Vernehmlassung zur Wiedereinführung des E-Voting Probebetriebes

Termin: 28.08.2021

WEB: Neue Verordnung BK 2021 über die elektronische Stimmabgabe (noevoting.ch)
(3sprachig, offizielle Version deutsch)

Von René Droz
Inhalt
Management Summary

Management Summary

Der Dialog mit der Wissenschaft hat die Problematik nun auf ein angemessenes wissenschaftliches Niveau gebracht. Die Komplexität findet in der Verordnung und deren Anhang durchaus einen angemessenen Ausdruck. Nicht erkannt werden die politischen Folgen einer solchen Komplexität. Den Kantonen, die niemals alle die notwendigen Ressourcen dafür bereitstellen können werden die Überprüfung all der hochkomplexen Massnahmen aufgebürdet, die daraus zu folgen hätten. Deren Risiko-Management wird deshalb mit untragbaren Kompromissen an die Sicherheit enden. Damit kann das Vertrauen in das E-Voting nicht gewonnen werden.

Die systemisch verbleibenden 6 Mängel des E-Voting im Einzelnen:

[1] Die Entdeckung von **Lecks und der Diebstahl von Zugangscodes** zur Abstimmung können von Benutzern auf der ganzen Welt begangen werden. Solche Angriffe sind schwer zu erkennen und können mit der aktuellen Lösung nicht wirksam verhindert werden. Das Recht des Nichtwählers, die Nutzung seiner allfällig fälschlich abgegebenen Stimme überprüfen zu lassen, ist dabei nicht praktikabel.

[2] Die Folgen von **unsicheren Endgeräten** trägt nicht nur der Benutzer selbst, sondern auch das **Kollektiv der Stimmbürger**. Insbesondere gehört auch das Abstimmgeheimnis hiezu.

[3] Das **Ausmass einer Manipulation** kann niemals festgestellt werden. Dadurch ergibt sich ein riesiges Potential an Verunsicherung bei jeglichen Unregelmässigkeiten. Es besteht deshalb Grund für Misstrauen gegenüber Anbieter und Behörden in Bezug auf Transparenz.

[4] Die Funktion einer **Wahlkommission** im bestehenden Sinne kann nicht mehr stattfinden. Es sind nur noch höchstqualifizierte IT-Experten und Mathematiker, die etwas zur Gültigkeit des Abstimmungsvorganges sagen können. Deren Kompetenz und Redlichkeit unterliegen keinerlei demokratischer Legitimation.

[5] Das **Zeitfenster** für Abklärungen bei Meldungen von möglichen Manipulationen wird immer zu klein sein, um in jedem Fall rechtzeitig die Gültigkeit von Wahlen und Abstimmungen zu kommunizieren.

[6] Ein Probebetrieb wird jahrelang für Anbieter und Nutzer stark defizitär ausfallen. Wenn die definitive Einführung auf einer guten System-Sicherheit basieren soll, so ist das Ende des Probebetriebes kaum abzusehen. **Nutzen und Aufwand** stehen in einem dramatisch schlechten Verhältnis.

NEIN, die Demokratie muss nicht per se digitalisiert werden. Sie ist kein Verwaltungsablauf. Es geht da einzig um das Vertrauen in den wichtigsten der politischen Prozesse. Insbesondere wenn wir das Abstimmungsgeheimnis bewahren wollen kann E-Voting nicht in Frage kommen.

1. Einleitung

Gerne nehmen wir die Einladung zur erneuten Stellungnahme zur vorgesehenen Wiederaufnahme des Versuchsbetriebes E-Voting an.

1.1. Autor

Der Autor René Droz[1] war zwischen 2005 und 2015 verantwortlich für die Einführung und die Leitung der operativen Cyber Defense in der Armee (milCERT). Er befasst sich seit 5 Jahren mit dem E-Voting und gehörte dem Initiativ-Komitee „Für eine sichere und vertrauenswürdige Demokratie“ an. Er hat im Namen des Initiativ-Komitees auch die „Vernehmlassung über das neue Gesetz zu den politischen Rechten“ verfasst.

1.2. Ausgangslage beim E-Voting

Dass die direkte Demokratie zu den vorrangigsten Errungenschaften der Eidgenossenschaft gehört, ist hierzulande wohl kaum bestritten. Die Einführung eines E-Voting ist deshalb mit allen auch nur denkbaren Vorsichtsmassnahmen zu versehen. Von den Cybergefahren wird zwar viel gesprochen, aber das Ausmass der möglichen Bedrohungen wird nur von den besten Experten einigermassen angemessen erkannt.

Grundsätzlich ist die IT heute nicht mehr vollständig zu sichern, weil es unmöglich ist, auf nicht unter Kontrolle stehende Mainstream-Komponenten zu verzichten. Man müsste die gesamte IT neu erfinden, um wirkliche eine Kontrolle aller Prozesse zu bekommen, um so die Sicherheit zu gewährleisten. Das ist nicht realistisch. Heute wird nur deshalb IT erfolgreich und doch mit meist genügender Sicherheit betrieben, weil es in fast allen Bereichen kontrollierbare Ergebnisse gibt. So wird das Risiko begrenzt und ist daher statistisch einsehbar und managebar.

Beim E-Voting – das ist sozusagen der einzige öffentliche Bereich mit diesem Kriterium der fehlenden Kontrollierbarkeit - ist das nicht der Fall. Durch das Abstimmungsgeheimnis ist eine öffentliche Kontrolle nicht möglich. Auch wenn gewisse Experten versuchen, diese Kontrolle elektronisch nachzuvollziehen, so entgeht sie doch **in jedem Fall** einer demokratischen Kontrolle durch die Öffentlichkeit. Die Funktion einer Wahlkommission findet in der ursprünglich vorgesehenen Form nicht mehr statt.

Der Versuch E-Voting sicher zu machen, gleicht der Quadratur des Kreises. Man kann immer näher kommen und wird es doch nie erreichen. Da es keine sichere IT per se gibt, kann man versuchen, alle dazugehörigen Prozesse zu sichern mit ganz viel Kompetenz und das Vertrauen zu gewinnen mit ganz viel Transparenz. Man muss sich lösen von der Vorstellung, es gebe irgendwann von irgendwem ein „sicheres IT-System“ und damit sei dann das Problem gelöst. Das „System“ umfasst nämlich immer auch sämtliche Inbetriebsetzungs- und Betriebs-Prozesse und die sind dynamisch zu betrachten, menschengesteuert und umfassen eine Unmenge an immer wieder neuen technischen Eingriffen, bei denen jeder einzelne fatale Folgen haben kann. Weil durch die einseitige Kommunikation der

[1] www.Noevoting.ch

Verwaltungen (Bund + Kantone) diese Tatsache in der öffentlichen Wahrnehmung weitgehend unbekannt ist, werden die unausweichlichen Konsequenzen nur von einer Minderheit erkannt. Wenn man diese Konsequenzen alle verhindern will, ergibt das aufwändige, langwierige Prüfverfahren, die an Komplexität kaum noch zu überbieten sind.

Um diese Problematik zu erkennen und der breiten Öffentlichkeit zugänglich machen zu können, könnte der Versuchsbetrieb ein geeignetes Gefäss werden.

1.3. Das verlorene Vertrauen

Versprechungen und Zusicherungen, dass E-Voting viel sicherer sei, als das, was wir heute hätten, hörten wir von der engagierten Bundesseite und den kantonalen Befürwortern über viele Jahre. Nicht zuletzt deshalb hatte E-Voting lange Zeit eine gute Zuspruchs-Quote. Unterdessen sieht diese wesentlich zweifelhafter aus. Zwar kann man die Lernfähigkeit der Bundeskanzlei nicht absprechen. Wie kann aber der Stimmbürger nach all diesen Jahren insgesamt den gleichen Personen Vertrauen entgegen bringen, die das heute wieder postulieren für ein System von morgen, das noch gar keiner kennt? *„Die Erfahrungen mit den bisherigen Systemen seien nützlich gewesen“*, heisst es von dieser Seite. Effektiven Nutzen hat die Erkenntnis, dass man den Zusicherungen auch von Bundes-Seite nicht blind vertrauen kann. Die Erkenntnis, dass es Firmen gibt, welche Systeme entwickeln, die sie nicht genügend verstehen und andere, welche noch dazu Zertifikate ausstellen, bringt ausserdem tatsächlich den notwendigen Realitätssinn in die Diskussion.

1.4. Der alte und neue Versuchsbetrieb

Einerseits war und ist unbefriedigend, dass der bisherige Versuchsbetrieb ohne verfassungsmässige Grundlagen für den neuen Stimmkanal und damit auch ohne Volksentscheid eingeführt wurde. Man kann einräumen, dass ohne Versuchsbetrieb all die Notwendigkeiten zur Wahrung der Sicherheit kaum in der notwendigen Tiefe definiert und umgesetzt werden könnten, d.h. rein auf theoretischen und wissenschaftlich bekannten Erkenntnissen. Der alte Versuchsbetrieb sollte offenbar wesentlich zur Vertrauensgewinnung beitragen. Dass dies 2019 deutlich schiefgegangen ist, liegt u.E.

- An der Fehleinschätzung der Cybergefahren
- An der Überschätzung von Zertifizierungsstellen
- An der mangelnden Transparenz gegenüber den interessierten Stellen
- An der mangelnden Wissenschaftlichkeit der technischen Grundlagenerstellung
- An der Expertenzusammensetzung

Die Opposition gegen den Versuchsbetrieb als solchen war andererseits auch begründet in dem viel zu grossen Anteil des Elektrorates, welcher in keiner Branche der Wirtschaft für Testversuche zur Anwendung käme. Jetzt ist dieser reduziert worden, was begrüsst wird.

Die kommenden absehbaren Fehler beim Versuchsbetrieb dürfen auf keinen Fall Raum geben für Zweifel an der Authentizität der Gesamt-Ergebnisse an den Urnengängen. **Deshalb ist nicht zu begrüssen, dass die Auslandschweizer offenbar nicht bei den 10 % Anteil mitgerechnet werden sollen.** Damit erhöht sich u.E. die Manipulationsgefahr wiederum zu deutlich bei einem System, das noch nicht die einmal zu definierenden minimalen Anforderungen erfüllen muss.

1.5. Übrige Punkte bei der neuen Aufgleisung E-Voting

Der Bund hat mit seinem Massnahmenkatalog[2] Gefässe geschaffen, welche es erlauben sollen, die Risiken des E-Voting zu minimieren. Die neuen Anforderungen bestehen offenbar im Wesentlichen aus folgenden Neuerungen:

1. *Transparenz: Es wird gefordert, dass alle Teile eines E-Voting Systems (d.h. die Software-Bausteine) in der Öffentlichkeit einsehbar und verfügbar sind, so dass jedermann sich von der Unbedenklichkeit selbst überzeugen kann.*
2. *Permanente Überwachung und Prüfung der Systeme: Nicht eine einmalige Prüfung muss das System bestehen, sondern es kann jederzeit neu geprüft und beurteilt werden.*
3. *Eine Gruppe von unabhängigen Wissenschaftlern beobachtet die weitere Entwicklung und berät die Bundeskanzlei mit Bezug auf die Sicherheitsproblematik.*
4. *Das Ziel der Sicherheitsbestrebungen ist nicht die absolute Korrektheit der Resultate, sondern die „vollständige Verifizierbarkeit".*
5. *Interessierte Gruppen können jederzeit Fehler suchen und erhalten Geld, wenn sie welche finden („Bug Bounty Programm").*

Die Punkte 1-3 gehören zu industriellen IT –Sicherheits-Standards und werden selbstverständlich begrüsst.

Der Punkt 4 ist in der Praxis nur ausgesprochen aufwendig erreichbar (s. 4.1.4). Der verwendete Begriff gaukelt der Öffentlichkeit vor, der Stimmbürger selbst und die Behörde könnten Manipulationen an der korrekten Zählung der Stimmen entdecken. Das war bisher nicht einmal für die eigene Stimmabgabe möglich. **Lediglich die Manipulation *bei der Erstellung und Übertragung* der Daten – hätte man theoretisch selbst entdecken können.** Das wären dann entdeckbare Manipulationen beim Handy oder Heimcomputer. Für eine individuelle Verifizierbarkeit bräuchte man zusätzlich mindestens eine öffentliche Liste der Voting Codes („Public Voting Board") mit der jeweiligen Stimme oder Wahlabgabe. Da ja jeder nur den eigenen Voting Code kennt, könnte jeder so die Auszählung für sich selbst prüfen, ohne dass das Abstimmgeheimnis dadurch in relevantem Umfange gefährdet wäre. „Vollständig" ist die Verifizierbarkeit aber trotzdem nicht, solange nicht sichergestellt ist, dass alle gezählten Stimmen zu authentischen Stimmbürgern – die wirklich gewählt haben- zugeordnet werden können und jeder nur eine Stimme hat. Aber auch die „Vollständige Verifizierbarkeit" bringt nicht das Vertrauen zurück, wenn (a) nicht nachvollziehbar und mehrheitsfähig geregelt ist, was im Falle einer negativen Verifizierung (insbesondere auch beim „Public Voting Board") geschehen soll und (b), wenn auch im Nachhinein **nicht festgestellt werden kann, welches Ausmass eine potentielle Manipulation überhaupt haben könnte.** Für beides ist leider keinerlei vernünftiger Lösungsansatz erkennbar. Im Gegenteil: Das Einzige, was in diesen Fällen sicher ist, ist die Tatsache, dass solche Feststellungen grösstmögliche Verunsicherung im Stimmvolk zur Folge hätten. Die weitere Folge davon ist, dass eine Verschleierung von Problemen für jeglichen Provider und auch die staatlichen Stellen opportun ist. Und das wiederum fördert jedes Misstrauen ins Gesamtsystem „E-Voting".

Der Punkt 5 wird – wenn gleich verstanden wie bei der letzten Hacker-Wettbewerbsausschreibung- keinen Beitrag liefern und dient offenbar mehr zur Beruhigung der Öffentlichkeit. Für aussenstehende Experten scheint er eher kontraproduktiv und zeigt etwas die Hilflosigkeit für die

[2] 64680.pdf (admin.ch)

Behandlung des Themas an, falls die öffentliche Fehlersuche (weiterhin) nicht auf die wirklich wichtigen Schwachstellen (Social Engineering, operative Sicherheit an allen Orten der Auswertung) ausgeweitet wird.

Mit der guten Definition dieser Grundsätze ist ausserdem noch nichts gewonnen, sie müssten auch konsequent umgesetzt werden. Das würde sehr, sehr teuer werden. Man darf deshalb Zweifel haben, dass im Laufe dieser Entwicklung die Sicherheitsanforderungen jederzeit in voller Gänze Priorität geniessen werden.

2. Bedingungen für einen sicheren E-Voting Versuchs-Betrieb

Die Bedingungen für einen sicheren Betrieb sind im Dokument „Dialog der Wissenschaft“ skizziert worden. Grundsätzlich ist dort die Wissenschaftlichkeit der Ansätze erkennbar. In Ergänzung dazu müsste gesagt werden:

- Absolute Offenlegung und Überprüfung **aller Source Codes** der beteiligten Komponenten durch die Provider, **insbesondere auch aller Prüfroutinen ist Pflicht.**
- **Vertrauenswürdige unabhängige und kompetente Experten sind unabdingbar. Diese sollten den Bedingungen in Kap 3 entsprechen.**
- **Detaillierte Prüfung der Prüfmechanismen durch die Experten mit permanenter Möglichkeit zur Einführung weiterer Prüfungen ist zwingend**
- **Überwachung der Durchführung der Auswertungsprüfung geschieht in jedem Einsatzfall beim Urnengang durch die Experten im Detail**
- **Entschädigungen für die generellen Anstrengungen und insbesondere für diese Sondereinsätze bei allen Urnengängen sind unabdingbar und müssen angemessen sein. Sie werden in die Gesamtkosten für den E-Voting Betrieb eingehen.**
- **Es braucht dringend Alarm-Kriterien, die eine sofortige Intervention zur Folge haben, sowie Kriterien zum Abbruch eines Urnenganges.**
- **Die Alarmkriterien müssen auch durch die Experten definiert und festgestellt werden können.**
- **Ein Massnahmenkatalog muss mit den Experten abgesprochen und transparent bereitgestellt werden**

Die öffentliche Überprüfung kann logischerweise erst mit Zeitverzug erfolgen, wenn die Experten alle Analysen gemacht und Dokumente in verständlicher Form bereitgestellt haben. Das führt zu einem Zeitfenster, in dem die möglichen Unregelmässigkeiten festgestellt und bewertet werden können. Wir empfehlen für den Anfang ein zweistufiges Verfahren:

- Feststellung des mutmasslich korrekten Ablaufes innerhalb von 3 Stunden.
- Feststellung des sicher korrekten Ablaufes innerhalb von 4 Tagen

Es kann zu Vertrauensverlusten führen, wenn sich z.B. im Hinterher die festgestellten Probleme, die evtl. eine Manipulation anzeigen, als gravierender erweisen, als man zunächst geglaubt hat. Das darf nicht dazu führen, dass man Abstriche an der Transparenz vornimmt, sondern eher die Wiederholung des Urnengangs oder evtl. sogar die Aussetzung oder den generellen Verzicht des aktuellen E-Voting –Systems in Kauf nimmt.

3. Auswahl und Funktion von unabhängigen und kompetenten Experten

Zur Vertrauensbildung ist die Auswahl von unabhängigen und kompetenten Experten von kapitaler Wichtigkeit. Normalerweise sind die kompetenten IT-Experten auf der Lieferanten- oder Providerseite, denn sie befassen sich hauptamtlich mit den Gegebenheiten ihres Systems. Sie sind aber interessensgebunden, man kann deshalb von ihnen nicht erwarten, dass sie allen Unregelmässigkeiten mit voller Seriosität nachgehen und allenfalls ihr eigenes System kompromittieren. Andererseits gibt es Experten, die mit voller Seriosität den Unregelmässigkeiten nachgehen würden, sie haben aber möglicherweise einen tieferen Wissensstand in Bezug auf das aktuell eingesetzte Produkt. Das führt dazu, dass man ihnen Zeit geben muss, den Fragen nachzugehen und die Insider -Informationen kritisch zu hinterfragen und zu überprüfen. Das kann zu hitzigen Diskussionen, Zeitverzug und Zweifeln im Raum führen. Das gehört aber zu einer Fehlerkultur, die gerade beim E-Voting zwingend notwendig ist.

Zur Auswahl und Funktion der Experten soll deshalb Folgendes gelten:

- Sie dürfen nicht eingebunden sein in Organisationen, die auf die Interessen des Providers, des Herstellers oder Lieferanten ausgerichtet sind.
- Mindestens die Hälfte der Experten muss eine kritische Voreinstellung gegenüber E-Voting haben und darf nicht der Verwaltung angehören.
- Die Organisationen Digitale Gesellschaft, Chaos Computer Club und Piratenpartei gelten in diesem Sinne als vertrauenswürdig für die Expertise.
- Die Namen der Experten werden veröffentlicht.
- Die Experten haben ein Recht, ihre Meinung an die Öffentlichkeit zu bringen. Mehrheits- und Minderheitsmeinungen werden veröffentlicht und als solche gekennzeichnet.

4. Risiken und Gegenmassnahmen

Einige Risiken und Gegenmassnahmen wurden beim Dialog mit der Wissenschaft grundsätzlich erkannt bzw. identifiziert. Andere müssten unbedingt ebenfalls in geeignetem Masse berücksichtigt werden

4.1. Zu wenig beachtete Risiken im Cyberkrieg

4.1.1.Codeabfluss: Die in den Druckzentren erstellten Codes, die die Sicherheit der Übertragung gewährleisten sollen, können von diesen Zentren auf diverse Arten abfliessen, genauso wie immer wieder weltweit Passwörter von hochkompetenten IT-Zentren in grossem Masse gestohlen werden. Diese Tatsache zeigt, dass es offenbar sehr schwierig ist, generell IT-Zentren vor Datenabfluss zu schützen. Damit können weltweit gültige Abstimm-Ballots hergestellt werden, die dann kurz vor E-Voting Eingabeschluss versucht werden, im System anzubringen. Nur diejenigen Voting Codes, die bereits vom authentischen Besitzer verwendet wurden, würden zu einem Misserfolg führen. Bei einer Nichtwählerquote von z.B. 55% ergibt dies ein erhebliches Manipulations-Potenzial.

Die Verhinderung von solchem Datenabfluss müsste durch operative Vorgaben verhindert werden und diese Massnahmen müssten für die Experten nachvollziehbar und jederzeit überprüfbar sein,

sowie von diesen Experten glaubhaft an die Öffentlichkeit kommuniziert werden können. Mit dem Test 4.2.1 könnten evtl. Anhaltspunkte für einen Codeabfluss festgestellt werden.

Das Recht des Nichtwählers, seine evtl. fälschlich abgegebene Stimme zu überprüfen, stellt zwar eine rechtswirksame Massnahme dar, ist aber als Erkennung von relevanten Manipulationen untauglich, denn sie wird wohl nur in den seltensten Fällen wahrgenommen. Warum sollte ein politisch nicht interessierter Mensch an der Frage interessiert sein, ob seine Stimme widerrechtlich abgegeben wurde?

4.1.2.Manipulation durch Insider: Leute mit Privilegien an den Systemen können Eingriffe vornehmen, die sie nicht unbedingt verstehen müssen und die sie nicht einmal zu beabsichtigen brauchen. Manipulatoren können unter irgendwelchen Vorwänden Insider dazu animieren, allenfalls zu erpressen, Eingriffe vorzunehmen, die ganz andere Effekte haben als kommuniziert.

Zu diesen Manipulatoren können unterwanderte Lieferfirmen, Geheimdienste, mafiöse Organisationen sowie Einzelpersonen (innerhalb und ausserhalb der Fa. des Providers) gehören, wie diverse Ereignisse in der Vergangenheit gezeigt haben. Die Feststellung und Analyse von solchen Manipulationen bedarf einer rigorosen und aufwändigen Überwachung des Zuganges und Zutrittes zu allen betroffenen Systemen (operative Sicherheit). Diese müsste ausserdem von einem vom Provider unabhängigen Dienstleister durchgeführt werden (Z.B. Bund/Armee).

4.1.3.Versteckte Schwachstellen im Zentralsystem: Um Manipulationen vorbei an den Sicherheitseinrichtungen auszuführen, ist im ersten Schritt eine Schwachstelle notwendig. Neben den jährlich 10000 neu entdeckten und registrierten Schwachstellen ist auch mit einer Anzahl entdeckter aber nicht registrierter Schwachstellen zu rechnen, die solche manipulative Eingriffe erleichtern oder überhaupt erst möglich machen. Diese ändern sich mit jedem Update, der alte Schwachstellen eliminiert und/oder auch neue Schwachstellen einführt. Da das Potenzial an Angreifer sich massiv vergrössert, wenn man die bekannten Schwachstellen länger offenlässt, gibt es keine Alternative zu den permanenten Updates der Lieferfirmen, die doch immer wieder jeweils einige der wichtigsten bekannten Schwachstellen eliminieren. Jedoch ist mit jedem Update auch eine neue Schwachstelle wieder möglich.

Wenn die Gegnerschaft eine staatliche Stelle ist, kann das Risiko mit einem neuen Update durchaus grösser sein als das kurzfristige Belassen eines geprüften Zustandes. Es gibt aber keine abschliessend sichere Methodik. Diese Gefahren wurden am Rande gestreift aber umfassende und wirksame Gegenmassnahmen sind bis dato nicht zu erkennen.

4.1.4.Unsichere Endgeräte: Die mögliche Manipulation an einem Endgerät (Handy, Computer) soll bekanntlich mit der kryptologischen Lösung des E-Voting entdeckt werden können („individuelle Verifizierbarkeit“). Das ist zwar formell richtig, wird aber in der Praxis nicht funktionieren. Ein manipuliertes Endgerät kann den Confirmation Code bei „falscher Wahl“ zurückhalten und den Abstimmenden in der Meinung lassen, er habe abgestimmt. Zwar sieht der dann den Finalization Code nicht, aber 90% der Abstimmenden würden sich bestimmt auch mit einem „Vote OK“ o.ä. am Bildschirm zufriedengeben. Damit kann der Urnengang massiv manipuliert werden und nur einige wenige werden sich wundern über den fehlenden Finalization Code. Da für so einen Fall nur die Entscheidung des Abstimmenden, doch auch noch an die Urne zu gehen, übrigbleibt, darf damit gerechnet werden, dass solche Fälle grösstenteils unbemerkt bleiben. Was mit allfällig dennoch

durchkommenden Meldungen zu machen wäre, bleibt völlig im Dunkeln, denn die Dunkelziffer ist nicht einmal annähernd abschätzbar. Überprüfungen solcher Meldungen sind ausserdem derart aufwendig, dass es im besten Fall nach einigen Tagen gelänge, einige wenige Beispiele zu analysieren. Würde man bei wenigen Meldungen bereits rigoros eingreifen, so könnte man auch auf eine vorgetäuschte Manipulation hereinfallen. Vertrauenswürdig ist deshalb keines der möglichen Abwehr-Dispositive.

Wie bei der Pandemie darf es nicht reichen, dass sich der Einzelne sich selbst (gegen Stimmen-Manipulation) schützt, sondern er muss auch die ganze Gesellschaft schützen helfen. Jeder, der dies nicht tut, ist eine Schwachstelle und trägt zu einer möglichen Manipulation bei. Wenn das Ganze nicht kontrollierbar ist, ist ein sicheres und vertrauenswürdiges Ergebnis deshalb nicht zu erreichen. Bis jetzt wurde diese Gefahr auch von der einbezogenen Wissenschaft nicht erwähnt.

4.1.5. Handel mit Voting Codes: Da nach wie vor mit ca. 40-50% abstinenten Urnengängern gerechnet werden muss, ergibt sich dank den einfach zu handelnden Codes ein Potenzial für eine Börse von Nicht-Wählerstimmen. Angebot und Nachfrage auf dem Darknet sind vor der Justiz weitgehend geschützt. Ein passendes Geschäftsmodell dazu wäre durchaus denkbar.

Bis jetzt gibt es keine Vorkehrungen gegen diese Gefahren. Der Benutzer handelt in diesem Fall vielleicht illegal, aber Kontrolle ist kaum möglich.

4.1.6 Kompromittierung des Abstimmgeheimnisses: Durch das Hacken z.B. eines Handys können Abstimmungsdaten bequem abfliessen zu einer Datenbank, die Interesse am Wählverhalten der Leute hat. Eine App, die z.B. das komplizierte manuelle Prüfverfahren vereinfacht, hätte nicht nur die Möglichkeit zur Manipulation der Stimme sondern auch zur Weitergabe an Dritte.

Bis jetzt gibt es offenbar keine Vorkehrungen gegen diese Gefahren. Man scheint das Risiko einfach dem Benutzer zu überlassen, da ja keiner gezwungen wird, E-Voting zu machen. Vergessen wird dabei aber, dass in weiten Teilen der Bevölkerung der Anspruch besteht, dass der Staat etwas gegen diese Gefahren unternimmt.

4.2. Mindest-Prüfobjekte im Versuchsbetrieb

Der Schritt von der – nicht ausreichend geschützten – „individuellen Verifizierbarkeit“ zur sog. „vollständigen Verifizierbarkeit“ besteht in einer Serie von Prüfungen, die zum Zeitpunkt der Auswertung als Mindestanforderung folgendes sicherstellen sollen:

#	Prüfung	Beschreibung	Gegenmassn. zu
1	Dass alle Ballots mit einem aktuellen, gültigen, einzigartigen Voting Code versehen sind	Nur Ballots mit gültigen Voting Codes werden gezählt Ungültige Doppel-Versuche mit gleichem Voting Code werden gelistet mit Herkunfts-IP Nicht vorhandene Voting Codes führen zu einem Alarm Die gesicherten Vergleichs -Daten dazu müssen beigezogen werden.	4.1.2,4.1.3 4.1.1. partiell
2	Dass alle Voting Codes einen gültigen Stimmbürger repräsentieren	Die gesicherten Vergleichs -Daten (Voting Codes) dazu müssen beigezogen werden. Der Name des Stimmbürgers ist nicht notwendig.	4.1.2,4.1.3

3	Dass mit den richtigen Mitteln geprüft wird (Gemeinsame Prüfung einer von den Experten erstellten Prüfroutine(n))	Der Provider und die Experten begutachten die Prüfroutine, die die Auswertungsroutinen prüfen muss	4.1.2,4.1.3
4	Dass die Ergebnisse den vorhandenen ballots entsprechen (Authentizität der Auswertungsroutinen 1-2)	Die Auswertungsroutinen werden von den Experten inhaltlich geprüft. Das kann mit einer von den Experten ausgearbeiteten Prüfroutine erfolgen. Die Auswertungsroutinen dürfen seit der letzten (Source Code-Prüfung inkl. Maschinencodeübersetzung) nicht verändert worden sein Die Auswertungsroutine muss ordnungsgemäss angewendet worden sein für die Ermittlung der Prüfergebnisse	4.1.2,4.1.3
5	Dass die Resultate nicht von der Plattform abhängen (Authentizität der Plattformen)	Die Auswertungen werden auf 4 verschiedenen Plattformen ausgeführt, die keine gemeinsamen Anteil haben	4.1.2,4.1.3

5. Weiterhin ungelöste Problemkreise

Aus obigen Ausführungen geht klar hervor, dass man auch heute noch keine wirksamen Gegenmassnahmen für alle der Cyberbedrohungen definieren kann. Man schätzt ja offenbar deshalb den Rahmen für die Dauer des neuen Versuchsbetriebs auf weitere 15 Jahre.

Von den genannten Einzel-Risiken (Kap 4.1), die keine genügenden Gegenmassnahmen sehen, sind folgende absolut prioritär und müssten umgehend angegangen werden:

- **Codeabfluss für Autorisierungen und Authentifikation (4.1.1)**
- **Unsichere Benutzerendgeräte und genannte Folgen (4.1.4)**
- **Kompromittierung des Abstimmgeheimnisses durch „normale“ Cyberkriminalität (also auch ohne Annahme eines staatlichen Gegners) (4.1.6)**

Weiter sehen wir folgende kritische Punkte:

- **Zeitfenster** für alle Prüfungen zu kurz. Die Komplexität der Erkennung von möglichen Cyberangriffen und Manipulationen ist derart gross, dass in keinem Fall erwartet werden kann, dass man innerhalb von wenigen Stunden eine abschliessende Beurteilung hat, wenn zweifelhafte Teilergebnisse an den Prüfstellen vorliegen. Es wird politisch ausserordentlich heikel sein, wenn man nach Tagen oder erst Wochen zu Ergebnissen kommt, dass die Wahl möglicherweise kompromittiert wurde. Auch hier könnte die Abschätzung des Ausmasses eine grosse Herausforderung darstellen.
- **Die eigentliche Funktion der Wahlkommission** wird von IT-Experten wahrgenommen, die keine politische Legitimation haben. Diese Tatsache wäre womöglich politisch nicht akzeptierbar, wenn sie denn in der Öffentlichkeit klar wahrgenommen würde.
- **Der Anbieter** will mit seinem Produkt ja kommerziell erfolgreich sein. Es ist kaum vorstellbar, dass dies bereits in einem Versuchsbetrieb gelingt, wobei die Kantone sich ja noch gar keine

Vorstellungen machen, welchen Preis sie dafür bezahlen müssten. Sicher ist einzig, dass die Unsicherheit über die weiteren Entwicklungen gross ist und dass wohl über längere Zeit keine Abnahme-Garantien abgegeben werden können. Eine transparente Kommunikation dieser Tatsache würde wohl die Begeisterung in manchen Kantonen und beim im Moment einzig sichtbaren Anbieter begrenzen.

6. Ziele für den Versuchsbetrieb

Bei den Zielen für den Versuchsbetrieb müssten u.E. die folgenden Mindestanforderungen eingehalten werden:

- **Transparenz für die Öffentlichkeit aller durch die Experten entdeckten Problemkreise**. Nur so lässt sich Vertrauen gewinnen, falls es berechtigt ist.
- **Lösungsansätze für die genannten weiteren ungelösten Problemkreise werden definiert**. Nur so lässt sich die desolate Sicherheitssituation entschärfen.
- **Definition für Kriterien eines Wahl- bzw. Abstimmungs-Abbruchs**. Nur so kann glaubhaft gemacht werden, dass der Abstimmungsprozess auch im elektronischen Fall unter Kontrolle ist.
- **Abschätzung der Kosten und des Zeitbedarfes für all die Sicherungsmassnahmen**. Nur so lässt sich eine Vereinbarung zwischen Anbieter und Abnehmer auf absehbare Frist etablieren.
- **Veröffentlichung des Ressourcenbedarfes**. Nur so lässt sich die Öffentlichkeit vom Sinn dieses Projektes überzeugen.

7. Schlussbemerkungen

Bei der Pressekonferenz am 21.12.2020 wurde erstmals deutlich, dass das E-Voting keine höhere Stimmbeteiligung, also verbesserte politische Beteiligung des Volkes (mehr) anstrebt. Zu oft wurde der Nachweis des Fehlens eines diesbezüglichen Zusammenhanges erbracht. Es verbleiben demnach nur noch Vorteile für Sehbehinderte und einige Tausend Auslandschweizer, welche tatsächlich ein Problem mit postalischen Zustellungen haben. Für letztere gäbe es weitgehend kompensierende Massnahmen[3].

Als Stimmbürger kann ich zwar die Anspruchshaltung haben, E-Voting müsse möglich sein. Als Fachmann muss ich zugeben, dass wir mit E-Voting als Stimmbürger alle die Gewähr für die richtigen Ergebnisse in die Hände von einigen uns unbekannten Spezialisten legen und auch das Risiko für Manipulationen nicht wirklich abschätzen können. Selbst für die Tatsache, dass wir gegebenenfalls eine solche bemerken würden, gibt es keine Garantie. Und falls dies doch der Fall wäre, wäre das Ausmass unbekannt und daraus die abzuleitenden Konsequenzen einer Willkür ausgesetzt. Was das für das Vertrauen in unsere demokratischen Institutionen bedeutet, kann sich jeder selbst ausmalen. Vom Politiker erwarte ich, dass er all diese Tatsachen zur Kenntnis nimmt bzw. offenlegt und ***dann*** eine Meinung äussert, warum man dennoch E-Voting einführen sollte oder eben nicht.

Ich als Stimmbürger jedenfalls, würde auch mit einer entsprechenden Anspruchshaltung unter diesen Umständen lieber auf E-Voting verzichten.

[3] Verspätete Abstimmungs-Post: Die Lösung liegt im früheren Versand - SWI swissinfo.ch