# E-Voting CH Testbetrieb: Ein nutzloses, ewiges Experiment[1]

**Der Bundesrat hat die Wiederaufnahme des Testbetriebs E-Voting beschlossen. Ein Ende ist nicht abzusehen, denn es verbleiben erhebliche Zweifel, dass dem Betrieb in absehbarer Zeit eine «hinreichende Sicherheit» zugeordnet wird, so dass er regulär werden kann.**

## 1. Was wurde eigentlich getestet seit bald 20 Jahren und warum soll das nun weitergeführt werden?

**Nur die Akzeptanz wird getestet**. Es wird von der Bundeskanzlei aus immer wieder behauptet, es seien bis jetzt „alle 300 Versuche erfolgreich“ verlaufen. D.h. man hat also keine Cyberangriffe bemerkt. Das Einzige, was aber wirklich getestet wurde und wird, ist die Anzahl der Abstimmenden mit E-Voting und damit die **Akzeptanz**. Wenn die aufwärts geht, so muss offenbar das Projekt ein Erfolg sein. Die Leute machen dann mit, wenn sie denken, dass es sicher genug sei, sagt die Studie[2]. Aber tun sie das zu Recht oder ist der Wunsch als Vater des Gedankens hier der, dass man sich einfach daran gewöhnen soll?

**Nur der breite Widerstand der E-Voting Gegner hat Erkenntnisse gebracht.** Die eklatanten Unstimmigkeiten, die sich beim früheren E-Voting gezeigt haben, sind nicht aufgrund irgendeines Tests im Testbetrieb publik geworden, sondern weil sich breiter Widerstand regte gegen die Einführung eines regulären Betriebes. Dazu kam allerdings noch die unglaublich naive Übernahme eines spanischen Systems durch die Post, das sich nach Untersuchungen von echten Experten in allen Teilen als unbrauchbar bzw. unsicher erwies. Diese Experten wurden aber nicht im Rahmen von Expertendialogen durch die Bundeskanzlei angegangen, sondern durch erklärte E-Voting Gegner, die das ganze Vorhaben ablehnen. Von der BK wurden Expertendialoge mit konstruktivem Gehalt erst nach dem Neustart initiiert. Man darf davon ausgehen, dass dort etwelche **Experten des Bundes**, auch wenn sie konstruktiv-kritisch an Verbesserungen mitarbeiten, auch eher **skeptisch** in Bezug auf das Gelingen des ganzen Vorhabens sind. Der Hauptgrund dafür ist die fehlende Vorstellung darüber, wer mit welchem Aufwand welche Aufsichts-Funktionen übernehmen und wer dabei vertrauenswürdig und zugleich kompetent die Einhaltung der Sicherheitsansprüche überwachen soll und kann.

**Aufwandfrage für Sicherheit an die Kantone abgeschoben**. Der Testbetrieb selbst hat keine Erkenntnisse zur Sicherheitslage gebracht und wird das wohl auch in Zukunft nicht tun, wenn nicht die Aufwandfrage abschliessend und mehrheitsfähig geklärt ist. Genau dies wird wohl niemals der Fall sein, denn diese **Kompetenz ist – wie bei der klassischen Wahl - an die Kantone delegiert**[3]. Und da diese grösstenteils glauben, dass die Sicherheit durch die Bewilligung des Bundes automatisch gegeben ist, werden die Kantone wohl wenig bis gar nichts tun in dieser Hinsicht. Denn die dafür notwendigen Ressourcen sind ja auch kaum vorhanden.

**Der Testbetrieb ist deshalb unnütz.**

Einzig eine Einstellung des Vorhabens könnte man als ein konstruktives Ergebnis der ganzen Testbetrieb-Periode bezeichnen.

- **Welche neuen Erkenntnisse will man jetzt noch aus weiteren jahrelangen „Versuchen“ gewinnen, wo die Schwachstellen und Risiken doch grundsätzlicher Natur sind? Es gibt in der IT immer wieder neue Szenarien, die zu Zweifeln an der Integrität der Ergebnisse führen[4].**
- **Welche Firma würde Produkte in der Produktionsumgebung (mit echten Kunden) testen, deren Risiken sie bereits kennt und gegen die sie nichts Wesentliches machen kann?**
- **Braucht es wirklich einen Super-Gau, damit man die Risiken auch in der Politik wirklich zur Kenntnis nimmt, obwohl die Szenarien schon jetzt absehbar sind?**

## 2. Welche Gründe könnte es haben, dass man sagen konnte und auch sagen wird, es hätte bisher keine Manipulationen gegeben?

**Es gibt eine ganze Reihe von Gründen, warum viele glauben, dass «bis jetzt ja alles gut gegangen» sei. Aber : man weiss eigentlich gar nicht, ob das stimmt und zweitens ist Fakt:**

| | 6 Szenarien für mögliche Gründe | Hinweise, die dafür sprechen |
|---|---|---|
| 1 | Erwiesenermassen hatte das alte System schon in der Applikation derartige Schwachstellen, dass man eine Manipulation gar *nicht notwendigerweise bemerken* musste. Das wurde lange Zeit bestritten. Beim neuen System hat man z.Zt noch nichts gefunden. | Diese Tatsache wird von niemandem (mehr) bestritten. |
| 2 | **Mangelnde Erfolgsaussichten wegen kleiner Zahl**<br>Es hat tatsächlich *niemand angegriffen*, weil der Anreiz für die Erfolgsaussichten aufgrund der bisher kleinen Anzahl von E-Votern nicht gross genug war. | Die **Anzahl der E-Voters** war bis 2019 und macht weiter tatsächlich nur einige Prozent des Elektorats aus. |
| 3 | **Keine genügende Sensorik einsetzbar.**<br>Eine wirksame technisch-operative *Sensorik* für Cyberangriffe auf den Netzen, bei den Kunden und in den Auswertungssystemen ist *nicht flächendeckend implementiert* und deshalb konnte man gar nichts feststellen. | Die **Cyber-Kompetenzen** sind in der Schweiz generell rar und bei den Kantonen wohl meist noch gar nicht vorhanden. Sie sind damit nicht in der Lage, ihre per neuer Verordnung polR festgelegte Aufsichtsfunktion wahrzunehmen.<br><br>Es gibt gar keine adäquaten Aufgabenbeschreibungen, die eine solche **Aufsichtsbehörde** wahrnehmen müsste.<br><br>Der Betreiber POST wird sich hüten, irgendwelche Unregelmässigkeiten publik zu machen, falls diese eine Wirkung haben könnten, der man nachgehen müsste aber nicht könnte: Es liegt nicht in deren **Interesse**!<br><br>Auch bei Kantonen und der Bundeskanzlei dürfte das Interesse an schlechter Publizität nicht dominieren. |
| 4 | **Ungenügendes Knowhow für Cyberwaffen.**<br>Es haben Angriffe stattgefunden und niemand hat etwas davon bemerkt, weil diese *geschickt genug vorgetragen* wurden mit Wissen, das hier bisher nie aufgedeckt wurde. | |
| 5 | **Zeitmangel und ungenügendes Interesse**<br>Es haben Angriffe stattgefunden und Techniker haben zwar etwas bemerkt, können es aber nicht sicher zuordnen und so werden von Verantwortlichen des Betreibers die Spuren kleingeredet, um das Projekt und die Vertrauenswürdigkeit nicht zu gefährden.<br><br>Falls Experten verfügbar wären, die etwas entdecken könnten und würden, würden diese nicht genug Zeit haben bzw. bekommen, irgendwelchen Unregelmässigkeiten in genügender Tiefe nachzugehen. Man müsste für jede Unregelmässigkeit mit tage- oder sogar wochenlanger Analysearbeit rechnen. | |
| 6 | **Fehlende Meldungen von Stimmbürgern**<br>Es würden vielleicht Stimmbürger bei einer Hotline wegen Unregelmässigkeiten bei der Nutzung des E-Voting reklamieren, aber sie laufen Gefahr, als digitale Anfänger eingeordnet zu werden. Das hindert viele, eine Reklamation überhaupt in Betracht zu ziehen.<br><br>Es könnte sich effektiv jeweils immer auch um eine vorgetäuschte Unregelmässigkeit handeln, die andere Ziele verfolgt. Abklärungen, ob Reklamationen berechtigt sind, wären viel zu langwierig und kostspielig. Von Amtes wegen wohl als ausserdem unnötig betrachtet, da jeder, der seinem Endgerät nicht vertraut, ohnehin gehalten ist, die Brief- oder Urnenwahl zu nutzen.<br><br>Ausserdem wird sicher darauf hingewiesen werden, dass die Anzahl der festgestellten Unregelmässigkeiten viel zu klein sei, um eine Verfälschung anzunehmen.<br><br>Das alles wiederum ist ein Grund für manchen Bürger, auf Meldungen dieser Art zu verzichten. | Die Hotline hat bei Problemen als Generalantwort: „Die Briefwahl kann im Zweifel benutzt werden."<br><br>Reklamationen werden weder gezählt noch bewertet und eingeordnet. Das wäre viel zu aufwendig, bzw. gar nicht machbar in der zur Verfügung stehenden Zeit.<br><br>So würde eine Zählung auch nicht viel bringen denn eine riesige Dunkelziffer ist nicht abzuschätzen. |

## 3. Wie verordnet man Cyber-Sicherheit per Gesetz? Gar nicht!

Unbestritten ist, dass man zwar Anforderungen an technische Systeme ins Gesetz schreiben kann. Staatsrechtler mögen Systeme einfordern, die vertrauenswürdige Resultate liefern. Sollte es Hinweise auf Manipulationen geben, muss der Staat diesen nachgehen. Strafrechtler mögen Manipulationen am Wahlsystem unter Strafe stellen. Die Frage ist aber, ob diese Rechtsnormen dann einen wirksamen Schutz gegen Verfälschungen an den Wahl- und Abstimmungs-Ausgängen darstellen.
Wo kämen denn solche Hinweise her? Der einzelne Stimmbürger wäre hoffnungslos überfordert. Beim Staat fehlen sowohl die technischen Voraussetzungen als auch das Wissen. Wer hätte aufgrund wovon welche Aktivitäten zu tätigen? Wie aufwendig wären diese und wie lange hätte man Zeit, ein Abstimmungsresultat anzufechten? Wenn ein Schaden nicht sichtbar ist und mögliche Täter unidentifizierbar sind, sind solche Unterfangen in der Praxis aussichtlos.

Hinweise könnten praktisch nur von involvierten Experten kommen, die aber in den meisten Fällen ein Eigeninteresse am problemlosen Betrieb haben und somit Partei sind. Das notwendige Wissen für eine fundierte Aussage zu möglichen Hinweisen ist ausserdem so riesig, dass die Justiz nur in seltensten Fällen per Zufall mit relevanten Erkenntnissen beliefert werden könnte.

Und weil praktisch nie ein sichtbarer Schaden vorliegt, wird eine Manipulation zu beweisen zur Unmöglichkeit, und somit ist auch nie schlüssig, ob das mit der fehlenden Umsetzung einer gesetzlichen Anforderung zu tun hätte. Mit dem Verdecken des Schadens entsteht somit auch zugleich ein Freibrief für entlastende Expertise: Kein Schaden nachweisbar - Kein Schuldiger – Kein Problem! Die juristischen Normen sind nutz- und wertlos.

**Fazit:**
**Sicherheit kann nicht per Gesetz verordnet werden. Es gilt einzig, das Risiko-Management im Griff zu haben. Der Risikoträger ist das Stimmvolk, sind wir also alle zusammen. Haben wir alle das wirklich im Griff? Kennen alle Stimmbürger die wesentlichen Risiken und stimmen sie zu, einen möglichen Schaden zu tragen? Da bin ich sicher: NEIN!**

## 4. Das Misstrauen in die demokratischen Vorgänge ist vorprogrammiert

Aufgrund der Bekanntheit der oben aufgeführten Fakten, sind alle Behauptungen von Wahlfälschungen weder beweis- noch widerlegbar. Behörden können keine Beweise aufbringen, dass Manipulationen nicht stattgefunden haben. **Ein vertrauenswürdiges Nachzählen ist nicht mehr möglich**. Das öffnet Tür und Tor für jegliche Verschwörungstheorien. Unregelmässigkeiten können effektiv auftreten oder auch gefälscht sein. Wenn nun zwar Unregelmässigkeiten festgestellt oder gemeldet werden, diese aber weder sicher zum einen noch sicher zum andern Schluss führen, bleibt ein Zweifel bestehen[6]. So ist dieser **Zweifel von grundsätzlicher Natur**. Das Feststellen von Unregelmässigkeiten verliert damit seine Bedeutung und ist einzig noch als Alibi-Funktion verwendbar oder wird gar nicht mehr gemacht. Wenn das allgemein bekannt wird, ist nachvollziehbar, dass die ganze Übung mit der «Verifizierbarkeit»-Argumentation auch als Täuschung der Öffentlichkeit aufgefasst werden kann. Und damit wird das Vertrauen breitflächig zerstört.

## 5. Fazit: E-Voting wichtiger als Vertrauen in die Demokratie aufgrund von nachvollziehbaren Fakten?

Wollen wir der Digitalisierung tatsächlich das Vertrauen in unsere Demokratie opfern? Ich glaube, es gibt keine Partei, die das ernsthaft wollen kann. Aber offenbar kennen nicht alle Politiker alle Risiken in genügendem Masse, und damit meine ich nicht nur die technischen Sicherheitsrisiken sondern insbesondere auch die aufgezeigten politischen. Und wenn man jetzt noch den bescheidenen Nutzen in Rechnung zieht: Wie kann man dann noch zu einem andern Schluss kommen als: «Die Nachteile überwiegen, die Vorteile sind zu klein», also genau so wie es unterdessen auch die Journalisten von inside-it tun?

[1]NZZ, 9.4.2023, «E-Voting: das ewige Experiment»
[2]Studie Reber, Uni Lausanne 2018
[3]Im Falle der Brief/Urnenwahl durchaus adäquat. Im Falle E-Voting aber gar nicht!
[4]Inside -IT 28.03.2023, E-Voting-Report: Wie sicher ist sicher genug? (inside-it.ch)
[5]In Genf hatte jemand einst versucht zu beweisen, dass das damalige E-Voting System die Anforderungen des Gesetzes nicht erfüllt, indem ein Hacker bewies, dass er es überlisten konnte. Resultat: Der Hacker wurde verurteilt, das System belassen. (Bericht CCC)
[6]Fabrizio Gilardi, Uni ZH, «Die Tech-Community überschätzt die digitalen Fähigkeiten»