolés !** Dans la Constitution, nous avons laissé aux 26 cantons la responsabilité d'assurer un dépouillement correct. En réalité, ce n'est plus l'ensemble des compteurs et de leurs superviseurs, mais quelques spécialistes informatiques de 1 à 2 entreprises sélectionnées.

2.5.5 Risque E : perte de l'anonymat en raison de la fuite des données de vote.

Maintenant qu'il est établi que toutes les stations PC connectées à Internet qui ne sont pas protégées par des cloisonnements spéciaux peuvent être piratées, il est également évident que les données de vote peuvent également s'échapper de la propre station PC et parvenir à des tiers non autorisés. Il faudrait toutefois établir un lien avec le nom et l'adresse du votant pour générer un ensemble de données irréprochable, utilisable à des fins criminelles. Ce ne sera pas facile, car le votant n'est pas

forcément le propriétaire ou l'utilisateur standard du PC. Le code d'authentification pour l'identification ne peut certes pas être calculé, mais la génération et la distribution de ces codes sont également soumises aux divers risques informatiques généraux. La valeur de ces données pour la criminalité internationale ou les services secrets devrait certes être plutôt limitée par rapport à une décision politique. Mais ce risque est assumé par les électeurs eux-mêmes. Cela donne donc une autre vision des choses.

2.6 Qui sont les pirates informatiques ?

Il existe aussi bien des individus que des organisations qui lancent des cyberattaques. On distingue [3]5 niveaux de menace selon le DDPS :

(1) Amateurs / hackers amateurs. Il s'agit de particuliers disposant de connaissances et d'outils pour débutants, achetés ou développés par eux-mêmes, et qui ne sont pas dangereux pour le vote électronique.

(2) Développeurs d'outils de piratage motivés par des raisons intrinsèques. Ils travaillent avec des méthodes et des outils professionnels et ne sont pas directement dangereux, mais peuvent éventuellement devenir des fournisseurs d'organisations criminelles. En raison du partage mondial de ces outils ("open source"), ils ne sont souvent pas conscients des conséquences que leur travail peut avoir.

(3) Des cybercriminels professionnels ordinaires disposant de finances et de liens avec des plateformes de clients anonymes. Ils sont bien organisés comme des groupes et font des milliards d'affaires avec des logiciels malveillants commerciaux en vente et en utilisation. Les dommages causés par ces produits peuvent être en grande partie combattus par des mesures de défense plus ou moins coûteuses, car ils sont utilisés à grande échelle et peuvent donc être rapidement découverts. L'industrie de la sécurité informatique est en lutte permanente contre ces logiciels et fournit après peu de temps (quelques heures ou quelques jours) des "patterns" qui détectent et éliminent ces éléments nuisibles.

(4) Les cybercriminels professionnels disposant de finances importantes et de liens avec les services de renseignement et/ou ayant accès à des connaissances non publiques sur les produits. Ils peuvent créer des produits spéciaux très spécifiques pour des clients spéciaux. Toutes les mesures de défense connues ne les détectent pas, ou alors bien plus tard, avec des méthodes très élaborées (exemple de l'affaire du DFAE de 2012, a été mentionnée en marge dans la presse en 2014).

(5) Le top 5 : Parmi eux, la NSA, le FSB et la Chine : ils savent pour ainsi dire tout sur les portes dérobées et les points faibles de toutes les technologies de l'information (y compris le matériel), du moins celles provenant de leur propre pays, où l'on peut s'attendre à tout. (Exemple Stuxnet : intervention dans le programme nucléaire iranien)

2.7 La cybercriminalité

Pour pouvoir évaluer correctement le risque du vote électronique, il faut fondamentalement être au clair sur les risques généraux de la cybercriminalité et sur le lien avec la réalité actuelle.

Les motifs des cybercriminels ne diffèrent pas beaucoup de ceux de la criminalité normale en termes de motivation : il s'agit du pouvoir et de l'argent. La cybercriminalité n'est pas un risque théorique,

[3] S. DDPS Intra 1/17

elle existe. En 2015, 70000 cas de cybercriminalité auraient été signalés en Suisse[4]. Le nombre d'attaques sur le réseau sur le territoire suisse devrait représenter un chiffre à 810 chiffres. Chacun pourrait mesurer celles qui se produisent localement chez lui s'il le voulait et s'il y consacrait un peu de temps. Seules quelques attaques ont un début de succès et seule une fraction d'entre elles ont des effets effectifs. Et seuls les cas les plus importants ou les plus spectaculaires sont portés à la connaissance du public.

On distingue ici la criminalité générale pour des intérêts matériels et les attaques ciblées contre certaines personnes ou installations pour des motifs politiques.

2.7.1 Le succès

Ce qui est très important, c'est de reconnaître que le succès est donné par les facteurs suivants :

(1) En raison de l'énorme quantité d'escrocs

On peut considérer que l'ensemble de la population mondiale participe à Internet et que tous les criminels du monde sont donc quasiment à notre porte. Grâce à l'accès largement libre aux connaissances techniques et à l'énorme potentiel de butin, les organisations criminelles de tous bords tentent de se tailler une part de cet énorme gâteau dans le monde entier.

(2) En raison de l'énorme quantité de victimes potentielles

Les victimes se trouvent partout où l'on consomme, où des transactions financières ont lieu et où la connaissance de données confidentielles ou la manipulation de celles-ci peuvent conduire à des actions de chantage.

(3) Grâce à l'anonymat

L'anonymat incite souvent des personnes vertueuses à commettre des actes criminels lorsqu'elles se trouvent dans une situation de détresse. Avec un peu d'habileté, ils peuvent sans autre rester anonymes. Un effort de l'Etat pour enquêter sur de tels agissements serait énorme et est entravé par divers facteurs.

(4) Par la connaissance d'informations spécifiques et secrètes

Les cas plus difficiles d'attaques ciblées sont ceux où il faut compter avec des mesures de défense. Les installations informatiques des autorités et de l'armée sont dotées de mesures de protection particulières. Dans ces cas, la tentative d'intrusion nécessite des informations spécifiques supplémentaires sur le système à explorer, qui doivent être collectées au cours d'essais prolongés. Dans les cas extrêmes, il faut en outre des connaissances secrètes (points faibles, portes dérobées) sur certains produits technologiques, dont seuls les autorités, les services secrets et les entreprises technologiques disposent. Ce n'est pas un secret que de telles connaissances sont également commercialisées.

2.7.2 Les espèces

Les possibilités d'activités criminelles dans le cyberespace sont extrêmement variées. Elles vont de la publicité non sollicitée aux crimes graves. Il convient donc de regrouper les catégories les plus importantes :

- Les "**produits de masse**" comprennent l'introduction de publicités et l'utilisation de la capacité de calcul des ordinateurs, en passant par le phishing (simulation de faux sites web et animation de l'utilisateur pour qu'il saisisse des mots de passe) jusqu'au chantage par le

[4] S. http://www.anwalt.org/cyberkriminalitaet/

cryptage des données sur son propre ordinateur, qui ne sont décryptées que lorsqu'une certaine somme d'argent est versée sur un compte étranger, qui est immédiatement effacé une fois la transaction effectuée.

- **L'e-banking** est l'intervention directe dans les transactions financières.
  - La perte des identifiants de compte primaires est protégée par un code via une deuxième voie avec la possession d'un deuxième appareil.
  - La méthode "man in the middle" part du principe que le flux de données est interrompu en direct pendant une transaction et qu'il passe par l'ordinateur frauduleux, qui prend également connaissance des authentifications de deuxième voie, mais modifie ensuite les données du compte cible. Les méthodes cryptologiques permettent de lutter contre ce type de cyberattaque.
  - Des chevaux de Troie spécifiques installés sur l'ordinateur pourraient ici aussi falsifier les entrées et les sorties et faire croire à l'utilisateur qu'elles sont correctes. Les banques ajoutent des contrôles de plausibilité qui stoppent les transactions[5] suspectes et les remettent en question.

- **Les attaques spécifiques à une organisation** sont coûteuses et ne peuvent s'appliquer qu'à un groupe d'objets cibles déterminé. Elles requièrent généralement des capacités de la catégorie de menace 4 ou 5. L'espionnage industriel, le chantage par la compromission de données confidentielles ou personnelles, l'espionnage d'administrations en font partie jusqu'à l'influence sur la politique et les capacités militaires.

2.7.3 Facteurs favorisants et cadre juridique

- *Protection des données*

  La protection des données doit veiller à ce que les données personnelles d'une certaine qualité soient protégées contre tout accès étranger. Cela signifie que des règles et des restrictions sont établies pour tous ceux qui entrent légitimement en contact avec ces données. L'État n'utilise donc pas ces données de toutes les manières possibles, mais uniquement de manière minimale, dans la mesure où le service concerné en a besoin pour accomplir sa mission. La protection des données ne protège cependant pas activement les données, mais seulement contre une utilisation excessive par les services qui respectent de toute façon le droit.

  De ce fait, la surveillance n'est souvent pas possible et les cyberattaques ne peuvent donc pas être détectées. La protection des données compromet donc souvent indirectement la sécurité des données.

- *Peu d'entraide judiciaire internationale*

  Outre le fait que les normes juridiques telles que la protection des données diffèrent de toute façon d'un pays à l'autre, les procédures transnationales pour cybercriminalité sont très rares. Elles se limitent à quelques cas réellement dans l'intérêt des deux parties, par exemple des dommages de plusieurs millions à la charge de ces États. Elles se limitent en outre aux cas où des procédures juridiques peuvent être engagées, c'est-à-dire que les

[5] On remarque par exemple que les comptes d'objectifs sont créés à court terme et rapidement clôturés, en particulier à l'étranger.

suspects et les faits sont connus. En amont de telles procédures, où les données doivent d'abord être déterminées, les indices pour l'entraide judiciaire ne sont pratiquement jamais donnés.

- *Collusion entre les escrocs et les banques ?*
  Les banques, qui sont souvent au centre d'agissements cybercriminels, ont intérêt à garder secrètes les failles de leurs systèmes informatiques. Les dommages causés aux clients donnent une mauvaise image et doivent être passés sous silence autant que possible. Mais les dépenses informatiques sont généralement énormes et doivent être optimisées. Il s'ensuit que dans les cas mineurs, la banque prendra en charge le dommage et n'essaiera de prouver l'erreur du client que dans les cas importants. Si elle n'y parvient pas, elle devra prendre en charge le dommage et tenter d'analyser le cas avec suffisamment de précision pour qu'il ne se reproduise plus après une correction. Le milieu criminel, qui a intérêt à continuer à exploiter la faille, travaillera sur le plus petit feu possible en ce qui concerne l'ampleur des dommages. Dans le cas contraire, il faudra chercher de nouvelles victimes et/ou développer de nouvelles méthodes.

- *Le Dark Net*
  Dans l'Internet normal, les URL, c'est-à-dire les chemins d'accès aux objets cibles (serveurs), sont attribués à une adresse IP via le *service de noms de domaine* (DNS). Via le fournisseur d'accès, l'adresse IP mène à un point précis du réseau dont les coordonnées sont connues. Seuls les derniers mètres de l'éventuel WLAN peuvent encore entraîner une incertitude quant à la localisation de l'abonné au réseau, mais en général, il existe un abonné au réseau responsable de cette IP avec un nom et une adresse postale.
  Le Dark Net regroupe tous les ordinateurs dont les adresses IP ne sont PAS mises à disposition du DNS public. Mais comment peut-on les trouver ? Il n'est pas nécessaire de les trouver ! Il suffit de se connecter à un point du réseau TOR[6].
  Ces chemins y sont accessibles, mais sans que l'on sache soi-même comment ils s'appellent ou à quelles adresses IP ils sont attribués. On pourrait dire que la passerelle TOR le sait et qu'il suffit de la consulter. Mais d'une part, il existe un exploitant privé de cette passerelle qui ne révélerait jamais ces informations et d'autre part, ces connexions TOR sont imbriquées plusieurs fois. Ce serait une action mondiale de les suivre toutes pour localiser une seule connexion Darknet. L'installation de telles passerelles TOR sur Internet n'est pas illégale en raison de la protection des données, sauf dans les dictatures qui l'interdisent dans la mesure où elles le peuvent, car il est difficile de localiser tous ces appareils. Grâce à ces connexions darknet, il est en effet possible, dans les dictatures par exemple, d'établir des connexions avec des sites web interdits et d'obtenir des informations autres que celles favorables au gouvernement, sans que l'expéditeur puisse être localisé.

- *Le bitcoin*
  Cette monnaie permet de payer dans le monde entier. Bien que les États perdent ainsi des millions en impôts et que le contrôle des flux financiers échappe aux banques (contrôlables), presque aucun État n'a osé interdire cette monnaie. Cela n'a d'ailleurs servi à rien, car tant

[6] *L'itinéraire de l'oignon*

que l'on peut changer dans un seul Etat, cette monnaie fonctionne. La cybercriminalité s'appuie dans le monde entier sur le financement par le bitcoin. On peut supposer que l'OCDE s'y intéressera un jour de plus près, mais comme nous l'avons dit, tant qu'il existe des "oasis", une tentative internationale d'assèchement ne sert à rien.

2.7.4 Comment les dictatures se protègent-elles ?

Sans les conditions-cadres restrictives de la protection des données, les dictatures peuvent se protéger non seulement contre les informations indésirables au sein du peuple, mais aussi mieux contre la cybercriminalité, en limitant les voies d'accès et en surveillant de manière restrictive tout trafic de réseau de données - du moins les flux transfrontaliers. Exemples : la Chine : Chine, Russie, Turquie. Pour cela, on ne craint ni les coûts ni les restrictions de disponibilité pour les utilisateurs.

2.7.5 Et nous ?

Chez nous, l'abus de l'activité de surveillance par l'État est actuellement encore considéré par beaucoup comme un risque plus élevé que les conséquences de la cybercriminalité mondiale par des puissances étrangères et des organisations criminelles. Toutefois, l'adoption récente du renforcement de la loi sur la MN en Suisse[7] a déjà laissé entrevoir un léger changement de tendance ou une correction de cap.

2.7.6 Prévenir les risques grâce à une "informatique sécurisée

On parle souvent d'informatique sécurisée et d'informatique non sécurisée. On entend généralement par "TI sûre" le fait que les dispositions et les éléments de sécurité usuels ont été pris, alors que dans le cas d'une TI non sûre, ceux-ci font également défaut. Il va de soi que la sécurité peut être mesurée et évaluée à un nombre infini de niveaux, mais qu'elle n'est jamais totale. Un niveau important pour la distinction est toutefois la question de savoir si l'on est connecté exclusivement à des systèmes (également) sûrs ou s'il en existe au moins un qui ne répond pas aux exigences ?

Que signifie être connecté exclusivement à des systèmes (tout aussi) sûrs ? Cela signifie qu'aucun de mes partenaires ne peut se connecter à un système inconnu, c'est-à-dire qu'il est "connecté à Internet". Cela ne pourrait être le cas que dans les systèmes d'entreprise, où un service central contrôle et surveille la sécurité de tous les participants au réseau. En outre, toutes les connexions doivent être cryptées à l'aide d'un algorithme sécurisé. Mais comme ces systèmes ont généralement besoin d'un accès Internet (non crypté), ils ne sont pas vraiment sûrs non plus. La sécurité exige l'exclusion de tous les risques pertinents, l'insécurité se contente de la présence d'un seul.

La sécurité est la contrepartie du risque. Chacune des parties de l'ordinateur peut présenter des risques et le risque le plus important détermine le niveau de sécurité.

- Le système d'exploitation
  Le système d'exploitation constitue le principal point faible de tous les ordinateurs, en particulier dans l'aspect de la mise en réseau tel qu'il est abordé ci-dessus. Chaque système d'exploitation est le chef de l'ordinateur. Ses points faibles sont réparés à un moment ou à un autre par le fabricant via Internet, mais de nouveaux points faibles sont aussi régulièrement ajoutés. Nombre de ces vulnérabilités sont connues des pirates informatiques. Ils profitent du temps nécessaire pour que les ordinateurs soient mis à jour. Ces failles leur

[7] Loi fédérale du 25.09.2015 sur le renseignement (LRens)

permettent ensuite d'introduire en plusieurs étapes leur code malveillant[8], qui modifie l'ordinateur dans leur sens. Cela ne doit réussir qu'une seule fois. La mise à jour ultérieure du système d'exploitation ne sert alors plus à rien. Un programme antivirus ne reconnaîtra une telle chose que s'il s'agit d'un modèle connu dans le monde entier.

- L'application de vote électronique
  Nous supposons ici que l'application de vote électronique a été créée dans les règles de l'art, sinon elle représenterait un risque supplémentaire considérable. Actuellement, elle ne comprend même pas un module partiel sécurisé (avec une puce matérielle) dans lequel les données ne peuvent pas être modifiées par un système d'exploitation manipulé. Mais ce que ce dernier ne pourra jamais contrôler, ce sont les entrées et les sorties de l'utilisateur. Ce qui n'est pas sûr, c'est donc le clavier et l'écran de l'ordinateur. Le code malveillant veille à ce que l'utilisateur et le manipulateur soient satisfaits. Un échange approprié de fichiers DLL fait en sorte que ce ne soit pas le résultat de la fonction de vérification qui se produise, mais une fonction du cheval de Troie. Pour cela, il faut (seulement) le contrôle du système d'exploitation. Et cela peut être obtenu à tout moment par une cyber-attaque correspondante.
  La transmission de la saisie (falsifiée) est ensuite protégée de manière cryptologique et ne peut pas être (encore une fois) falsifiée. Les dépenses énormes pour ce dernier point peuvent être vendues à des fins publicitaires et font impression. Ils font oublier que le problème se situe ailleurs. L'homme doit en effet vérifier la cryptologie.

La sécurité est un aspect global. *La confidentialité, la disponibilité, l'intégrité, l'authenticité, la non-répudiation* doivent être garanties. Les procédés cryptologiques, lorsqu'ils sont bons, empêchent la manipulation des données et l'accès de l'extérieur. Toutes les exigences peuvent ainsi être couvertes. Mais dans l'ordinateur lui-même, les données ne sont pas cryptées. Un code malveillant peut faire n'importe quoi avec elles. Aucune des exigences mentionnées ne peut donc plus être couverte.

Une sécurisation du système d'exploitation serait certes techniquement possible, mais elle est assortie de telles restrictions, exigences de surveillance et prémisses organisationnelles que l'approche prévue, qui consiste à effectuer un vote électronique sécurisé avec l'ordinateur personnel de l'utilisateur, constitue tout simplement une absurdité.

Il faudrait postuler un système propre qui ne puisse faire que de l'e-voting, par exemple sur l'une de plusieurs machines virtuelles complètement séparées, installées sur le matériel de l'utilisateur. Il faudrait en outre surveiller en permanence le fonctionnement et la sécurité de ce système virtuel. Mais dans ce cas, seuls les informaticiens pourraient encore voter par e-voting. Car qui d'autre veut une telle solution pour son ordinateur personnel, à part les informaticiens eux-mêmes ? Et qui les contrôlerait ?

Une solution de vote électronique gelée, qui bloquerait toutes les autres connexions et fonctions et n'autoriserait aucune fonction d'administration, serait également envisageable en termes de

[8] Chevaux de Troie, logiciels malveillants, virus et leurs multiples appellations

sécurité. Mais c'est ce que craignent tous les fabricants de matériel informatique, car cette solution ne serait plus maintenable. Qui supporterait alors les coûts ?

2.7.7 Et les risques liés au téléphone portable ?

La prochaine étape dans notre société d'exigence sera de pouvoir voter non seulement chez soi, mais aussi à tout moment en déplacement. Qu'y a-t-il de plus à dire sur le téléphone portable ?

Tous les points faibles des ordinateurs existent aussi pour les téléphones portables. De plus, n'importe qui peut créer lui-même une application, la mettre sur l'Appstore et la proposer au téléchargement. Ces apps peuvent avoir accès à toutes les fonctionnalités et à toutes les données. Il n'y a plus de sécurité du tout, car les données sur le téléphone portable ne sont plus protégées.

2.7.8 Comparaison entre e-banking et e-voting

Toutes les discussions avec la CF indiquent que, selon son argumentation, le vote électronique doit être considéré comme l'e-banking. Il n'est certes pas sûr à 100%, mais si cela fonctionne aussi, pourquoi l'e-voting ne serait-il pas assez sûr ? On mise généralement sur la possibilité de contrôle et la réaction à ce contrôle. Mais quels sont-ils dans le cas du vote électronique ? La comparaison des éléments de sécurité entre l'e-banking et l'e-voting est sans appel :

- *La prévention : mesures de sécurité*

	E-banking	Vote électronique
en général	La banque connaît un comportement "normal" et peut identifier, remettre en question et/ou prévenir les écarts.	Il n'y a pas de comportement normal ou attendu, car ma voix ne m'est pas du tout attribuée.
En cas de perte des Account Credentials[9]	Généralement sécurisé par un code supplémentaire via le réseau de téléphonie mobile et un appareil séparé (téléphone portable).	Pas de sauvegarde par deuxième voie. Impression avec ID utilisateur par voie postale. Toutefois, même chose que pour le vote par correspondance.
En cas de perte de contrôle de l'ordinateur suite à une cyberattaque	Pas de sauvegarde préventive. Après constatation, le même type de dommage ne se produit toutefois qu'une seule fois. La banque prend en charge les mesures visant à empêcher le même type d'attaque.	Pas de garantie préventive. La constatation n'est pas garantie. Même lorsqu'elle se produit, il n'existe pas toujours de mesures pour corriger et prévenir la perte de confiance.

- *Le contrôle et la constatation de la fraude*

E-banking	Vote électronique
Je constate toujours mon préjudice et je peux prendre des mesures pour y remédier en collaboration avec la banque.	La société dans son ensemble peut constater un dommage sur la base de suppositions, mais n'a aucun moyen d'y remédier. La démocratie est suspendue.

- *La victime et la souveraineté de la réaction*

E-banking	Vote électronique
Mon compte manipulé me porte préjudice (uniquement). J'en ai le contrôle.	Ma voix déformée nuit à la société dans son ensemble. Elle ne peut - dans son ensemble - rien faire. La Chancellerie fédérale a le contrôle. Elle décide arbitrairement de la réaction.

2.7.9 Conclusion

Les initiés de l'informatique et nos services de renseignement le savent depuis longtemps, mais depuis les révélations d'Edward Snowden, tout le monde pourrait désormais le savoir : Avec une informatique en réseau, il est possible de faire pratiquement n'importe quoi, si les capacités des attaquants sont suffisamment grandes.

[9] ID utilisateur/mot de passe, ou données de la carte de vote. Elles peuvent être volées à grande échelle.

Le risque du vote électronique est que nous puissions perdre notre démocratie directe en raison de la possibilité de manipuler notre système de comptage. D'un point de vue social, ce risque n'est comparable à aucun autre. Il faut en mesurer les conséquences.

3 Les conséquences de l'introduction du vote électronique

Une éventuelle manipulation doit être précédée d'une décision politique dont l'issue est si importante pour le manipulateur potentiel qu'il n'hésite pas à investir dans une manipulation. J'estime qu'un million de francs suisses pour l'engagement de bons hackers pour l'effort initial de cette tâche, qui ne doivent pas nécessairement être payés selon des salaires suisses, suffira largement.

Il ne faut pas oublier, premièrement, que de nombreux outils de piratage sophistiqués sont déjà disponibles à bas prix aujourd'hui et, deuxièmement, que cet investissement constitue également un bon investissement pour d'autres manipulations futures.

3.1 Comment faut-il se représenter une manipulation ?

Aujourd'hui, on entend généralement par "manipulation" dans les débats politiques l'utilisation différente des médias et la différence de budget publicitaire entre les points de vue. On peut le comprendre ainsi. Mais qu'en est-il lorsque des organisations peuvent influencer directement les résultats d'une votation ?

Comment cela pourrait-il se produire ? On peut facilement imaginer deux manières :

A. Un **groupe d'intérêt** national cherche anonymement sur le Darknet un lien avec un groupe de pirates anonymes de catégorie 4.
   - Une transaction est négociée dans laquelle la performance et les prix sont fixés en bitcoin. La prestation consiste à manipuler quelques pourcentages de votants. Les pourcentages supplémentaires sont plus chers. Si le vote aboutit à un résultat positif, la transaction est considérée comme effectuée. Dans le cas contraire, le montant en bitcoins est remboursé.
   - Le fournisseur ne connaît pas le client et inversement. Les adresses IP sont masquées par une chaîne de centaines de milliers de serveurs TOR légaux et incontrôlables dans le monde entier, rendant ainsi impossible la localisation et la traçabilité.
   - Les manipulations doivent être développées, pratiquées et optimisées. On commence par de petits succès avec quelques centaines de résultats et on augmente progressivement en optimisant les algorithmes. Cela permet d'augmenter le prix.
   - Le paiement en bitcoins se fait également de manière anonyme et ne peut pas être suivi par une banque. Les bitcoins sont échangés quelque part dans le monde et à un moment donné par de toutes autres personnes.

B. Après avoir planifié une votation aux conséquences internationales, une **puissance étrangère** de cat. 5 peut aussi avoir l'idée, de sa propre initiative, d'influencer le développement politique de la Suisse en sa faveur.

Il faut savoir que même sur le Darknet, il existe au sein de la cybercriminalité une pratique commerciale "propre", basée sur la confiance mutuelle. Sans cela, ce secteur ne pourrait pas exister. Cela signifie que même en tant que client anonyme, vous pouvez vous attendre à une bonne qualité.

3.2 La perte de confiance dans la politique

Aujourd'hui déjà, des déclarations sont faites après chaque votation, selon lesquelles les résultats ont été obtenus exclusivement grâce aux efforts financiers du camp adverse. La plupart du temps, c'est la gauche qui en fait le reproche à la droite, généralement plus forte financièrement. Il est certain que toutes les organisations politiques mettent de l'argent dans la balance (publicitaire) pour obtenir un certain résultat. Les preuves que le succès des résultats est proportionnel à l'argent dépensé n'ont jamais vraiment pu être apportées. La droite nationale elle-même craint davantage l'influence étrangère sur la politique par la pression de l'adaptation aux normes internationales et de la soumission aux grands marchés et à leurs prémisses. (Les libéraux, en revanche, ne craignent généralement que les restrictions du libre marché).

Si l'on ajoute à cela la crainte que les résultats des votations soient directement achetés avec de l'argent, cette critique a soudain un tout autre fondement[10]. Comment le débat politique va-t-il évoluer en Suisse ? Aura-t-il vraiment un effet positif sur l'enthousiasme des jeunes pour la politique, comme le prétendent les partisans du vote électronique ? C'est le contraire qui se produira ! Le nombre de personnes qui reconnaissent le cyber-risque va augmenter. Ils mettront en garde, mais n'auront pas la possibilité de prouver de tels incidents en quantité, ce qui serait nécessaire pour démontrer de manière indubitable la manipulation des élections. Nous avons pondu un œuf avec un système qui permet la manipulation, mais qui ne peut jamais être prouvé ! Et une fois que l'e-voting est introduit, comment peut-on le supprimer ? Avec le vote électronique ? Dans quelle direction la manipulation aurait-elle lieu ?

Le temps viendra où il y aura un décalage entre la vérité publique et ce que les gens savent. Officiellement, on affirmera que tout va bien, car le contraire n'a jamais été prouvé. Mais les gens savent que ce n'est probablement pas le cas, mais ils ne peuvent plus rien y faire. N'avons-nous pas connu de telles conditions à l'époque de la guerre froide dans le bloc de l'Est ?

Peut-être voterons-nous un jour sur une interdiction (avec le vote électronique, bien sûr) de contester et de critiquer les résultats des votations, et ce, bien sûr, uniquement pour des raisons de paix politique... Et à votre avis, cher(e) lecteur(trice), quel sera le résultat ?

L'ère des faits alternatifs a déjà commencé, elle mènera à une ère de mondes alternatifs où les gens craindront un débat politique. Est-ce ce que nous voulons ?

3.3 Le site économique

La situation politique restera-t-elle stable si, à l'avenir, non seulement quelques fous racontent que la démocratie ne fonctionne pas du tout en Suisse, mais si de plus en plus de gens savent que cela pourrait bien être le cas, mais qu'il est impossible de le prouver ? Quelle sera la réaction de l'État et celle de la population et de l'économie ?

3.4 Le trou financier sans fin

On trouvera toujours - comme pour tous les systèmes informatiques - quelque chose à améliorer dans le système de vote électronique. Les coûts d'exploitation augmenteront considérablement. Un service d'assistance pour tous ceux qui ont un problème sera nécessaire. Nombreux sont ceux qui

[10] Staline : "Ce n'est pas celui qui vote qui détermine le résultat, mais celui qui dépouille".

affirmeront que leur ordinateur ne fonctionne pas correctement ou qu'ils ont mal voté. Il faudrait enquêter sur chaque cas individuel, même si les cas signalés ne représentent qu'une fraction des cas effectifs, dont certains sont certainement faux. On ne pourra jamais vraiment le faire, mais on prétendra que l'on fait tout pour rendre la technique sûre. Cela engloutira de l'argent sans fin, sans résultats mesurables ou pertinents.

L'électeur suisse dans la pampa argentine a lui aussi le droit de faire vérifier que le décompte est correct. Qui paie cette dépense ? Y aura-t-il un jour une ordonnance stipulant que chaque électeur est lui-même responsable de son installation et qu'il doit en payer lui-même les frais d'exploitation ?

3.5 La mondialisation signifie-t-elle l'abolition de son propre espace juridique ?

Ou bien le fait que les votes soient intègres ou manipulés n'aura-t-il un jour plus aucune importance, car il n'y aura de toute façon plus rien d'important à voter ? Tout ce qui est important est défini par des normes internationales et des organisations supranationales et nous devons être présents partout, sinon le marché sera restreint ?
Avec le discrédit croissant du processus politique en Suisse, nous courons le risque de ne plus rien pouvoir opposer à cette tendance, même là où cela resterait possible et nécessaire.

4 Les causes de l'absence de protestation

Pourquoi n'y a-t-il pas plus de citoyens qui protestent contre cette folie sociale, qui équivaut pour ainsi dire à un suicide politique national à retardement ?

4.1 Le ventre et la tête

Chaque personne a ses propres expériences. Soit il les a traitées et classées dans sa tête. Ou bien il les a vécues mais ne les a pas encore traitées rationnellement. Dans ce cas, elles sont stockées dans le ventre et donnent lieu à une "intuition". Une manipulation sociale comme celle du vote électronique ne fait généralement pas partie d'une expérience vécue. On a entendu parler de cas, mais soit on les considère comme des cas isolés, soit ils sont controversés et dépendent de l'optique subjective de chacun, soit on considère tout au plus que les rapports à ce sujet sont exagérés. Quoi qu'il en soit, ce n'est pas une raison pour changer sa vision crédule du monde. Dans de nombreux cas, la devise suivante s'applique : *ce qui ne doit pas être ne peut pas être.*
Ce n'est que lorsque les tripes et la tête pointent dans la même direction que l'on obtient une image claire pour se forger une opinion.

4.2 La confiance dans les autorités

La confiance dans les autorités est en principe très grande et lorsqu'une conseillère fédérale, ancienne ou en exercice, émet une recommandation, celle-ci pèse des tonnes sur la décision du citoyen lambda. Le livret de vote de la Chancellerie fédérale a déjà fait l'objet d'un article : Comme il est si bien fait sur le plan méthodologique, les déclarations de fond ne sont guère mises en doute.

Les déclarations suivantes de la Chancellerie fédérale soutiennent la volonté d'acceptation du vote électronique :

Argument BK	Commentaire/Réponse
Nous ne faisons que des petits pas. Notre devise est "la	Oui, le projet traîne en longueur lors de son introduction,

sécurité avant la vitesse", Nous avons mené des consultations.	mais sans que les plus grandes lacunes en matière de sécurité n'aient été abordées. Les consultations n'ont concerné que les groupes d'intérêt, c'est-à-dire les partisans.
Jusqu'à présent, rien ne s'est passé, les tentatives ont toutes été couronnées de succès	1. la Chancellerie fédérale (ou les cantons) n'a tout simplement rien remarqué 2. la Chancellerie fédérale (ou les cantons) ne pourrait jamais s'apercevoir de rien non plus 3. lors de la phase de test de 2016, seuls 2% environ des électeurs étaient connectés au vote électronique. Cela ne constitue pas une plateforme pour une manipulation réussie. C'est pourquoi une telle affirmation n'a aucune valeur.
Pour le développement complet, nous comptons sur la vérifiabilité. C'est-à-dire que chaque électeur peut constater si son vote est bien arrivé. Cela doit suffire, car la sécurité absolue n'existe pas en informatique.	1. le conseiller technique Prof. Hänni FH BE a contesté[11] à juste titre l'atteinte de la vérifiabilité "à court et moyen terme". Voir aussi 2.7.6. 2. 30 % de l'électorat peuvent être intégrés même sans possibilité de vérification. Mais cela représente déjà une menace importante pour la manipulabilité.

On ne peut tout simplement pas s'imaginer que le Conseil fédéral ne dispose pas de la meilleure des informations pour se forger une opinion et qu'il n'en tienne pas compte. On ne sait souvent pas non plus que les offices se méfient les uns des autres et qu'ils s'ignorent parfois. La Chancellerie fédérale ne dispose même pas des ressources nécessaires pour un grand projet informatique. L'OFIT, l'USIC et la BAC ont des capacités bien plus importantes, mais même là, des projets informatiques ont déjà dérapé.

4.3 La complexité et l'ignorance

Si Mme Merkel a qualifié l'Internet de "terre inconnue" en 2013, il convient d'évaluer le niveau de connaissances des représentants des autorités en matière de problématiques informatiques. Ceux-ci dépendent donc entièrement de représentants de haut niveau de la science ou de l'économie. Mais quels intérêts ces derniers représentent-ils et les comprennent-ils correctement ?

Le vote électronique lui-même est déjà extraordinairement complexe en raison de la technique de sécurité sophistiquée au niveau de l'application. La complexité d'une manipulation semble à première vue encore plus complexe et donc hors de notre capacité d'imagination. C'est pourquoi le risque ne peut pas non plus être évalué correctement. On oublie toutefois qu'il suffit d'analyser les maillons les plus faibles de la sécurité pour évaluer le risque. Ceux-ci ont été cités en détail dans ce document.

4.4 Le plaisir de la nouveauté et la foi inébranlable en la technique

Qui voudrait nager à contre-courant ? Ceux qui lancent les tendances les lancent et ils ont toujours raison. Beaucoup de gens trouvent toujours le nouveau meilleur que l'ancien, peut-être quand ils ne vont pas très bien ou quand ils sont au début de leur vie. L'énorme influence que les technologies modernes ont apportée dans la vie de tout un chacun entraîne une dépendance vis-à-vis d'elles et, souvent, on oriente aussi son système de valeurs en fonction d'elles. Bien sûr, il est indéniable que ces réalisations ont également apporté d'énormes progrès dans la vie de tout un chacun.

[11] http://www.inside-it.ch/articles/28545

Mais ce n'est qu'avec une certaine maturité que l'on reconnaît aussi les risques qui ne sont décrits que comme une construction abstraite et dont les conséquences ne peuvent guère être vécues directement par soi-même.

4.5 Les lobbies en lice

Les Suisses de l'étranger ne se lassent pas d'exprimer leurs revendications quant à leur participation à la formation de la volonté politique en Suisse. Comme la poste à l'étranger n'est pas partout assez rapide pour que l'on puisse s'informer, voter et renvoyer l'enveloppe à temps, il faut absolument mettre en place l'e-voting.

Les représentants IT peuvent éventuellement se promettre des commandes lucratives pour la livraison, la mise en service, l'utilisation, l'exploitation et le service d'une telle installation. Ils feront tout pour prouver leur compétence en matière de sécurité informatique et tenteront peut-être toujours de contribuer à l'amélioration partielle de certaines problématiques par de nouvelles idées.

On ne peut pas reprocher à toutes ces personnes de faire passer leurs propres intérêts avant ceux de la société dans son ensemble. J'attends toutefois des représentants des autorités une attitude résolument opposée.

4.6 Le manque de conscience de la sécurité

Lorsque l'on met en garde contre des agissements criminels, le citoyen lambda a souvent le réflexe de dire : "*Nous avons la police et la justice pour cela ! Nous n'avons pas besoin de nous occuper de cela en politique.*

Mais on oublie que ces instances ont de très mauvaises cartes à jouer lorsqu'il s'agit de criminalité organisée, et encore plus lorsqu'elle se déroule en grande partie sur le territoire étranger. Elles ont de bonnes cartes en main lorsqu'il s'agit d'attraper les automobilistes qui ne respectent pas les règles de stationnement et de vitesse, car elles peuvent surveiller les parkings et les routes sans aucune restriction. Ils ne peuvent pas surveiller les ordinateurs, ou alors seulement si quelque chose de concret s'est déjà produit. Mais comment peut-on constater quelque chose si la surveillance "préalable" n'est pas autorisée en raison de la protection des données ? Le chapitre "Facteurs favorisants" (du risque) décrit les difficultés rencontrées par la police et la justice.

Il serait illusoire de croire que des manipulations sur les ordinateurs des électeurs pourraient être détectées, même si ces dispositions de protection des données n'existaient pas. Exiger la sécurité informatique à la maison à titre de prévention dans cette situation est certes une belle idée, mais elle n'a aucune chance non plus, car elle n'est pas vérifiable à un coût raisonnable et va même à l'encontre de la protection des données.

4.7 Quels sont les groupes de personnes qui soutiennent le vote électronique ?

En conclusion, j'aimerais distinguer les catégories suivantes de personnes qui soutiennent le projet de vote électronique, chacune avec sa propre argumentation :

Groupe	Leurs arguments	Contre-arguments
Ignorants	Qu'est-ce que c'est, une cyber-attaque ?	La technologie de la cyberattaque a fait autant de

d'Internet, crédules, croyants en l'autorité, Fidèle à la technique	Il ne s'est rien passé jusqu'à présent, pourquoi se passerait-il quelque chose à l'avenir ? Même en Amérique, on n'a pas pu prouver qu'il y avait eu un piratage lors du dépouillement des élections présidentielles de 2016.	progrès que l'informatique elle-même. Le criminel est à la manœuvre, il ne respecte aucune règle contrairement à notre propre État. Le Service de renseignement de la Suisse considère la cybermenace comme l'un des dangers dominants pour la Suisse. La prise d'influence directe dans les décisions populaires est le mode de manipulation le plus efficace. La sécurité n'est pas seulement une question de technologie. L'homme et tout l'environnement en font partie. La flexibilité et la commodité vont à l'encontre de la sécurité dans son essence même.
	Les cyber-attaques ne sont qu'un risque théorique. Ce serait bien trop compliqué et coûteux. On peut manipuler les gens autrement.	
	Les autorités veilleront à ce que ces produits soient sûrs.	
	La sécurité informatique s'améliore de plus en plus. Pour l'instant, il y a certes encore des problèmes, mais ils seront bientôt résolus.	
Fonctionnaires et optimiseurs d'efficacité	Les milieux intéressés peuvent prendre position dans le cadre de consultations De longues phases de test garantissent l'élimination des erreurs Nous avons un règlement qui régit le vote électronique. Nous devons suivre ce règlement et ne pas le mettre en doute. Il y a un moyen politique de lutter contre cela, si on le veut. Je ne suis pas responsable de l'évaluation de la société dans son ensemble.	La croyance inébranlable en la méthodologie parfaite de l'appareil d'État empêche de voir les relations sociales globales lors de l'évaluation des risques. Les décisions politiques ne sont en effet pas prises par le fonctionnaire, mais au niveau supérieur. Or, le sens des responsabilités des hauts fonctionnaires fait souvent défaut. Ils font passer leur opinion après leur devoir. L'amélioration de l'efficacité semble être pour eux le problème dominant qui touche à leur devoir.
	Nous pouvons enfin fournir le résultat des votes rapidement et à moindre coût !	
Les citoyens ordinaires et les technophiles en profitent	Suisses de l'étranger : nous pouvons enfin voter nous aussi ! Nous acceptons le petit risque ! Génération mobile : enfin, on regarde aussi pour nous ! Peut-être nous intéresserons-nous alors davantage à la politique.	Le fait de se focaliser sur son propre bien-être empêche de voir le contexte social dans son ensemble.
	fournisseurs informatiques : C'est une technique très intéressante. Nous aurions encore quelques idées de solutions à vendre...	
Utopistes et progressistes	Vous êtes tout simplement toujours contre la nouveauté : des ploucs et des rétrogrades ! Donnez donc une chance à l'avenir !	La foi inébranlable dans la nouveauté empêche de voir les risques énormes qu'elle implique. On ne peut pas tout essayer une fois et voir ensuite comment cela fonctionne. Le vote électronique ne disparaîtra jamais !
Élitaristes, "citoyens du monde	Le peuple n'est de toute façon pas en mesure d'évaluer correctement les projets politiques compliqués. Nous sommes pour une standardisation mondiale du droit. Il n'y a de toute façon plus de place pour une action nationale isolée. Le vote électronique n'est donc pas un sujet pour nous.	La démocratie directe est encore en vigueur ! Si un tel ordre mondial existait, il faudrait abolir la démocratie et non pas introduire le vote électronique !
Fatalistes	Les votes sont de toute façon manipulés par l'argent et les médias. Si maintenant la cybercriminalité s'en mêle, on n'aura pas perdu grand-chose de plus.	Cette attitude est dépourvue d'essentialité lorsque les faits sont avérés. Certes, les opinions peuvent être manipulées, mais jusqu'à présent, le décompte des opinions est au moins intègre !

Les utilisateurs potentiels des manœuvres cybercriminelles ne sont pas mentionnés ici, car ils ne représentent eux-mêmes qu'une infime minorité.

5 Conclusion

On a l'impression que depuis 2000, la Chancellerie fédérale tente de se faire un monument avec cette innovation en passant par des phases de test qui durent des années. Certes, on attribue toujours le rythme retardé aux problèmes de sécurité qui ne sont pas encore résolus, mais en même temps, le Conseil fédéral a été encouragé avec succès à prendre un engagement clair en faveur du vote électronique.

Apparemment, malgré les nombreux cas spectaculaires de cyberattaques, malgré les révélations d'Edward Snowden, le Conseil fédéral n'est toujours pas suffisamment conscient des risques liés aux systèmes informatiques sur Internet en général. Il pense peut-être qu'en Suisse, nous construisons déjà des systèmes plus sûrs que dans le reste du monde. Ou alors, il partage la croyance répandue en maints endroits selon laquelle le progrès des technologies apporterait toujours plus de sécurité. Malheureusement, l'actualité confirme qu'il n'en est rien. La criminalité mondiale et la politique de puissance des grandes puissances vont exactement dans le sens inverse : seuls les petits hackers sont de plus en plus entravés, les grands deviennent de plus en plus puissants.

L'application "e-voting" est certes déjà construite selon les dernières connaissances en matière de sécurité informatique. Mais le point le plus faible reste l'ordinateur de l'électeur/trice et son système d'exploitation, qui ne permettent pas de demander et de vérifier des données importantes, notamment en raison de la protection des données. Mais l'ordinateur manipulé manipulera aussi l'utilisateur ! Qui ne suit pas les instructions de l'ordinateur mais celles du livret d'instructions ? Le risque résiduel est certes connu de la Chancellerie fédérale, mais le processus politique fait que la responsabilité des conséquences n'y est pas assumée, mais largement répartie : Au Parlement, qui doit adopter la loi, aux cantons, qui sont responsables de l'utilisation du système et donc de l'exactitude des décomptes, aux votants eux-mêmes, qui sont eux-mêmes responsables si leur ordinateur génère un faux vote et qu'ils ne le remarquent pas. En effet, tout dépend de ce que l'on appelle *la vérifiabilité,* c'est-à-dire la possibilité pour l'électeur/trice de constater sans aucun doute si le vote a été exprimé comme il le souhaitait. On n'exige pas qu'il le fasse, mais seulement qu'il le puisse. On oublie que nous dépendons tous du fait que tous les votants soient correctement comptés et pas seulement le nôtre à chaque fois.

Ce projet est extrêmement dangereux pour la Suisse : avec l'e-voting, nous nous dirigeons vers l'abolition insidieuse de la démocratie directe, vers la fin d'un ordre politique stable et peut-être aussi vers la fin d'une place économique prospère. J'en appelle à la responsabilité démocratique de tous et je lance un appel pour mettre fin à ce projet funeste !

6 L'appel

Rien n'y fait : si le Parlement n'est pas en mesure de rejeter en bloc une loi visant à introduire le vote électronique, nous devons, en tant qu'électeurs, nous défendre avant que cette absurdité ne se répande dangereusement. Nous avons besoin d'une interdiction du vote électronique, comme l'a décidé la Cour constitutionnelle allemande. (L'Allemagne n'est pas non plus connue pour ne pas vouloir faire de progrès technologique).

- **Rejetez cette loi lors du référendum !**
- **Nous voulons conserver la démocratie directe !**
- **Les cantons conservent la souveraineté sur le dépouillement des votes !**
- **Le décompte des voix doit rester vérifiable !**
- **Nous en avons assez des projets informatiques coûteux et non réfléchis de la Confédération !**

Vers l'auteur :

Ingénieur électricien diplômé EPF René Droz, 64 ans, a dirigé pendant 10 ans le Computer Emergency Response Team militaire au sein de l'aide au commandement du DDPS. Il dispose de 28 autres années d'expérience professionnelle dans l'industrie et l'administration dans les domaines de la technique de réseau et de la sécurité informatique.
Il est aujourd'hui à la retraite et s'engage bénévolement pour les causes politiques qui concernent

