Thèses sur le vote électronique [Droz]

1. **Le vote électronique est une approche absurde, car le vote et les élections ne sont pas simplement des actes administratifs** qui doivent être optimisés, ils sont la souveraineté de l'électeur. Le moindre doute sur l'authenticité des processus est intolérable. Le vote électronique résout tout au plus un petit problème, mais en produit un bien plus grand : la perte de confiance du citoyen dans l'institution de la démocratie par le biais de doutes sur l'exactitude des résultats.

2. **La cyberguerre existe et n'est pas une fantaisie de théoriciens du complot**. Il existe une scène criminelle mondiale à vocation commerciale et une scène politico-stratégique dans laquelle les grandes puissances s'assurent de leurs ambitions d'exercer une influence. Il n'y a pas de protection contre les meilleurs de ces acteurs dans un environnement informatique grand public. (Internet Vrb/ Systèmes d'exploitation principaux / Navigateur). L'entrée et la sortie sont sous le contrôle du système d'exploitation ou du navigateur qui peut être attaqué.
   Exemples :
   a) Stuxnet : Les Américains et les Israéliens manipulent avec succès la production de centrifugeuses iraniennes avec des activités cybernétiques. Détails épicés : (1) Les installations n'étaient même pas en ligne sur Internet. Les activités ont été réalisées via la logistique des clés USB. (2) Sans la volonté politique pénétrante des Israéliens, cet incident n'aurait jamais été porté à l'attention du public.
   b) Wannacry : Les pirates de la scène criminelle parviennent à contrôler 200 000 ordinateurs en une journée. Là il s'agissait de chantage, avec ce moyen on aurait atteint aussi tous les autres buts de la manipulation de l'écran.
   c) Cas du DFAE 2012-2014 : un service de renseignement étranger parvient à extraire des données sensibles du département polonais, ce qui est passé inaperçu pendant 2 ans et n'a été découvert que par hasard. L'informatique de l'administration fédérale n'est donc en aucun cas mieux protégée que d'autres en Suisse ou à l'étranger.

3. **La cryptologie utilisée dans la solution de vote électronique peut** au mieux assurer des flux de données de bout en bout, mais **pas l'entrée/sortie de l'ordinateur, pas sa disponibilité et pas la compréhension correcte du comportement correct de l'utilisateur.**
   - Les manipulations à l'écran incitent l'électeur à soumettre le code de confirmation plus tôt ou à s'abstenir de vérification, selon son comportement de vote. Ces cas peuvent difficilement être détectés. Les messages à ce sujet arrivent par hasard.
   - La soumission du code de confirmation peut être supprimée par des codes malveillants, ce qui rend le vote invalide. L'utilisateur pourrait le remarquer (code de finalisation manquant), mais reçoit un message rassurant à l'écran et est satisfait.

4. **La sécurité holistique dans le centre informatique** ne consiste pas seulement en l'intelligence de la solution applicative, sur laquelle le BK attire l'attention à plusieurs reprises. Toutes les parties de l'informatique centrale **devraient faire l'objet d'un contrôle de sécurité**. Comme cela doit faire l'objet d'un processus de renouvellement dynamique (faute de quoi les contrats de maintenance ne peuvent être exécutés), un contrôle de sécurité complet devrait être effectué dans ***chaque canton et avant chaque vote***. Cela coûterait énormément d'argent. Les entreprises cantonales n'ont pas les moyens, mais ne sont pas conscientes de la nécessité d'une telle cyberdéfense. Cet examen de la sécurité comprenait, entre autres :

- Vérification de la vulnérabilité de tous les systèmes du siège social.
- Vérification de la mise à jour de tous les systèmes et des progiciels de vote électronique au siège social.
- Contrôles permanents d'accès et d'accès et vérifications périodiques de toutes les interventions sur tous les systèmes par plusieurs chefs qui se contrôlent les uns les autres.

De plus, vous devriez faire ce qui suit à un seul endroit :

- Vérification du code source de l'application e-voting après chaque mise à jour (4-12 semaines de travail)
- Le code source n'a toujours pas été publié.

5. **Si des cyberattaques sont signalées, la Confédération et les cantons sont immédiatement submergés.** Toute décision gouvernementale sur la façon de procéder deviendra arbitraire, car aucune information suffisamment précise ne sera disponible. La confiance dans le fonctionnement de la démocratie ne peut se réaliser que par un comptage clair et précis.
    - Chaque message comporte à la fois un facteur d'incertitude et un nombre non déclaré. Le nombre de cas non signalés ne peut même pas être estimé. Un seul examen médico-légal d'un PC piraté prend environ 1 à 2 semaines et un résultat négatif pourrait également être dû à un brouillage minutieux de toutes les traces.
    - Si l'on parvient à la conclusion des autorités qu'il y a trop peu de rapports pour renverser le résultat, l'accusation d'arbitraire est déjà dans la salle en raison du manque d'exactitude de l'estimation du nombre de cas non déclarés.
    - Si l'on arrive trop vite à la conclusion du côté officiel, le vote est truqué et réélu, l'accusation d'arbitraire est également faite, car la partie perdante pourrait en bénéficier.

Cognition :

L'informatique d'aujourd'hui ne peut être protégée, mais la démocratie a droit à une protection totale.

Conséquences :

Aujourd'hui, le vote électronique doit être désactivé. Un réexamen ne peut être envisagé que lorsque les objections ci-dessus sont obsolètes.