Was ist uns unsere Demokratie wert?

Bevor wir über den Sinn und Unsinn von E-Voting nachdenken, müssen wir uns bewusst werden, auf welches zivilisatorische Gut wir hier einwirken. Es ist in weiten Teilen unserer Bevölkerung unbestritten, dass es vor allem die Einzigartigkeit der direkten Demokratie ist, die unser Land zusammenhält. Wir geben notfalls vielleicht sogar die Vorteile eines riesigen Binnenmarktes auf zu Gunsten der Beibehaltung der Souveränität des Volkes und das im Wissen, dass wir einzig auf unserem Staatsgebiet selbst souverän bestimmen können und Abhängigkeiten vom Ausland durchaus bestehen.

Wir glauben an die Korrektheit der Stimmenauszählung, so wie sie heute unter Mitwirkung von sehr vielen Köpfen stattfindet. Selbst Abstimmungen mit 0.1% Mehrheiten werden von den Verlierern als Selbstverständlichkeit akzeptiert. Das zeugt von einem sehr grossen Respekt und Vertrauen in das System und in die Repräsentanten des Staates. Denn ein kleiner Betrug schon hätte das Ergebnis der Volksbefragung oft kippen können. Ein Sack von Stimmzetteln, von denen man nicht weiss, wo sie herkommen, wird in fernen Ländern manchmal mitgezählt, bei uns niemals! Die Rechtmässigkeit und die absolute Korrektheit aller Staatsorgane werden vorausgesetzt und nicht in Zweifel gezogen. Fälle von einigen Dutzend Stimmzettel mit gleicher Handschrift gereichen bei uns schon dann zum Skandal, wenn das keinerlei Einfluss auf das Ergebnis gehabt hat und wenn die dazugehörigen Vorgänge auch gar nicht kriminell gewesen waren.

Wie kommt man auf die Idee, E-Voting einzuführen?

In dieses hohe zivilisatorische Gut, das wir als Selbstverständlichkeit betrachten, dringt jetzt die Digitalisierung und gaukelt uns vor, wir können das alles auch haben, aber viel schneller, bequemer, günstiger und gleich sicher. Die Digitalisierung gilt als Synonym für Kosteneffizienz. E-Government bringt die Bürger näher zum Staat und ist kaum mit nennenswerten Risiken verbunden. Kosten- und Zeitersparnisse kommen nicht nur den Ämtern zugute, sondern auch der/die Bürger/-in profitiert in hohem Masse davon.

Aufgrund dieser Entwicklung ist es vordergründig nicht verwunderlich, dass im Jahr 2000 die Idee aufkam, man könnte auch Wahlen und Abstimmungen digitalisieren. Es winken sofortige Resultaterkennung, Einsparungen bei den Auszählungsprozessen, Vergrösserung der Abstimmungsbeteiligung durch die „Generation Handy“, durch handicapierte Personen und auch auf Seiten der Auslandschweizer, welche oft Mühe haben mit Lieferfristen per Post.

Leider muss man feststellen, dass die unbestrittenen Vorteile der Digitalisierung auch zu einem Machbarkeitswahn ausarten können, wenn vergessen wird, welche ungeheuren, permanent zunehmenden Kosten die IT – und davon insbesondere die IT-Sicherheit - heute verschlingt und mit welchen oft kaum kalkulierbaren Risiken sie trotzdem verbunden ist.

Prestige Projekte bei der IT führen oft zu übertriebenem Ehrgeiz und zu einer Denkmalsetzung für die Verantwortlichen. Das Verhältnis zwischen Nutzen einerseits und Kosten/Risiken andererseits ist schwierig zu beurteilen, wenn Projekte nicht in überschaubaren Zeiträumen endgültig abgehandelt werden können. Die Politik ist oft verantwortlich für die Verzögerungen, sie dient aber andererseits auch als bequeme Ausrede für nicht zu Ende gedachte Konzepte. Die Lösung heisst dann

„Testphase“. Wenn dann etwas genügend lang getestet ist, ohne dass ein wirklicher Skandal offenkundig wurde, so muss es gut genug sein?

Was ist das Spezielle an E-Voting im Vergleich mit E-Banking?

Wenn es um IT Sicherheit geht, so wird meist E-Banking herangezogen: Jeder macht es, manchmal gibt’s zwar Probleme aber insgesamt gesehen funktioniert alles recht gut. Es gibt Ähnlichkeit im Vergleich der Architekturen punkto IT Sicherheit: Man hat ein relativ teures, gut überwachtes Zentralsystem und billige, unsichere Usersysteme. Warum kann man das zwar vergleichen aber niemals gleichsetzen?

Es gibt entscheidende Unterschiede bei der Prävention, also Sicherheitsmassnahmen, Unterschiede bei der Kontrolle der Transaktionen und beim Feststellen des Betruges sowie Unterschiede beim Opfer und der Hoheit über seine Reaktionsmöglichkeiten:

- *Die Prävention: Sicherheitsmassnahmen*

Crime cases	E- Banking	E-Voting
Initialbedingungen	Die Bank kennt ein „normales“ Verhalten und kann allenfalls Abweichungen erkennen, hinterfragen und/oder verhindern.	Es gibt kein normales oder erwartetes Verhalten, da meine Stimme mir gar nicht zugeordnet werden kann (Anonymitätsanspruch).
Missbrauch von Dritten bei Diebstahl der Account Credentials[1]	Authentizität der Benutzer wird meist gesichert durch Zusatzcode via Zweitkomponente (Handy) über Handy Netz.	Keine Sicherung durch Zweitkomponente. Printout mit Voting Codes werden über Postweg zugestellt. (Allerdings gleiches Risiko wie bei Briefpost- Voting.)
Bei Verlust der Kontrolle über Computer durch Cyberattacke	Keine präventive Sicherung. Die gleiche Schadensart passiert nach der Feststellung aber nur einmal. Die Bank übernimmt Massnahmen zur Verhinderung des gleichen Angriffsmusters.	Keine präventive Sicherung. Die Erkennung ist nicht garantiert. Wenn erkannt, einzige sichere Massnahme zur Korrektur für das nächste Mal ist die Neuinstallation des PCs.

- *Die Kontrolle und das Feststellen des Betruges*

E- Banking	E-Voting
Ich stelle meinen Schaden bei jeder Transaktion immer und präzis fest und kann zusammen mit der Bank Massnahmen gegen den erlittenen Schaden ergreifen.	Der Einzelne könnte zwar einen Betrug bei sich feststellen und evtl. noch brieflich abstimmen. Er tut es aber nicht zwingend. Das Ausmass des gesamten Schadens kann nicht nachgemessen werden (Wie viele Infizierte, die nicht oder falsch abgestimmt haben?). Deshalb keine Massnahmen zur Korrektur möglich.

- *Das Opfer und die Hoheit über die Reaktion*

E- Banking	E-Voting
Mein manipuliertes Konto schadet (höchstens) mir, allenfalls der Bank. Ich habe die Kontrolle darüber. Die Bank hilft beim Kalkulieren und Optimieren der Risiken und trägt allenfalls den Schaden mit.	Meine verfälschte Stimme schadet dem gesamten Stimmvolk. Dieses kann – als Ganzes – nichts tun. Die Bundeskanzlei hat die zentrale nationale Kontrolle. Sie trägt aber den Schaden nicht.

Wie gut ist das E-Voting System CH und was sind die Risiken?

Hier sind 3 Fragen zu beantworten: Wie günstig, benutzerfreundlich und wie sicher ist das E-Voting CH?

Die *Kostengünstigkeit* kann zurzeit weder bestritten noch belegt werden. Es kostet den Anwender offenbar (vorläufig) nichts. Allerdings fehlen auch noch die Kostentransparenz und das Finanzierungskonzept. Es dürften seit 2000 schon sehr viele Millionen geflossen sein und noch viele weitere fliessen. Aber solange die nicht in Gänze aufgezeigt werden, kann man auch keine Kosten/Nutzenrechnung anstellen.

[1] User ID/ Passwort bzw. Voting Card data. Sie könnten gestohlen (kopiert) werden.

Die *Benutzerfreundlichkeit* lässt sich an der Anleitung ableiten, die von den Kantonsverwaltungen herausgegeben wird. Es sind diverse, ellenlange Codes einzutippen und auf der Empfangsseite zu überprüfen, bevor man jeweils den nächsten Schritt machen kann. Verglichen mit der Briefwahl kann man bei bestem Willen nicht von einer Vereinfachung der Abstimmungsprozedur reden, denn das Einzige, was Sie damit nicht mehr tun müssen, ist, den Brief zuzukleben und zum nächsten Briefkasten zu bringen.

Die *Sicherheit* der Lösung trägt viele Aspekte: Die IT-Architektur ist mit E-Banking vergleichbar, mit den oben erwähnten Unterschieden bei Prävention, Kontrolle und Verantwortung. Es werden für die Kantone 2 Applikationslösungen angeboten zur Vermeidung eines absoluten Hersteller-Klumpenrisikos. Im Vergleich zu der Verteilung der Verantwortung auf 26 Kantonsverwaltungen stellt das aber immer noch ein relativ grosses Klumpenrisiko dar.

Den Systemanforderungen an die Applikation darf unterstellt werden, dass sie der kryptologischen Sicherheit genügend Rechnung tragen. Ob die beiden Umsetzungen davon dies ebenso tun, dürfte wohl keine demokratisch legitimierte Instanz kaum je prüfen und bestätigen bzw. widerlegen können. Dennoch würde die Fachwelt die grössten Risiken nicht zuerst da suchen, es gibt genügend offensichtlichere Risiken, die prioritäre Aufmerksamkeit einfordern und wohl den grösseren Risikobeitrag ausmachen.

Das Ziel der Anonymität der Stimmabgabe wurde bei der inzwischen verbotenen Lösung des Kt. ZH offenbar verfehlt, bei den verbleibenden 2 Lösungen CHVote und Scytl wurde die Erfüllung dieser Anforderung glaubhaft gemacht. Allerdings gilt die Aussage nur *ohne* Berücksichtigung der hackbaren, völlig ungesicherten IT Architektur des User PCs. Man darf daraus schliessen, dass der Staat zwar daran gehindert wird, mit E-Voting Gesinnungsschnüffelei zu vollziehen, dass aber Cyber-Kriminelle durchaus in der Lage wären, Abstimmungs-Daten zu ermitteln. Was die damit machen würden, darüber kann spekuliert werden. Diese Konstellation finden wir flächendeckend in der IT Landschaft und zeigt, dass der Staat generell nicht bzw. nur in speziellen Fallkategorien in der Lage ist, die Bürger vor dem Cybercrime zu schützen. Die Frage stellt sich, ob man so einen Anspruch überhaupt stellen sollte, und welche Konsequenzen man daraus ziehen sollte, wenn man es nicht kann.

Das applikatorische Ziel der Sicherung gegen Stimmverfälschungen wurde insofern erreicht, als glaubhaft gemacht wird, dass die Kryptologie (d.h. die Erstellung der zu überprüfenden Codes) von Aussenstehenden nicht gefälscht werden kann. Es bedingt aber, dass der/die Stimmbürger(-in) das komplizierte Verfahren der Codeüberprüfungen beim Abstimmungsverfahren genau kennt und insbesondere merkt, wenn sein Computer etwas anderes zu wollen scheint als die Original-Applikation und die Anleitung der Kantonsverwaltung vorgeben. Selbst dann kann der Benutzer aber im besten Fall nichts anderes machen als eine Briefwahl oder einen Urnengang, wobei die Behörden dann in jedem einzelnen Fall manuell nachprüfen müssen, ob die Stimme nicht zweimal abgegeben wurde[2]. Bereits heute ist klar, dass in so einem Fall Auslandschweizer Stimmbürger dafür meist **nicht**

[2] Aufgerubbelter Bestätigungscode auf dem Stimmausweis

genügend Zeit haben werden für die Briefwahl, denn diese ist nur 24h länger offen als die E-Vote Wahl.

Der Mensch bildet somit wieder einmal die grösste Schwachstelle im E-Voting, bei dem man sich doch so grosse technische Mühe zur Herstellung von Sicherheit gegeben hat. Nicht nur der Mensch als Stimmbürger, sondern auch der Mensch als Betreiber oder Hersteller der Auszählungsanwendungen könnte natürlich bei entsprechender krimineller Energie Manipulationen einspeisen, die kaum überprüfbar sind. Eine kleine Gruppe von Insidern könnte eine riesige Wirkung bei der Resultatausgabe auslösen, genauso wie Stalin gesagt hat: „Nicht die Abstimmenden bestimmen das Resultat, sondern die Auszähler". Welche Massnahmen hier zur Verhinderung solcher Möglichkeiten vorgesehen oder nicht vorgesehen sind, unterliegt keiner Kontrolle einer demokratisch legitimierten Instanz. Man müsste eine Art ENSI für Cybergefahren erfinden, die sich damit befassen müsste. Aber selbst dann wissen wir, dass auch damit nicht alle Risiken ausgeschlossen sind.

Folgender Risikokatalog der technischen Risiken kann man zusammenstellen:

	Risiko Kategorie	Beschreibung	Detektion	Mögliche reaktive Gegenmassnahme	Risikobeurteilung
1	*Cybercrime Outsider benutzerseitig*	Einspeisen von Schadcodes in die Applikation: - verleiten den User, Codes einzuspeisen - verleiten den User, Codes nicht zu überprüfen - behindern die Abstimmung alles in Funktion der Abstimmungsabsicht	Möglich aber mit grosser Dunkelziffer	Wenn detektiert, Briefwahl im Einzelfall Nachzählung ist nicht möglich	Wahrscheinlich, trifft Gesellschaft
2	*Cybercrime Outsider Zentrale*	Einspeisen von Schadcodes in die zentralen Vorgänge zur Manipulation der Auszählung	Möglich	Wenn detektiert, Wahl-Wiederholung Nachzählung ist nicht möglich	Möglich, nicht kalkulierbar, trifft Gesellschaft
3	*Cybercrime Insider Zentrale*	Manipulieren der Auszählung	Kaum	Keine	Möglich, nicht kalkulierbar, trifft Gesellschaft
4	*Diebstahl der Voting Codes*	Abstimmungsrecht geht an nicht autorisierte Personen	Ja, aber nicht garantiert	Nur auf Antrag der Betroffenen kann korrigiert werden	Möglich, nicht kalkulierbar, trifft Gesellschaft
5	*Abfluss des Stimmgeheimnisses*	Die Stimme von z.B. prominenten Bürger(-inne)n wird zwecks Erpressung oder Herabsetzung veröffentlicht	Ja	Justiz	Möglich, nicht kalkulierbar, trifft Einzelnen

Das Risiko wird bestimmt durch den Anreiz eines Gegners, entsprechenden Schaden zufügen zu *wollen* (bzw. Nutzen daraus zu ziehen), sowie aufgrund seiner Fähigkeiten, es tun zu *können*. Die Schweiz in ihren politischen Entscheidungen zu beeinflussen, dürfte einen sehr grossen Anreiz auslösen. Wir müssen deshalb damit rechnen, es mit den besten Gegnern zu tun zu bekommen: Geheimdienste von ausländischen Mächten, kriminelle Organisationen mit entsprechenden Netzwerken und finanzkräftigen Kunden irgendwelcher Art. Alles was möglich ist, wird via Darknet und Bitcoin in der Anonymität und im quasi rechtsfreien Raum gemacht werden. Die Fähigkeiten wiederum sind auch abhängig vom Schwierigkeitsgrad des Manipulationsvorganges.

Für Insider- und Outsider-Risiken sind komplett unterschiedliche Ansätze zu kalkulieren. Ohne genaueste Kenntnisse der technisch-betrieblichen Sicherheits-Bedingungen lässt sich bei *Insidern*

nämlich nur eines sicher sagen: Das Risiko kann nicht wirklich kalkuliert werden, vor allem nicht, wenn man die dynamischen Umgebungsparameter eines Informatik Centers mit ins Kalkül zieht, wie Software-Migrationen und -Updates, Hardwarewechsel, Zutritts- und Notfallregelungen, Personalüberprüfungen, personelle Wechsel bei Verantwortlichen, Betreibern, Lieferanten, Reinigungspersonal etc. Bei den besten *Outsidern* weiss man, dass ihre Fähigkeiten sich nicht nur auf bekannte Schwachstellen und deren Exploits[3] in den Betriebssystemen und Browsern stützen, die gerade noch nicht behoben sind, sondern dass es zudem einige unbekannte Schwachstellen in den Systemen gibt, welche (vorerst) nur Eingeweihte mit Zugang zu Geheiminfos von Herstellern und anderen Geheimdiensten bereits kennen. Solche Angriffe gab es schon in der Bundesverwaltung und sie waren erst nach Jahren zu entdecken.

Beim Risiko 1 kann man darum jetzt schon die Wahrscheinlichkeit attestieren, dass es passieren wird. Der Gegner wird sich aber erst formieren, wenn es attraktiv und erfolgversprechend genug ist, er wird keine mehrjährige Testphase brauchen. Der verwendete Trojaner wird vielleicht nicht die Abstimmungscodes simulieren können, aber er kann z.B. verhindern, dass auf dem User-PC die Verifikation oder die Bestätigung der Verifikations-Kontrolle durchgeführt werden kann, und das abhängig davon, was abgestimmt wurde. Einige Stimmenden werden das merken, andere nicht. Einige werden die Hotline anfragen. Die Antwort dort wird immer die gleiche sein: „Die Briefwahl ist für Sie noch offen“. Aber selbst bei diesen Leuten wird es einige geben, die die Zeit, die Lust oder die Möglichkeit nicht mehr haben, die Stimme mit dem Brief oder an der Wahlurne abzugeben, und das sind z.B. insbesondere die Auslandschweizer. So entsteht ein *nicht vernachlässigbares Potential an entweder manipulierten oder verhinderten Stimmen.*

Wie funktioniert die Cyberkriminalität?

Wenn wir von den besten aller möglichen Gegner reden, so sind das vor allem Geheimdienste der Gross- und Supermächte. Aber auch die organisierte Kriminalität ist weitgehend in der Lage, solche Operationen durchzuführen. Die Frage ist dann für wen, denn diese Kreise interessiert einzig das Geld. Das Brisante an der Cyberkriminalität ist, dass die Leute die so etwas bewirken wollen und diejenigen, die es können, nicht unbedingt identisch sein müssen. Sie müssen sich nicht einmal kennen oder offiziell miteinander in Kontakt treten. Im sog. *Darknet* treffen sich Kunden und Lieferanten anonym. Mit Bitcopins wird bezahlt, so dass auch die Geldflüsse nicht nachvollzoigen werden können. Das Risiko, entdeckt zu werden, ist minimal, der Aufwand, das zu entdecken dafür ist gigantisch. Enge, internationale Kooperationen wären dazu dringend nötig, sind aber noch viel schwieriger als normale polizeiliche Aufgaben, denn kein Land möchte sich enttarnen in Bezug auf seine Cyber-Fähigkeiten.

Der Erfolg des Cybercrime hängt davon ab, wie gut man in ein System gelangt und es massgeblich manipulieren kann. Dafür braucht es lediglich 3 Dinge:

a. 1 Schwachstelle in den Betriebssystemen und/oder Browsern. Dabei unterscheidet man: bekannte Schwachstellen, die in einer neuen Version einige Zeit später korrigiert sind, aber noch vielerorts unkorrigiert verwendet werden, bekannte Schwachstellen, die noch nicht korrigiert sind, und unbekannte Schwachstellen, die vorerst nur Insider kennen. Bekannte Schwachstellen gibt es zu Tausenden, bei den Unbekannten ist man auf Vermutungen angewiesen. Sie unterliegen dem Handel der Geheimdienste.

[3] Ausnutzungs-Prozedur, die dank der Schwachstelle Zugang verschafft

b. 1 entsprechenden Exploit, d.h. eine Prozedur, wie durch diese Schwachstelle ein Eindringen ins System möglich wird. Tausende smarte Informatiker/-innen in aller Welt finden so ihr bestmögliches Auskommen.
c. 1 Bot-Netz Infrastruktur, die es verunmöglicht, den Urhebern dieser Exploits nachzugehen. Botnetze werden mit unseren Computern zu Hause hergestellt, wenn dort selbst passende Schwachstellen festgestellt werden.

Damit kann man, wenn nötig, Hunderttausende von PC Stationen infizieren, wie im letzten Jahr in der Öffentlichkeit bekannt geworden ist. Die Herausforderungen, die sich der Hackerwelt stellen, sind:

a. Die unglaubliche Vielfalt der Versionen von SW-Komponenten, die alle ihre eigenen Schwachstellen haben, die immer wieder korrigiert und mit neuen versehen werden, verlangen eine stetige, flexible Adaption der Exploits auf eine möglichst grosse Anzahl von Komponenten und Versionen.
b. Die Antivirenprogramme, die immer wieder die Exploits erkennen und ausfiltern, verlangen, dass die Exploits immer wieder verändert werden, um eine Zeitlang erfolgreich zu sein.
c. Die wertvollen Exploits, die auf unbekannte Schwachstellen zielen, dürfen nicht leichtfertig und grossflächig angewendet werden, weil es sonst zu gute Chancen gibt, diese nachträglich zu analysieren und damit würde auch die Schwachstelle bekannt und ist anschliessend „verloren“ für ganz wichtige Einsätze, die nicht erkannt werden dürfen.

Daraus wird ersichtlich, dass es zwar durchaus nicht einfach ist, am Cybercrime erfolgreich teilzunehmen, aber mit genügend grossem Aufwand eine machbare Option darstellt für sämtliche kriminellen oder staatlichen Organisationen der Welt.

Wo sind die Überlegungsfehler im Projekt bei der Bundeskanzlei?

Man stellt sich die Frage, ob denn die federführende Bundeskanzlei denn nicht um diese Gefahren der Cyberkriminalität weiss? Die Antwort ist ganz einfach: Doch sie weiss es. Ihr Standpunkt ist: „Unsere Anweisungen zu einer sicheren Stimmabgabe sind klar. Sie müssen sich einfach genau an diese Anweisungen halten, und wenn Sie einen Fehler in Ihrem Computer bemerken, können Sie noch brieflich abstimmen. Dazu müssen Sie einfach früh genug mit E-Voting anfangen.“ Daraus ist zu schliessen, dass der Stimmbürger selbst schuld ist, wenn er das System nicht kennt, und nur den Anweisungen des Computers folgt, während dem die Bundeskanzlei ihre Arbeit richtig gemacht hat.

In der Verwaltung geht man davon aus, dass die Bürger alles korrekt ausführen und wenn nicht, trifft es sie selbst und sie müssen es auch selbst auslöffeln. Der Anspruch des (-r) Stimmbürgers(-in), vom Staat geschützt zu werden, vor all den anderen Bürgern, die ihre Stimme aus Unachtsamkeit einer kriminellen oder ausländischen Organisation überlassen, scheint kein Thema zu sein. Statt der Verifikation wird nur eine Verifizierbarkeit angeboten. Sollte die Demokratie denn im Übrigen nicht eher das Vertrauen der Bürger zum Staat und seinen Institutionen optimieren als nur die Effizienz der Verwaltungsvorgänge?

Gemäss Auskunft aus der Bundeskanzlei ist vorgesehen, dass man dort, wenn während einer Abstimmung „genügend Meldungen über Unregelmässigkeiten“ aufträten, E-Voting suspendieren könne und wolle. Leider hat man aber offenbar keine Ahnung, mit welcher Dunkelziffer man rechnen

müsste. Meldet so einen Vorfall jeder fünfte oder jeder fünftausendste? Kommen diese Meldungen bei der Hotline an, sind die qualitativ brauchbar, werden sie verdichtet und analysiert, und wenn ja vom wem? Und wer würde dann den „Halt"-Knopf drücken, in welchem Augenblick und bei welchem Anlass? Und was geschieht mit bereits gefälscht eingegebenen und bestätigten Stimmen, wer zählt die verhinderten Stimmen und avisiert die Betroffenen, die es nicht gemerkt haben?

Was sind die Folgen von breiter Einführung E-Voting CH?

Wie auch immer die oben gestellten Fragen beantwortet werden, es muss klar erinnert werden, dass neben diesen bekannten „akuten" Risiken es noch die „chronischen", erwähnten nicht-kalkulierbaren IT-Risiken gibt. Diese können u.U. nicht einmal detektiert werden, wenn sie eintreffen (s.Risiko-Katalog).

Wenn das erstere noch nicht dazu gereichen sollte, führt zumindest diese Tatsache garantiert zu einer Verunsicherung in der Bevölkerung. Es könnte aber auch umgekehrt zu einer Vortäuschung von Cybercrimes kommen, da diese ebenso schwierig zu evaluieren sind, wie die echten Cybercrimes selbst. Unterlegene politische Gruppierungen werden somit alles behaupten können und keiner der Verantwortlichen kann etwas sicher bestätigen oder widerlegen. Feststellungen verbleiben in vagen Vermutungen. Für genaue Überprüfungen bräuchte es gigantische Ressourcen. Das Zeitalter der „alternativen Fakten" wird dann auch hierzulande aufblühen.

Das Vertrauen in Politik und Staat wird massiv gestört, die gesellschaftlichen Folgen wären verheerend: Das Urgestein unseres nationalen Zusammenhaltes zerbröselt.

Was läuft zur Zeit in der Politik in Sachen E-Voting?

Seit einigen Jahren versuchen einige Parlamentarier immer wieder, das E-Voting Projekt, das seit 2000 läuft, schneller voranzubringen. Sie werden von der Regierung vertröstet mit der schwierigen gesetzlichen Grundlage, die von der Bundeskanzlei noch zu schaffen sei und bei der offensichtliche Herausforderungen noch gelöst werden müssten. „Sicherheit vor Tempo" ist der Slogan der Bundeskanzlei, wobei ich aber keine Fortschritte in der Sicherheit feststellen kann. Es bleibt ja alles gleich, nur der Prozentsatz der sich beteiligenden Auslandschweizer nimmt zu. Der Testbetrieb, der auf relativ kleinem Feuer bleibt, verhindert zwar, dass sich ernsthafte Gegner bereits formieren aber gaukelt deshalb auch vor, dass alles paletti sei.

Würde man ernsthaft IT Sicherheit auch beim User zu Hause einfordern, kämen wohl massive Kosten auf uns zu. Kosten und Finanzierung sind in der Öffentlichkeit aber bis jetzt nicht transparent gemacht worden. Müssten die E-Voter/-innen die Kosten alleine tragen, gäbe es möglicherweise keine Freiwilligen mehr. Dann müsste man alle dazu zwingen, was aber wahrscheinlich wiederum politisch nicht durchsetzbar wäre: Ein echtes Dilemma!

Es sind jetzt auch Vorstösse im Parlament unterwegs mit kritischer Grundeinstellung. NR Grüter (LU), SVP, fordert ein Moratorium für 4 Jahre, bis alle gesetzlichen Unterlagen verabschiedet sind. Jungparteien haben das Thema entdeckt und sind durchwegs skeptisch durch das ganze Parteienspektrum hinweg. Die Medienberichterstattung wird auch zunehmend kritischer. Datenschützer beginnen sich zu wehren.

E-Voting und die Demokratie

Das Parlament ist jetzt gefragt. Die Gesetzgebung zu E-Voting kommt wohl erst in 2-3 Jahren. Bis dann läuft das Ganze als Testbetrieb ohne gesetzliche Grundlage munter weiter. Man könnte sich z.B. auch an den Erkenntnissen anderer Länder orientieren: Sie haben E-Voting abgesagt (Norwegen, Frankreich, Deutschland). Wer will das in 3 Jahren noch stoppen, wenn bis dann noch keine offensichtliche Skandale – hervorgebracht durch Medien - vorliegen?

Es ist gut, dass wir eine direkte Demokratie haben. Lassen wir es nicht zu, dass sie verlorengeht. Alle politischen Vorstösse gegen das laufende Projekt E-Voting CH sind zu befürworten.