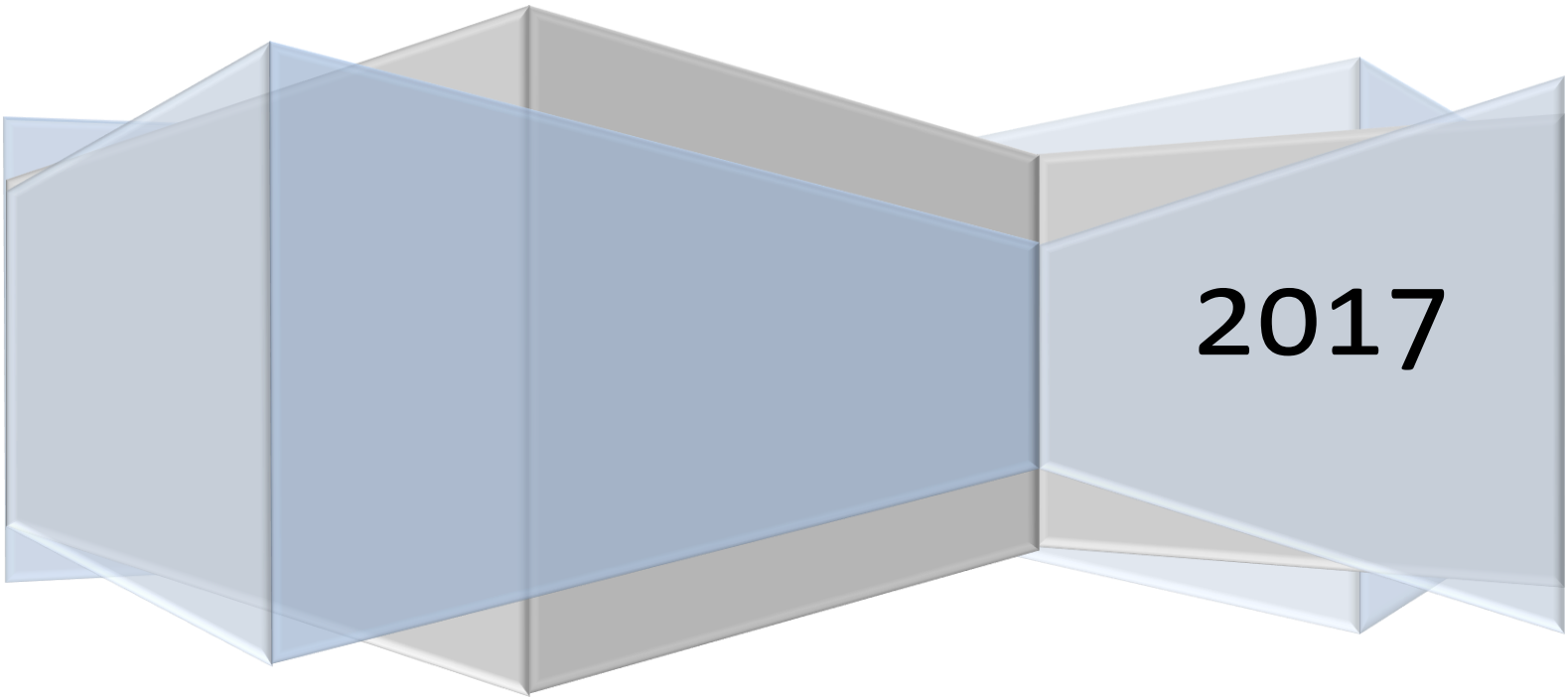
René Droz

E-Voting
Das Ende der Demokratie

Jetzt legen wir uns ein Kuckucksei ins Netz

2018/01.3.0



E-Voting Schweiz - Das Ende der Demokratie

Vorwort

Die Bundeskanzlei möchte mit E-Government den Kontakt zwischen Bürger und Staat modernisieren und vereinfachen. E-Voting als Teil des E-Governments soll für die Stimmbürger auch das Wählen und Abstimmen -verglichen mit der Briefwahl- noch bequemer machen, wobei aber wohl auch die Effizienz der Auszählungsarbeit bei den Behörden vorne im Blickfeld gestanden haben dürfte.

Auslandschweizer Verbände monieren immer wieder, dass sie je nach Auswanderungsland bei der brieflichen Abstimmung durch die schlechten postalischen Bedingungen behindert werden. Sie dienen damit als praktisches Aushängeschild für die Notwendigkeit des Projektes, das ansonsten wenig Zwingendes aufweist.

Progressive Kreise glauben, dass wenn die Politik näher an die neuen Technologien rutscht, sie von den Jungen besser akzeptiert würde. Man schielt wohl auf eine Vergrösserung des eigenen Wählerpotentials.

Kritische Stimmen gibt zwar es schon, aber so lange der politische Prozess korrekt eingehalten wird, prallen inhaltliche Argumente über Risiken und Kosten an der Realität mit der Verordnung 161.116[1], welche noch über keine konkrete Grundlage auf Gesetzesstufe verfügt, ab. Jetzt ist der Bundesrat an der Ausarbeitung eines Gesetzesentwurfes, der dann vom Parlament zu genehmigen ist. Es ist zu hoffen, dass das Parlament den Gesetzesentwurf beerdigt, oder dass es mindestens zu einem Referendum kommt. Das Risiko ist nicht tragbar.

Ich beschäftige mich vertieft mit der Frage, warum dieses unmögliche Fehlkonstrukt eines trojanischen Pferdes, das die Grundlagen unseres politischen Systems in Frage stellt, sich nicht mit mehr Opposition konfrontiert sieht. In dieser Broschüre versuche ich, auch darauf einige Antworten zu geben.

Zwar geht es mir nicht primär um die Kosten, welche schon seit Jahren hier ausgegeben werden. Wie bei allen skandalträchtigen IT Projekten des Bundes, sind aber auch hier die Kosten und die Kostendeckung nicht transparent gemacht worden. Es ist daher zu vermuten, dass der Steuerzahler, nicht der Kunde (=Stimmbürger/in) die Zeche bezahlen wird und schon gar nicht der Besteller des Systems.

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

Inhalt

Versionskontrolle:
Neuerungen seit 2017/09.01.1 in Kap. 1.1, 2.5.1, 2.5.3, 2.5.5, 2.7.2, 2.7.6, 2.7.8, 3.4, 5

1 Die Geschichte des E-Voting CH

Im Rahmen von E-Government sucht die Bundeskanzlei nach Verbesserung der Effizienz bei der Zusammenarbeit zwischen Volk und Behörden. Selbstverständlich darf dieser Grundsatz unterstützt werden.

1.1 Motivation für E-Voting

Nachvollziehbare Gründe beim E-Voting sind folgende auszumachen:

- *Auslandschweizer mit langen Postzustellungszeiten haben Mühe mit der Stimmabgabe*
- *Invalide können bequem zu Hause auch abstimmen*
- *Kürzere Auszählungszeiten/ oekonomische und oekologische Einsparungen*
- *Akzeptanz des politischen Prozesses bei den Jungen*

1.2 Chronik bis 2017/4

Folgende Chronik ist bei der Bundeskanzlei (BK) veröffentlicht worden:

2000	*Start Vote électronique*
2004	*Genf: erste Versuche bei eidgenössischen Abstimmungen*
2005	*Neuenburg: erste Versuche bei eidgenössischen Abstimmungen*
2005	*Zürich: erste Versuche bei eidgenössischen Abstimmungen*
2008	*Genf, Neuenburg, Zürich: gleichzeitige Versuche*
2008	*Neuenburg: erstmals Auslandschweizer und Auslandschweizerinnen zugelassen*
2009-2011	*Beherbergungsverträge zwischen Genf und den Kantonen Basel-Stadt, Luzern und Bern für Auslandschweizerinnen und Auslandschweizer*
2009	*Gründung des Consortiums Vote électronique bestehend aus den Kantonen Aargau, Freiburg, Graubünden, Schaffhausen, St.Gallen, Solothurn und Thurgau*
2010	*Erste Versuche in 12 Kantonen*
2011	*Erste Versuche bei den Nationalratswahlen in den Kantonen Basel-Stadt. Aargau, Graubünden und St. Gallen. Die Versuche sind auf Auslandschweizerinnen und Auslandschweizer konzentriert.*
2012	*50% AuslandschweizerInnen können die elektronische Stimmabgabe bei Bundesabstimmungen nutzen*
2013	*Dritter Bericht zu Vote électronique des Bundesrates*
2014	*Inkrafttreten der neuen Rechtsgrundlagen*
2015	*Nationalratswahlen mit Einsatz der elektronischen Stimmabgabe in fünf Kantonen*
2015	*Auflösung des Consortiums Vote électronique*
2016	*Freiburg: erster Einsatz des Systems der Schweizerischen Post*

Die letzte Meldung war die folgende:

Bern, 05.04.2017 - An seiner Sitzung vom 5. April 2017 hat der Bundesrat die nächsten Schritte zur flächendeckenden Einführung der elektronischen Stimmabgabe beschlossen. Im Fokus stehen Massnahmen im Bereich der Transparenzbildung (Offenlegung des Quellcodes) sowie namentlich die Überführung der elektronischen Stimmabgabe von der derzeitigen Versuchsphase in den ordentlichen Betrieb.

1.3 Zuständigkeiten

- *Die Bundeskanzlei erstellt die Verordnung über die Zulassungsbedingungen*
- *Die Kantone betreiben die Anlage und sind für deren Einsatz zuständig*
- *Der Bürger soll „möglichst" auf die briefliche Stimmabgabe verzichten (Wahlen und Abstimmungen)*

1.4 Abstimmungsunterlagen

Auf das elektronische Versenden der Abstimmungsunterlagen verzichtet die BK. Sie kennt also das Risiko von Verfälschungen und dasjenige der Vortäuschung von Verfälschungen. Das würde die Verwaltung ganz schnell überlasten und diskreditieren.

1.5 E-Referenden ?

Sie sind nicht vorgesehen. Das ergäbe dann doch allzu schnell zu viele Referenden und würde die Bundes- und Kantonsverwaltungen überlasten.

2 Das Risiko

Ein Risiko besteht grundsätzlich aus dem Produkt der Wahrscheinlichkeit, dass ein Vorfall eintritt, und der Schwere seiner Folgen, falls er eintritt.

2.1 Das Risiko des Einzelnen

Das Leben ist riskant. Jeder geht Risiken ein. Am Morgen bei der Überquerung der Strasse kann man tödlich verunfallen, beim Bewerbungsgespräch kann man sich unter dem Wert verkaufen, beim Haustürverkauf über den Tisch ziehen lassen.

Persönliche Risiken werden persönlich verwaltet. Jede(r) entscheidet selbst über das Eingehen ganz bestimmter Risiken. Jede(r) hat daher auch ein bestimmtes Einschätzungsvermögen, welche Risiken für ihn/sie tragbar sind und welche nicht. Das mag im Einzelfall total falsch sein, weil der/die Einzelne sich falsche Vorstellungen macht, aus welchen Möglichkeiten das effektive Risiko besteht. Doch weil der/die Einzelne das Risiko auch selbst trägt, ist das für die Gesellschaft als Ganzes kein Problem.

2.2 Wie werden gesellschaftliche Risiken bewertet?

Wenn ich ein Risiko eingehe, dessen mögliche Folgen die Allgemeinheit tragen muss, so handelt es sich um ein gesellschaftliches Risiko, auf das die Gesellschaft einen Einfluss nehmen sollte und normalerweise auch will. Jeder lässt sich z.B. obligatorisch versichern und die staatliche Versicherung trägt den Schaden. Wer aber kann ein solches Risiko abschätzen, damit mit den Prämien die Kosten gedeckt sind? Das Bundesamt für Statistik liefert Zahlen aus der Vergangenheit und meist sind Volk und Politik darüber einig, dass diese Zahlen einigermassen realistisch das Risiko widergeben. Bei neuartigen Risiken lässt man gerne eine Studie machen, wobei aber gerade bei Abstimmungen immer wieder festgestellt werden muss, dass diese wissenschaftlichen Erkenntnisse immer wieder der realen Zukunft nicht standgehalten haben. Die Studiengeber geben dabei meist auch die Rahmenbedingungen an, von denen auszugehen sei. Es ist nicht verwunderlich, dass solche Ergebnisse auch so enden wie von Auftraggebern erwartet. Da stellt sich die Frage, wer überprüft denn die Wissenschaftlichkeit des Studienauftrages?

Die Bundeskanzlei ist trotz dieser schlechten Erfahrungen von Staates wegen zuständig für die abschliessende Beurteilung der möglichen Auswirkungen von Abstimmungsergebnissen. Das „Abstimmungsbüchlein“, welches formell immer hervorragend gemacht ist, hinterlässt für die meisten Leute einen so guten Eindruck, dass sie auch den oft völlig daneben liegenden numerischen Aussagen über die Abstimmungs-Folgen der Regierung Glauben schenken und ihre Risiko-Überlegungen daran festmachen.

Zum Glück kommen aber immer auch Gegner zu Wort und diese haben manchmal die inhaltlich besser nachvollziehbaren Argumente. Es gibt Risiken, die lassen sich eben nicht durch Messungen aus der Vergangenheit beschreiben und dann müssen von jedem(-r) Stimmbürger/-in Grundsatzüberlegungen mit einbezogen werden, für die sowohl sein Kopf als auch sein Bauch eine passende Antwort finden muss. Der „gesunde Menschenverstand“ berücksichtigt und rechnet das menschliche Verhalten bei veränderten Grundbedingungen mit ein, unabhängig davon, ob es für solche Situationen passende Statistiken gibt.

Was besonders stossend ist, insbesondere für Insider der Bundesverwaltung, dass oft nicht einmal einschlägige interne Bundesstellen wie der Nachrichtendienst für Fragen von Sicherheits-Risiken konsultiert werden. Offenbar ist die Einheit der Regierungsmeinung wichtiger, als die *kontradiktorische Auseinandersetzung* mit dem Thema. Ein generelles Misstrauen zwischen Ämtern kann daraus ebenfalls abgelesen werden. Das wiederum bestätigt dem kritischen Bürger, dass es notwendig ist, selber mitzudenken. Die Faktenlage der Risiken ist wichtig für deren Bewertung, gibt aber noch keine eindeutige Antwort auf diese Bewertung. Dazu wird das eigene Wertesystem benötigt und das unterliegt der freien politischen Willensbildung.

2.3 Wer bestimmt, welche Risiken wir als Gesellschaft eingehen wollen?

Da erkennen wir den wesentlichen Unterschied, der unsere schweizerische Gesellschaft von fast allen anderen unterscheidet. Während in allen anderen Ländern eine Elite gewählt wird, welche über die Geschicke des Landes und damit über gesellschaftliche Risiken entscheidet, haben wir in der Schweiz die direkte Demokratie. Das Volk, der Souverän, kann die Erkenntnisse einer Elite über den Haufen werfen, wenn die Mehrheit der Leute mit der Regierungsmeinung nicht überzeugt worden ist. Eine absolut zentrale, ganz wichtige Einrichtung der Demokratie! Mehrheit vor Wahrheit.
Es gibt ja nur 2 Alternativen: Wahrheit vor Mehrheit oder Mehrheit vor Wahrheit. Die Frage beim ersteren ist oben beschrieben: Wer bestimmt, was wahr ist? Wenn die Risiken nicht richtig eingeschätzt werden, so werden die Überlegungen der Abwägung zwischen Risiken und Chancen garantiert falsch herauskommen. Für die demokratische Willensbildung ist also die „Wahrheit“ durchaus zentral, man kann sie zwar nie ganz für sich beanspruchen, aber man kann ihr mit besseren Begründungen so nahe wie möglich kommen. Man muss das vor allem wollen. Informationen dazu gibt es heutzutage genug, man muss sich lediglich die Mühe machen, diese alle aufzunehmen, zu sortieren und zu bewerten, selbst wenn dabei der Einzelne Fehler machen kann. Auch wenn bzw. gerade weil die Regierung versucht ist, die richtige Antwort uns bequem auf dem Tablett zu servieren. Sie macht nämlich auch Fehler, sowohl bei der Beurteilung der Faktenlage als auch bei der Bewertung der Risiken!
Demokratie ist eben nicht nur einen Mausklick weit weg, sondern muss durch geistige Anstrengung erarbeitet werden. Schon allein diese Erkenntnis hätte zum Schluss führen müssen, dass E-Voting ein Schritt in die falsche Richtung ist. Nicht die Bequemlichkeit der Entscheidung bringt mehr Demokratie, sondern verbesserte Abklärungen und Kommunikation von Sachverhalten und die Versachlichung von Debatten.

2.4 Die Relativierung von Risiken im Leben

Um die Tragbarkeit eines einzelnen Risikos sinnvoll einschätzen zu können, vergleicht der intelligente Mensch dieses Risiko mit allen anderen, die er einzugehen bereit ist. Darauf richtet er sein Augenmerk. Wenn es ein auffallendes Risiko ist, so wird er es bekämpfen (vermindern, abwälzen, vermeiden), wenn nicht, wird er es mittragen (akzeptieren, ignorieren) wie alle anderen Risiken.

Es gibt ein paar einschlägige Risiken, die wir im Leben kennen.

- Der Blitzschlag

Der Blitzschlag ist zufällig, trifft einen selber, ist äusserst selten, wenn er aber vorkommt, ist er meist tödlich. Wie reagiert der Mensch darauf? Er achtet auf die beeinflussenden Parameter und vermeidet alle Situationen, die das Risiko zum Problem machen können: Bei Gewitter keine offenen Felder oder Bäume suchen. Schema: Das Risiko trage ja ich, darum schütze ich mich.

- Das Atomkraftwerk

Ein grösserer atomarer Unfall ist äusserst selten, hängt von der strikten Einhaltung der Sicherheitsbedingungen durch die Betreiber ab. Wenn er aber vorkommt, kann er für ganze Regionen, also auch für andere als die, die das Risiko bestimmen, fatale Folgen haben. Also ein gesellschaftliches Risiko. Wie reagiert diese darauf? Sie achtet peinlich auf die Einhaltung der Sicherheitsnormen, eine Oberaufsicht beaufsichtigt die Aufsicht dafür. Ist der Unfall aber nur davon abhängig? Die in letzter Zeit eingebrachten Bedenken wegen möglicher Selbstmordattentäter, die mit Flugzeugen oder Raketen den Vorfall bösartig herbeiführen könnten, sind in den Sicherheitsüberlegungen noch nicht ernsthaft berücksichtigt worden. Noch gibt es weltweit erst einen einzigen vergleichbaren Vorfall (2001) und das entsprechende Risiko wird deshalb (noch) verdrängt. Schema: Das Risiko ist da, wird aber von der Gesellschaft getragen. Weil die Statistik noch nicht da ist, findet es im Abstimmungsbüchlein, d.h. in der öffentlichen Wahrnehmung keinen Einlass und wird damit gesellschaftsfähig.

2.5 Und das Cyberrisiko beim E-Voting?

Das Cyberrisiko – dass Wahlen/Abstimmungen bei der Auszählung manipuliert werden - ist offenbar für den Normalbürger ausserordentlich schwierig abzuschätzen. Es müssen folgende Einzel-Risiken betrachtet und mathematisch korrekt summiert werden:

A. Das Risiko, dass die Computer der Stimmbürger von Outsidern manipuliert werden
B. Das Risiko, dass die Computer der Stimmbürger von Insidern manipuliert werden
C. Das Risiko, dass die Computer der Auswertezentrale von Outsidern manipuliert werden
D. Das Risiko, dass die Computer der Auswertezentrale von Insidern manipuliert werden

Der Nachrichtendienst der Schweiz beurteilt das Cyberrisiko insgesamt als eines der dominanten Risiken der heutigen Schweiz. Auch wenn dort im sicherheitspolitischen Bericht nicht direkt das E-Voting genannt wird, sollte das doch eigentlich bei jeder Behörde zu den richtigen Erkenntnissen führen. Denn in der Cyberkriminalität gilt das Motto: *Alles was technisch möglich ist, wird gemacht.* Jeder Trick findet früher oder später eine passende Anwendung in der kriminellen Betätigung.

Während das Potential von falsch ausgezählten Briefwahlstimmen bei einigen wenigen Stimmen pro Gemeinde liegt, weil die einzelnen Auszählungen dezentral in jeder Gemeinde akribisch im Mehraugenprinzip überprüft werden und im Bedarfsfall auch nachgezählt werden können, ist auf dem Internet schnell mit Zehntausenden oder Hunderttausenden manipulierten Stimmen zu rechnen, die auf gar keine vernünftige Art und Weise zentral (d.h. von den Kantonen) überprüft oder nachgezählt werden können (s. unten).

Wenn wir das E-Voting Risiko heute 2017 betrachten, so beträgt das *Potential von gefälschten Stimmen*[2] wohl „nur“ einige wenige Prozente. Mit dem jetzt geplanten Ausbau der E-Voting Testanlage liegt aber der Möglichkeitsbereich bereits bei 30% und die 100% Marke wird vom Bundesrat bereits heute angestrebt.

Für meine Werthaltung ist ein Erwartungswert von mehr als 0.1 % falscher Stimmen nicht mehr tragbar. Diese Grenze unterliegt natürlich aber dem Wertesystem jedes Betrachters. Die Frage ist jetzt, wie steht es mit dem Risiko, dass das Potential genutzt wird? Man muss dabei bedenken, dass

[2] Anteil des Elektorates mit E-Voting

mit der Manipulation von 10% Stimmen fast alle Abstimmungen kippen. Bei der ME- Initiative wären es bereits 0.1% Stimmen gewesen.

2.5.1 Risiko A: Manipulation durch Outsider am Computer Stimmbürger

Dieses Risiko kann man wie folgt in einfacher Weise zusammenfassen. Folgende Bedingungen müssen alle erfüllt sein: Es braucht (1) Leute, die sehr gut hacken können und die das zu hackende System gut kennen, es braucht (2) Leute, die Geld dafür ausgeben, eine Manipulation zu veranlassen, (3) eine Umgebung, die möglich macht, dass die Beteiligten (1) und (2) anonym bleiben und dass (4) die Manipulation selbst unerkannt oder zumindest unbewiesen bleibt.

Um das Risiko jetzt zu beurteilen, muss ich nur noch wissen, wie sehr die einzelnen 4 Elemente erfüllt sind:

(1) Die **Existenz von Hackern** kann man nicht ernsthaft anzweifeln. Das VBS unterscheidet mit den 5 Kategorien von Hackern 5 unterschiedliche Bedrohungsstufen. Das E-Voting System selbst kann jeder Schweizer Bürger erwerben und dessen Verhalten analysieren. Das ist nötig, um die betreffenden Systeme erfolgreich manipulieren zu können.

(2) Die Tatsache, dass es Leute bzw. Organisationen gibt, die zumindest den **Willen** haben, für Geld politische Entscheidungen herbeizuführen, kann heute auch nicht mehr ernsthaft angezweifelt werden. Der Schritt, dafür in die Kriminalität zu gehen, ist bestimmt ein Schritt, der nicht jeder macht. Die Aussicht, dass die Anonymität garantiert ist, könnte aber sehr wohl den einen der andern dazu verleiten, dies zu versuchen…

(3) Dass es eine **Umgebung** gibt, die **anonymes Geschäften** möglich macht, ist vielleicht der breiten Öffentlichkeit entgangen. Insider jedoch wissen alle, dass im sog. „Dark Net“ z.B. Waffen illegal gekauft und Killer z.B. aus Russland angeheuert werden können, wobei in diesen Fällen die Warenübergabe und die Auftragsumsetzungen immer doch noch ein Restrisiko beinhalten und deshalb auch beliebig teuer sind. Das Manipulieren von Cyberresultaten an irgendwelchen Computern von Stimmbürgern hingegen enthält praktisch keine Risiken.

(4) Der Datenschutz und dessen Umsetzung bei der E-Voting Lösung sorgen dafür, dass ein Stimmresultat, einmal in der Zentrale angekommen, **nicht mehr** dem Stimmbürger zugeordnet, d.h. mit seinem Willen verglichen und damit zentral **kontrolliert** werden kann. Durch die sog. Verifizierbarkeit, die zwar offenbar selbst nach Erkenntnissen der Bundeskanzlei „kurz- und mittelfristig (gar) nicht zu erreichen ist“, müsste darum der Stimmbürger seine am Computer festgestellte Manipulation selbst erkennen und melden. So einen Vorfall kann es geben. Aber was motiviert einen Stimmbürger, der aus Bequemlichkeit das E-Voting gesucht hat, seinem Computer zu misstrauen und ihn akribisch auf kryptische Codes, konform zur ausführlichen Anleitung zu überprüfen, und sich nachher allenfalls noch mit einer Meldung an die Behörden herumschlagen, die „ja eh nichts nützt“? Vielleicht würde er als Idiot eingestuft, der mit den modernen Mitteln nicht zu Recht kommt oder gar selber verdächtigt, Fehler vorzutäuschen, um so die Glaubwürdigkeit des Abstimmungsresultates zu untergraben. Weder Kantonsbehörden noch die Bundeskanzlei haben Ressourcen, solchen Fällen wirklich nachzugehen und das schon gar nicht in einem Umfang, der für das Endresultat relevant wäre. Es gibt keinerlei Anhaltspunkte, wie gross die Dunkelziffer wäre. Offenbar erwägt die Bundeskanzlei trotzdem in solchen Fällen, die E-Votes nicht zählen zu lassen oder während des Abstimmungs-Vorganges zu blockieren. Das aber wäre reine Willkür und untergräbt das Vertrauen des Volkes in die Behörden ebenfalls in

höchstem Masse. Unbekannt ist auch, in welchem Masse die Öffentlichkeit von solchen Vorgängen erfahren würde.

Man kann deshalb mit Fug behaupten, dass alle Elemente für das Eintreffen des Risikos A erfüllt sind und es somit nur eine Frage der Zeit ist, bis es eintrifft oder zumindest berechtigte Zweifel das Grundvertrauen in den Staat in höchst gefährlicher Weise untergraben.

2.5.2 Risiko B: Manipulation der Abstimmungsresultate durch Insider am Computer Stimmbürger

Der Vater einer Familie loggt sich auf dem Computer ein und stimmt gleich für alle Personen in der Familie ab, weil er die Post der Behörden geöffnet hat. Das kann jedoch auch bei der Briefwahl passieren, wobei dort noch die Unterschrift gefälscht werden müsste, was aber auch kein wirkliches Hindernis darstellt.

Das Risiko B muss im Folgenden nicht mehr beachtet werden, es ist kein Zusatzrisiko im Vergleich zur Briefwahl und wird dominiert von Risiko A und D.

2.5.3 Risiko C: Manipulation der Abstimmungsresultate durch Outsider am Computer der Auswertung

Das Hacken der Auswertezentrale durch einen Outsider kann nicht vernachlässigt werden, aber stellt im Vergleich zu A) und D) einen eher minderen Risikobeitrag dar, falls alle Sicherheitsmassnahmen der Installation UND des Betriebes professionell getroffen wurden und dort insbesondere nicht gespart wird. Ob das aber hier der Fall ist, unterliegt keiner demokratischen Kontrolle. Mit Nachlässigkeiten von Insidern wären Manipulationen von Outsidern möglich, und die hätten noch verheerendere Auswirkungen, trifft es doch direkt das Endergebnis. Eine blosse Behinderung des Wahlvorganges dürfte ziemlich einfach sein, führt aber nicht unbedingt zu einer gezielten Manipulation. Eine solche Manipulation wäre theoretisch allenfalls zwar nachweisbar, aber wer garantiert, dass man dem nachgehen würde und dies auch veröffentlicht würde? Was stellt man hier für Vertrauensansprüche?

2.5.4 Risiko D: Manipulation der Abstimmungsresultate durch Insider am Computer der Auswertung

Hier wird ein korrupter Administrator benötigt, um dieses Risiko eintreten zu lassen. Es ist nicht davon auszugehen, dass ohne den Spezialisten der die Anlage bereitstellenden Firma eine eigenständige Überprüfung durch einen Kantonsbeamten stattfinden kann. Selbst wenn man den ganzen Aufwand einer zertifizierten Auditierung durch unabhängige Dritte auf sich nähme, könnte ein geheimes Eingreifen in den Code oder in die Ausgabe der Daten kaum zweifelsfrei belegt werden.

Dieses Risiko verweist auf die Abhängigkeit von Einzelpersonen. **Noch nie zuvor war die Integrität einer Abstimmung von einzelnen Personen abhängig!** In der Verfassung haben wir die Zuständigkeit für die korrekte Auszählung den 26 Kantonen überlassen. In Tat und Wahrheit ist es jetzt nicht mehr die Gesamtheit aller Auszähler und ihrer Überwacher, sondern einiger weniger IT Spezialisten von 1-2 ausgewählten Firmen.

2.5.5 Risiko E: Verlust der Anonymität durch Abfluss der Abstimmungsdaten.

Nachdem feststeht, dass jegliche PC Stationen am Internet, die nicht durch spezielle Abschottungen geschützt sind, gehackt werden können, ist auch offensichtlich, dass Abstimmungsdaten ebenfalls aus der eigenen PC-Station abfliessen und an unbefugte Dritte gelangen können. Es bedürfte allerdings dazu eine Verknüpfung mit dem Namen und der Adresse des Abstimmenden, um einen einwandfreien Datensatz zu generieren, der für irgendwelche kriminellen Zwecke brauchbar wäre.

Das wird nicht ganz leicht sein, weil der Abstimmende nicht unbedingt identisch mit dem Besitzer oder Standardbenutzer des PCs ist. Der Authentifizierungscode zur Identifikation ist zwar wohl nicht errechenbar, aber die Generierung und Verteilung dieser Codes unterliegt auch den diversen generellen IT-Risiken. Der Wert von solchen Datensätzen für internationale Kriminalität oder Geheimdienste dürfte zwar eher begrenzt sein, im Vergleich zu einem politischen Volksentscheid. Dieses Risiko hier aber trägt der einzelne Stimmbürger selbst. So ergibt das eine andere Sicht.

2.6 Wer sind die Hacker?

Es gibt sowohl Einzelpersonen als auch Organisationen, die Cyberangriffe durchführen. Man unterscheidet gemäss VBS[3] 5 Stufen der Bedrohung:

(1) Amateure / Hobby –Hacker. Sie sind Einzelpersonen mit Kenntnissen und gekauften oder selbst entwickelten Anfänger-Hilfsmitteln und nicht gefährlich für E-Voting.

(2) Intrinsisch motivierte Entwickler von Hacking Tools. Sie arbeiten mit professionellen Methoden und Hilfsmitteln und auch nicht direkt gefährlich, können aber auch u.U. Zulieferer für kriminelle Organisationen werden. Durch die weltweite Teilung von solchen Hilfsmitteln („Open Source“) sind sie sich oft auch nicht bewusst, welche Folgen ihre Arbeit u.U. hat.

(3) Gewöhnliche professionelle Cyberkriminelle mit Finanzen und Verbindungen zu anonymen Kundenplattformen. Sie sind wohlorganisiert wie Konzerne und machen Milliardengeschäfte mit kommerzieller Schad-Software in Verkauf und Einsatz. Den Schaden dieser Produkte kann man zu einem guten Teil mit mehr oder minder aufwendigen Abwehrmassnahmen bekämpfen, da sie breitflächig benutzt und deshalb auch schnell entdeckt werden können. Die IT-Sicherheitsindustrie ist in permanentem Abwehrkampf und liefert nach kurzer Zeit (Stunden bis Tage) „Patterns“, welche diese Schadteile entdeckt und entfernt.

(4) Professionelle Cyberkriminelle mit grösseren Finanzen und Verbindungen zu Geheimdiensten und/oder Zugang zu nicht-öffentlichem Wissen zu Produkten. Sie können hochspezifische Spezialanfertigungen für Spezialkunden erstellen. Diese werden von allen bekannten Abwehrmassnahmen nicht oder erst viel später mit sehr aufwendigen Methoden erfasst (Beispiel EDA-Fall aus dem Jahr 2012, wurde 2014 in der Presse am Rande erwähnt).

(5) The Top 5: Darunter NSA, FSB und China: Die wissen sozusagen alles über Hintertüren und Schwachstellen bei jeglicher IT (auch bei Hardware), zumindest der aus dem eigenen Land und dort ist mit allem zu rechnen. (Beispiel Stuxnet: Eingriffe ins iranische Atomprogramm)

2.7 Die Cyberkriminalität

Um das Risiko des E-Voting richtig einschätzen zu können, muss man sich grundsätzlich klar werden über die generellen Risiken der Cyberkriminalität und den Bezug zur aktuellen Wirklichkeit.

Die Motive der Cyberkriminellen unterscheiden sich nicht gross von der normalen Kriminalität in Bezug auf die Motivation: Es sind dies Macht und Geld. Die Cyberkriminalität ist kein theoretisches Risiko, sie findet statt. 2015 sollen in der Schweiz 70000 Fälle von Cybercrime gemeldet worden sein[4]. Die Anzahl der Attacken auf dem Netz auf dem schweizerischen Gebiet dürfte eine 8-10 stellige Zahl darstellen. Jede(r) Einzelne könnte diejenigen, die bei ihm lokal auftreten, messen, wenn er wollte und etwas Zeit dafür aufwendet. Nur wenige Attacken haben im Ansatz Erfolg und nur ein

[3] S. VBS Intra 1/17
[4] S. http://www.anwalt.org/cyberkriminalitaet/

Bruchteil von denen haben effektive Auswirkungen. Und nur die grössten bzw. spektakulärsten Fälle werden in der Öffentlichkeit bekannt.

Man unterscheidet hier die allgemeine Kriminalität aus materiellen Interessen und gezielte Attacken gegen bestimmte Personen oder Anlagen aus politischem Motiv.

2.7.1 Der Erfolg

Was ganz wichtig ist, ist die Erkenntnis, dass der Erfolg durch folgende Faktoren gegeben ist:

(1) Durch die riesige Menge an Betrügern

Man darf die gesamte Weltbevölkerung als Teilnehmende im Internet betrachten und somit sind auch weltweit alle Verbrecher quasi netzmässig vor der Haustüre. Durch den weltweit weitgehend freien Zugang zu technischem Wissen und dem riesigen Beutepotenzial versuchen kriminelle Organisationen jeglicher Couleur in aller Welt von dem riesigen Kuchen ein Stück abzuschneiden.

(2) Durch die riesige Menge an potentiellen Opfern

Opfer finden sich überall dort, wo konsumiert wird, wo Finanztransaktionen stattfinden und wo die Kenntnis vertraulicher Daten oder die Manipulation von solchen zu erpresserischen Aktionen führen können.

(3) Durch die Anonymität

Die Anonymität veranlasst oft auch rechtschaffene Leute zu kriminellen Taten, wenn sie sich in einer Notsituation befinden. Sie können mit etwas Geschick ohne weiteres anonym bleiben. Ein staatlicher Aufwand, solchen Machenschaften nachzugehen, wäre enorm und wird durch diverse Faktoren behindert.

(4) Durch das Wissen von spezifischer und von geheimer Information

Schwierigere Fälle von gezielten Attacken sind solche, wo mit Abwehrmassnahmen gerechnet werden muss. IT Anlagen von Behörden und Armeen sind mit besonderen Schutzmassnahmen versehen. Dort benötigt der Versuch einzudringen zusätzlicher spezifischer Informationen über das auszukundschaftende System, die in längeren Probeläufen gesammelt werden müssen. Im Extremfall wird zusätzlich Geheimwissen (Schwachstellen, Hintertüren) über bestimmte Technologieprodukte benötigt, über welches nur Behörden, Geheimdienste und Technologiefirmen verfügen. Es ist kein Geheimnis, dass solches Wissen auch gehandelt wird.

2.7.2 Die Arten

Die Möglichkeiten der kriminellen Betätigung im Cyberraum sind äusserst vielfältig. Sie reichen von unerwünschter Werbung bis zu Schwerverbrechen. Man muss deshalb die grössten Kategorien zusammenfassen:

- Die „**Massenprodukte**“ umfassen das Einschleusen von Werbung und die Nutzung der Rechenkapazität der Computer über das Phishing (Vortäuschen falscher Webseiten und Animation des Benutzers zur Eingabe von Passwörtern) bis zur Erpressung durch die Chiffrierung der Daten auf dem eigenen Computer, die nur dann wieder entschlüsselt werden, wenn ein bestimmter Geldbetrag auf ein ausländisches Konto fliesst, das sofort wieder gelöscht wird, wenn die Transaktion erledigt ist.

- **E-Banking** ist der direkte Eingriff in Finanztransaktionen.

- Der Verlust der primären Account Credentials ist abgesichert durch einen Code über einen Zweitweg mit dem Besitz eines Zweitgerätes.
- The „man in the middle“ Methode geht davon aus, dass der Datenfluss live während einer Transaktion unterbrochen wird und über den betrügerischen Computer führt, welcher die Zweitweg-Authentifikationen auch mitbekommt und die Daten des Zielkontos aber dann abändert. Kryptologische Methoden können diese Art Cyberattacke bekämpfen.
- Spezifische Trojaner auf dem Computer könnten hier auch die Ein- und Ausgaben fälschen und dem Benutzer die Richtigkeit vortäuschen. Die Banken fügen Plausibilitäts-Checks ein, welche auffällige Transaktionen[5] stoppen und hinterfragen.

- **Organisations-spezifische Angriffe** sind aufwendig und nur für eine bestimmte Zielobjektgruppe anwendbar. Sie verlangen meist Fähigkeiten der Bedrohungskategorie 4 oder 5. Industriespionage, Erpressung durch Kompromittierung vertraulicher oder persönlicher Daten, Ausspähung von Verwaltungen gehören dazu bis zur Beeinflussung von Politik und militärischen Fähigkeiten.

2.7.3 Begünstigende Faktoren und juristische Rahmenbedingungen

- *Datenschutz*

  Der Datenschutz soll dafür sorgen, dass persönliche Daten einer bestimmten Qualität vor fremdem Zugriff geschützt werden sollen. Das heisst, es werden Regeln und Beschränkungen erstellt für all die, welche mit den Daten rechtmässig in Berührung kommen. Der Staat nutzt deshalb diese Daten nicht in allen möglichen Weisen sondern nur so minimal, wie die entsprechende Dienststelle sie für die Erfüllung ihrer Aufgabe benötigt. Der Datenschutz schützt aber die Daten nicht aktiv, sondern nur gegen übermässigen Gebrauch von den Stellen, die sich sowieso ans Recht halten.

  Das sorgt dafür, dass Überwachungen oft nicht möglich sind, und deshalb auch Cyberattacken nicht festgestellt werden können. So kompromittiert der Datenschutz indirekt oft die Datensicherheit.

- *Kaum internationale Rechtshilfe*

  Abgesehen davon, dass Rechtsnormen wie der Datenschutz sowieso in jedem Land unterschiedlich sind, sind länderübergreifende Verfahren wegen Cyberkriminalität sehr selten. Sie beschränken sich auf wenige, wirklich in beidseitigem Interesse liegenden Fällen z.B. mit Millionenschäden zu Lasten dieser Staaten. Sie beschränken sich zudem auf Fälle, wo juristische Verfahren eingeleitet werden können, d.h. Verdächtige und Sachverhalte bekannt sind. Im Vorfeld von solchen Verfahren, wo die Daten erst ermittelt werden müssen, sind die Anhaltspunkte für Rechtshilfe praktisch nie gegeben.

- *Kollusion von Betrügern und Banken?*

  Die Banken, die oft im Zentrum von cyberkriminellen Machenschaften stehen, haben ein Interesse, Schwachstellen in ihren IT-Systemen geheim zu halten. Kundenschäden geben ein schlechtes Image und müssen möglichst verschwiegen werden. Der IT Aufwand ist aber meist

[5] Auffällig sind z.B. Zielkonten die – insbesondere im Ausland - kurzfristig erstellt und schnell wieder aufgelöst werden.

auch riesig und muss optimiert werden. Daraus folgt, dass in Bagatellfällen die Bank den Schaden übernehmen wird und nur in den grossen Fällen versuchen wird, einen Fehler des Kunden nachzuweisen. Gelingt dies nicht, muss sie den Schaden übernehmen und versuchen, den Fall so genau zu analysieren, dass er nach einer Korrektur nicht mehr auftritt. Die kriminelle Szene, die ein Interesse hat, die Schwachstelle weiter zu bewirtschaften, wird beim Schadensausmass auf möglichst kleinem Feuer arbeiten. Ansonsten müssen neue Opfer gesucht und/oder neue Methoden entwickelt werden.

- *Das Dark Net*
  Im normalen Internet sind die URLs, d.h. die Pfade zu den Zielobjekten (Servern) via *Domain Name Service* (DNS) jeweils einer IP Adresse zugeordnet. Via Netzprovider führt die IP Adresse zu einem bestimmten Punkt im Netz, dessen Koordinaten bekannt sind. Einzig die letzten Meter des möglichen WLANs können noch zu einer Ungewissheit zur Ortung des Netzteilnehmers führen, aber im Allgemeinen gibt es einen verantwortlichen Netzteilnehmer für diese IP mit Namen und Post-Adresse.
  Im Dark Net sind alle jene Computer zusammengefasst, deren IP Adressen NICHT dem öffentlichen DNS freigegeben werden. Wie aber kann man diese dann finden? Man muss sie nicht finden! Man muss sich einzig an einem Punkt eines TOR[6] Netzwerkes anschliessen.
  Dort sind diese Pfade erreichbar, aber ohne dass man selbst weiss, wie sie heissen bzw. welchen IP Adressen sie zugeordnet sind. Jetzt könnte man ja sagen, der TOR Gateway weiss es ja, man müsste nur dort nachschauen. Aber erstens gibt es einen privaten Betreiber/-in dieses Gateways, der/die diese Infos gar nie verraten würde und zweitens sind diese TOR Verbindungen mehrmals verschachtelt. Es wäre eine weltweite Aktion, diesen allen nachzugehen, um eine einzige Darknet Verbindung zu orten. Solche TOR Gateways am Internet zu installieren ist auch wegen des Datenschutzes gar nicht illegal, ausser in Diktaturen, die das wohl verbieten, soweit sie es können, denn es ist aufwendig, alle diese Geräte aufzuspüren. Dank diesen Darknet Verbindungen ist es z.B. in Diktaturen nämlich dennoch möglich, Verbindungen zu verbotenen Webseiten herzustellen und sich andere als regierungsfreundliche Informationen zu holen, ohne dass der Absender geortet werden kann.

- *Das Bitcoin*
  Mit dieser Währung kann weltweit bezahlt werden. Obwohl den Staaten dadurch Millionenbeträge an Steuern verloren gehen und damit überdies auch die Kontrolle der Geldflüsse an den (kontrollierbaren) Banken vorbeigeht, hat noch kaum ein Staat gewagt, diese Währung zu verbieten. Es nützte auch nichts, denn solange man in einem einzigen Staat wechseln kann, funktioniert diese Währung. Die Cyberkriminalität stützt sich weltweit auf die Finanzierung durch Bitcoin. Es ist anzunehmen, dass die OECD sich eines Tages damit näher befassen wird, aber wie gesagt, so lange es „Oasen“ gibt, nützt ein internationaler Versuch der Trockenlegung nichts.

2.7.4 Wie schützen sich Diktaturen?

Ohne die einschränkenden Rahmenbedingungen des Datenschutzes können sich Diktaturen mit Beschränkungen der Zuflusswege und restriktiver Überwachung jeglichen Datennetzverkehrs –

[6] *The Onion Routing*

zumindest des grenzüberschreitenden- nicht nur vor unerwünschter Information im Volk, sondern auch besser vor Cyberkriminalität schützen. Beispiele: China, Russland, Türkei. Dabei werden weder Kosten noch Verfügbarkeitseinschränkungen für die Nutzer gescheut.

2.7.5 Und wir?

Bei uns wird der Missbrauch der Überwachungstätigkeit durch den Staat zur Zeit bei vielen immer noch als höheres Risiko eingestuft als die Folgen weltweiter Cyberkriminalität durch fremde Mächte und kriminelle Organisationen. Allerdings hat die kürzlich erfolgte Annahme der Verschärfung des ND Gesetzes in der Schweiz[7] ebenfalls schon eine leichte Trendwende bzw. Kurskorrektur angedeutet.

2.7.6 Risikovermeidung durch „Sichere IT“

Es wird oft von sicherer und unsicherer IT gesprochen. Dabei wird unter „sicherer IT“ meist verstanden, dass die allgemein üblichen Vorkehrungen und Sicherheitselemente getroffen worden sind, während bei unsicherer IT auch diese fehlen. Selbstverständlich ist es auch hier so, dass die Sicherheit in unendlich vielen Stufen gemessen und beurteilt werden kann, aber nie vollständig vorhanden ist. Eine wichtige Stufe für die Unterscheidung ist aber die Frage, ob man mit ausschliesslich (gleich) sicheren Systemen verbunden ist oder ob es mindestens eines gibt, das den Anforderungen nicht genügt?

Was bedeutet es, ausschliesslich mit (gleich) sicheren Systemen verbunden zu sein? Es bedeutet, dass keiner meiner Partner mit einem unbekannten System Verbindungen haben kann, d.h. im Volksmund „mit dem Internet verbunden“ ist. Das könnte einzig in Firmensystemen der Fall sein, wo eine zentrale Stelle alle Netz-Teilnehmenden auf ihre Sicherheit überprüft und überwacht. Ausserdem müssen alle Verbindungen mit einem sicheren Kryptoalgorithmus verschlüsselt sein. Da diese Systeme aber meist doch auch einen (unverschlüsselten) Internet Zugang brauchen, sind auch sie nicht wirklich sicher. Die Sicherheit verlangt den Ausschluss sämtlicher relevanter Risiken, der Unsicherheit genügt das Vorhandensein eines einzigen.

Die Sicherheit ist das Gegenstück zum Risiko. Jeder der Computerteile kann Risiken haben und das grösste Risiko bestimmt den Sicherheitslevel.

- Das Betriebssystem

  Das Betriebssystem stellt die Haupt-Schwachstelle aller Computer dar, insbesondere im Aspekt der Vernetzung wie er oben besprochen ist. Jedes Betriebssystem ist der Chef des Computers. Seine Schwachstellen werden vom Hersteller via Internet irgendeinmal repariert und aber auch immer wieder mit neuen Schwachstellen versehen. Viele dieser Schwachstellen sind Hackern bekannt. Sie nutzen die Zeit, bis die Computer jeweils ihren Update eingefahren haben. Über diese Schwachstellen können sie dann in mehreren Schritten ihren Schadcode[8] einschleusen, der den Computer in ihrem Sinne abändert. Das muss nur einmal gelingen. Der nachträgliche Update des Betriebssystems nützt dann nichts mehr. Ein Virenschutzprogramm wird so etwas nur erkennen, wenn es ein weltweit bekanntes Muster ist.

- Die E-Voting Applikation

[7] Bundesgesetz vom 25.09.2015 über den Nachrichtendienst (NDG)
[8] Trojaner, Malware, Viren und deren vielfältige Bezeichnungen

Der E-Voting Applikation wird hier einmal unterstellt, dass sie nach allen Regeln der Kunst erstellt worden ist, sie wäre sonst ein erhebliches zusätzliches Risiko. Zur Zeit umfasst sie nicht einmal ein sicheres Teil-Modul (mit einem Hardware Chip), in welchem die Daten auch von einem manipulierten Betriebssystem nicht abgeändert werden können. Was aber auch dieses sicher nie unter Kontrolle hat, sind Input und Output des Benutzers. Das Unsichere sind deshalb die Tastatur und der Bildschirm des Computers. Der Schadcode sorgt dafür, dass sowohl der Benutzer als auch der Manipulator zufrieden sind. Ein entsprechender Austausch von DLL Dateien sorgt dafür, dass nicht das Resultat der Verifizierungsfunktion auftritt, sondern eine Funktion des Trojaners. Dazu braucht es (nur) die Kontrolle über das Betriebssystem. Und das ist jederzeit zu erreichen mit einem entsprechenden Cyberangriff.
Die Übertragung der (verfälschten) Eingabe wird nachher kryptologisch geschützt und kann nicht (noch einmal) verfälscht werden. Die riesigen Aufwendungen für diesen letzten Punkt können werbeträchtig verkauft werden und machen Eindruck. Sie lassen vergessen, dass das Problem wo anders liegt. Der Mensch muss nämlich hier die Kryptologie verifizieren.

Sicherheit ist ein ganzheitlicher Aspekt. *Vertraulichkeit, Verfügbarkeit, Integrität, Authentizität, Nicht-Abstreitbarkeit* sollen garantiert werden. Kryptologische Verfahren verhindern, wenn sie gut sind, Manipulation der Daten und den Zugang von aussen. Damit sind alle Ansprüche abdeckbar. Im Computer selbst sind aber die Daten nicht verschlüsselt. Ein Schadcode kann alles machen mit ihnen. Keine der genannten Ansprüche sind damit mehr abdeckbar.

Eine Sicherung des Betriebssystems wäre zwar technisch möglich, ist aber derart mit Einschränkungen, Überwachungsansprüchen und organisatorischen Prämissen versehen, dass der vorgesehene Ansatz, mit dem Heimcomputer des Benutzers ein sicheres E-Voting durchzuführen, schlicht eine Absurdität darstellt.

Man müsste ein eigenes System postulieren, das nur E-Voting kann, z.B. auf einer von mehreren komplett getrennten virtuellen Maschinen, die auf der Hardware des Benutzers installiert sind. Dieses virtuelle System müsste man ausserdem permanent auf seine Funktionsfähigkeit und Sicherheit überwachen. Dann könnten aber nur noch IT Leute mit E-Voting abstimmen. Denn wer sonst will eine solche Lösung für seinen Heimcomputer, ausser IT Leute selbst? Und wer würde diese überprüfen?

Eine eingefrorene E-Voting Lösung, die alle anderen Verbindungen und Funktionen unterbindet und keinerlei Administrationsfunktion zulässt, wäre sicherheitsmässig ebenfalls denkbar. Davor fürchten sich aber alle IT Hersteller, denn diese ist nicht mehr wartbar. Wer trägt dann die Kosten?

2.7.7 Und die Risiken beim Handy ?

Der nächste Schritt in unserer Anspruchsgesellschaft wird sein, dass man nicht nur zu Hause abstimmen können will, sondern auch jederzeit unterwegs. Was gibt es zusätzlich beim Handy zu sagen?

Alle Schwachstellen beim Computer gibt es beim Handy auch. Zusätzlich kann jedermann eine App selber erstellen, in den Appstore stellen und zum Download anbieten. Diese Apps können jegliche Funktionalitäten und auf alle Daten Zugriff haben. Es gibt gar keine Sicherheit mehr, denn die Daten auf dem Handy haben garantiert keinen Schutz mehr.

2.7.8 Vergleich E-Banking mit E-Voting

Alle Diskussionen mit der BK weisen darauf hin, dass gemäss ihrer Argumentation E-Voting wie E-Banking betrachtet werden muss. Es ist zwar nicht 100%ig sicher, aber wenn das auch funktioniert, warum soll dann E-Voting nicht sicher genug sein? Man setzt meist auf die Kontrollmöglichkeit und die Reaktion darauf. Aber was sind diese bei E-Voting? Der Vergleich der Sicherheitselemente zwischen E-Banking und E-Voting fällt eindeutig aus:

- *Die Prävention: Sicherheitsmassnahmen*

	E- Banking	E-Voting
generell	Die Bank kennt ein „normales" Verhalten und kann Abweichungen erkennen, hinterfragen und/oder verhindern.	Es gibt kein normales oder erwartetes Verhalten, da meine Stimme mir gar nicht zugeordnet werden kann.
Bei Verlust der Account Credentials[9]	Meist gesichert durch Zusatzcode via Zweitweg über Handy Netz und separaten Device (Handy)	Keine Sicherung durch Zweitweg. Printout mit User ID über Postweg. Allerdings gleich 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 Feststellung ist nicht garantiert. Selbst wenn sie eintritt, gibt es keine geregelten Massnahmen zur Korrektur und Verhinderung von Vertrauensverlust.

- *Die Kontrolle und das Feststellen des Betruges*

E- Banking	E-Voting
Ich stelle meinen Schaden immer fest und kann zusammen mit der Bank Massnahmen dagegen ergreifen.	Die Gesellschaft als Ganzes stellt u.U. einen Schaden fest, basierend auf Vermutungen, aber hat keine Möglichkeit etwas dagegen zu tun. Die Demokratie ist ausser Kraft gesetzt.

- *Das Opfer und die Hoheit über die Reaktion*

E- Banking	E-Voting
Mein manipuliertes Konto schadet (nur) mir. Ich habe die Kontrolle darüber.	Meine verfälschte Stimme schadet der gesamten Gesellschaft. Sie kann – als Ganzes – nichts tun. Die Bundeskanzlei hat die Kontrolle. Sie bestimmt willkürlich über die Reaktion.

2.7.9 Konklusion

IT-Insider und unsere Nachrichtendienste wissen es schon länger, aber seit den Enthüllungen von Edward Snowden könnte es allen nun bekannt sein: Mit einer vernetzen IT lässt sich praktisch alles machen, wenn die Fähigkeiten der Angreifer gross genug sind.

Das Risiko bei E-Voting ist so, dass wir unsere direkte Demokratie verlieren können durch die Manipulierbarkeit unseres Auszählungssystems. Dieses Risiko ist – aus gesellschaftlicher Sicht - mit keinen anderen Risiken vergleichbar. Man sollte sich über die Folgen davon klar werden.

3 Die Folgen der Einführung von E-Voting

Einer möglichen Manipulation muss ein politischer Entscheid vorausgehen, dessen Ausgang so wesentlich ist für den potentiellen Manipulator, dass er den Aufwand für eine Manipulation nicht scheut. Ich schätze, dass 1 Mio SFr. für das Engagement von guten Hackern für den initialen Aufwand dieser Aufgabe, die nicht unbedingt nach Schweizer Löhnen bezahlt werden müssen, bestens ausreichen wird.

[9] User ID/ Passwort. Sie können grossflächig gestohlen werden.

Man darf erstens nicht vergessen, dass heute bereits viele ausgeklügelte Hackerwerkzeuge billig verfügbar sind und dass zweitens diese Investition auch für künftige weitere Manipulationen eine gute Investition darstellt.

3.1 Wie muss man sich eine Manipulation vorstellen?

Heute wird unter „Manipulation“ bei der politischen Ausmarchung meist die unterschiedliche Nutzung der Medien und das unterschiedliche Werbebudget zwischen den Standpunkten verstanden. Das mag man ja so verstehen. Was aber, wenn Organisationen direkt auf die Abstimmungsresultate Einfluss nehmen können?

Wie könnte das geschehen? Man kann sich zwei Arten gut vorstellen:

A. Eine inländische **Interessengruppe** sucht anonym auf dem Darknet eine Verbindung zu einer anonymen Hackergruppe der Kategorie 4.
   - Es wird ein Geschäft ausgehandelt bei dem Leistung und Preise in Bitcoin festgelegt werden. Die Leistung besteht in der Manipulation von einigen Prozenten der Stimmenden. Mehr Prozente werden teurer. Sollte die Abstimmung zu einem erfolgreichen Ergebnis führen, gilt das Geschäft als erledigt. Andernfalls wird der Bitcoin Betrag zurückgeschrieben.
   - Der Lieferant kennt den Kunden nicht und umgekehrt. Über eine Kette von weltweit hunderttausenden unkontrollierbaren und legalen TOR Servern werden die IP Adressen verschleiert und damit die Ortbarkeit und die Nachverfolgbarkeit verunmöglicht
   - Die Manipulationen müssen entwickelt, eingeübt und optimiert werden. Man fängt mit kleinen Erfolgen bei einigen hundert Treffern an und steigert sich durch Optimierung der Algorithmen allmählich. Damit kann der Preis erhöht werden.
   - Die Bezahlung in Bitcoins erfolgt ebenfalls anonym und kann nicht über eine Bank verfolgt werden. Die Bitcoins werden irgendwo auf der Welt und irgendwann von ganz anderen Leuten umgetauscht.

B. Nachdem eine Abstimmung geplant ist mit internationalen Folgen, kann auch eine **ausländische Macht** der Kat. 5 aus eigenem Antrieb auf die Idee kommen, die politische Entwicklung der Schweiz zu ihren Gunsten zu beeinflussen.

Man muss wissen, dass auch auf dem Darknet innerhalb der Cyberkriminalität ein „sauberes“ Geschäftsgebaren besteht, das auf gegenseitigem Vertrauen beruht. Ohne dieses würde diese Branche nicht existieren können. Das heisst, Sie können auch als anonymer Kunde gute Qualität erwarten.

3.2 Das schwindende Vertrauen in die Politik

Es werden schon heute nach jeder Abstimmung Aussagen laut, nach denen die Ergebnisse ausschliesslich durch den finanziellen Aufwand der Gegenseite zustande gekommen seien. Meist ist es die Linke, die der meist finanzkräftigeren rechten Seite dies vorwirft. Sicher werfen alle politischen Organisationen Geld in die (Werbe-)Waagschale, um ein bestimmtes Resultat zu erreichen. Beweise, dass der Erfolg der Resultate proportional zum aufgewendeten Geld ist, konnten nie wirklich erbracht werden. Die nationale Rechte selbst fürchtet mehr die ausländische Einflussnahme auf die Politik durch den Druck der Anpassung an die internationalen Standards und die Anbiederung an die

grossen Märkte und deren Prämissen. (Die Liberalen hingegen fürchten meist nur die Einschränkungen des freien Marktes.)

Wenn jetzt noch zusätzlich Befürchtungen dazu kommen, dass Abstimmungsresultate mit Geld direkt gekauft sind, so hat diese Kritik aber plötzlich eine ganz andere Grundlage[10]. Wie wird sich wohl die politische Debatte in der Schweiz entwickeln? Wird sich das wirklich, wie von den E-Voting-Befürwortern behauptet, positiv auf die Begeisterung der Jungen für die Politik auswirken? Das Gegenteil wird der Fall sein! Die Anzahl der Leute, die das Cyberrisiko erkennen, wird zunehmen. Sie werden warnen, aber keine Möglichkeit haben, solche Vorkommnisse in einer Menge zu beweisen, welche es bräuchte, um die Wahlmanipulation zweifelsfrei zu belegen. Wir haben uns ein Ei gelegt mit einem System, das die Manipulation ermöglicht, aber nie nachweisen lässt! Und nachdem das E-Voting mal eingeführt ist, wie soll man es wieder abschaffen können? Mit E-Voting? In welche Richtung würde da wohl eine Manipulation stattfinden?

Es wird die Zeit anbrechen, wo die öffentliche Wahrheit mit dem Wissen der Leute auseinanderklafft. Offiziell wird behauptet werden, es sei alles in Ordnung, denn etwas Gegenteiliges ist nie bewiesen worden. Die Leute wissen aber, dass es wohl nicht so ist, aber sie können nichts mehr dagegen tun. Kennen wir solche Verhältnisse nicht aus der Zeit des kalten Krieges aus dem Ostblock?

Vielleicht werden wir dereinst über ein Verbot (natürlich mit E-Voting) abstimmen, dass Abstimmungsresultate nicht mehr angezweifelt und kritisiert werden dürfen, und das natürlich rein aus Gründen des politischen Friedens… Und was glauben Sie, liebe(r) Leser(in), welches Resultat wird da herauskommen?

Die Zeit der alternativen Fakten ist bereits angebrochen, sie wird in eine Zeit der alternativen Welten führen, wo die Leute eine politische Auseinandersetzung scheuen. Wollen wir das?

3.3 Der Wirtschaftsstandort

Werden die politischen Verhältnisse stabil bleiben, wenn künftig nicht nur ein paar Verrückte erzählen, dass die Demokratie in der Schweiz ja gar nicht funktioniert, sondern wenn immer mehr Leute wissen, dass es zwar durchaus so sein könnte, ein Beweis dafür aber unmöglich ist? Was wird die Reaktion des Staates sein, und was die Reaktion der Bevölkerung und der Wirtschaft?

3.4 Das endlose Finanzloch

Man wird – wie bei allen IT Systemen - an dem E-Voting System immer wieder etwas finden, was es zu verbessern gilt. Die Betriebskosten werden deutlich steigen. Eine Service Stelle für alle, die ein Problem haben, wird notwendig sein. Viele werden behaupten, dass ihr Computer nicht richtig funktioniert oder falsch abgestimmt hat. Man müsste jedem einzelnen Fall nachgehen, auch wenn die gemeldeten Fälle nur einen Bruchteil der effektiven sind und davon sicher auch einige falsch. Man wird es zwar nie wirklich können, aber so tun, als ob man alles unternehmen würde, um die Technik sicher zu machen. Das wird endlos Geld verschlingen, ohne dass messbare oder relevante Resultate vorliegen.

[10] Stalin: „Nicht der wer abstimmt bestimmt das Ergebnis, sondern wer auszählt“

Auch der Schweizer Stimmbürger in der argentinischen Pampa hat ein Anrecht auf die Überprüfung der korrekten Auszählung. Wer bezahlt diesen Aufwand? Wird irgendeinmal eine Verordnung kommen, dass jeder Stimmbürger selber verantwortlich ist über seine Anlage und deren Betriebskosten selbst zu berappen hat?

3.5 Bedeutet die Globalisierung die Abschaffung des eigenen Rechtsraumes?

Oder wird es eines Tages gar keine Rolle mehr spielen, ob die Abstimmungen integer sind oder manipuliert, weil es sowieso nichts Wichtiges mehr abzustimmen gibt? Alles Wichtige wird durch internationale Standards und supranationale Organisationen festgelegt und wir müssen überall dabei sein, weil sonst der Markt beschnitten wird?

Mit der zunehmenden Diskreditierung des politischen Prozesses in der Schweiz laufen wir Gefahr, dass wir auch dort nichts mehr diesem Trend entgegensetzen werden, wo es nach wie vor möglich und nötig wäre.

4 Die Ursachen für den mangelnden Protest

Warum nur protestieren nicht mehr Bürger gegen diesen gesellschaftlichen Wahnsinn, der quasi einem nationalen politischen Selbstmord auf Raten gleichkommt?

4.1 Der Bauch und der Kopf

Jeder Mensch hat eigene Erfahrungen. Entweder hat er sie verarbeitet und im Kopf abgelegt. Oder er hat sie gemacht aber noch nicht rational verarbeitet. Dann sind sie im Bauch gespeichert und ergeben ein „Bauchgefühl“. Eine gesellschaftliche Manipulation wie die über E-Voting ist in der Regel nicht Teil einer selbstgemachten Erfahrung. Man hat gehört von Fällen, hält diese aber entweder für Einzelfälle, oder sie sind umstritten und von der jeweiligen subjektiven Optik abhängig oder man hält allenfalls die Berichte darüber für übertrieben. Jedenfalls ist das kein Grund, sein gutgläubiges Weltbild abzuändern. Vielfach gilt das Motto: *Was nicht sein darf, kann auch nicht sein.*

Nur wenn Bauch und Kopf in die gleiche Richtung zeigen, ergibt sich ein eindeutiges Bild zur Meinungsbildung.

4.2 Das Vertrauen in die Behörden

Das Vertrauen in die Behörden ist grundsätzlich sehr gross und wenn eine ehemalige oder amtierende Bundesrätin eine Empfehlung abgibt, so wiegt diese tonnenschwer auf der Entscheidung des Normalbürgers. Über das Abstimmungsbüchlein der Bundeskanzlei ist schon berichtet worden: Weil es methodisch so hervorragend gemacht ist, werden auch die inhaltlichen Aussagen kaum angezweifelt.

Folgende Aussagen der Bundeskanzlei unterstützen die Bereitschaft zur Akzeptanz bei E-Voting:

Argument BK	Kommentar/Antwort
Wir machen nur kleine Schritte. Unser Motto ist „Sicherheit vor Tempo“, Wir haben Vernehmlassungen durchgeführt.	Ja, das Projekt wird bei der Einführung in die Länge gezogen, ohne dass aber die grössten sicherheitstechnischen Mängel angegangen worden sind. Vernehmlassungen gab es nur bei Interessensgruppen, also Befürwortern.
Bis jetzt ist noch nichts passiert, die Versuche waren alle erfolgreich	1. Die BK (bzw. die Kantone) hat einfach nichts gemerkt 2. Die BK (bzw. die Kantone) würde auch nie etwas merken

	können 3. In der Testphase 2016 waren nur ca. 2% der Stimmbürger E-votingmässig angebunden. Das stellt keine Plattform für eine erfolgreiche Manipulation dar. Deshalb ist eine solche Aussage ohne Wert.
Für den vollen Ausbau bauen wir auf die Verifizierbarkeit. D.h. Jeder Stimmbürger kann feststellen, ob seine Stimme richtig angekommen ist. Das muss genügen, denn eine absolute Sicherheit gibt es nicht in der IT.	1. Der technische Berater Prof. Hänni FH BE hat zu Recht das Erreichen der Verifizierbarkeit „kurz- und mittelfristig“ abgesprochen[11]. S. auch 2.7.6. 2. 30% des Elektorates dürfen auch ohne Verifizierbarkeit schon eingebunden werden. Das stellt aber bereits eine wesentliche Bedrohung für die Manipulierbarkeit dar.

Man kann sich einfach nicht vorstellen, dass der Bundesrat nicht die beste aller Informationen zur Meinungsbildung zur Verfügung hat und diese auch berücksichtigt. Man weiss oft eben auch nicht, dass Ämter sich misstrauen und manchmal ignorieren. Die Bundeskanzlei hat auch nicht einmal die notwendigen Ressourcen für ein IT Grossprojekt. BIT, ISB und FUB haben weitaus grössere Kapazitäten, aber selbst da sind schon IT- Projekte aus dem Ruder gelaufen.

4.3 Die Komplexität und die Ignoranz

Wenn Frau Merkel das Internet im Jahre 2013 als „Neuland“ bezeichnet hat, so ist abzuschätzen, welchen Stand des Wissens über IT Problematiken bei Behördenvertretern vorhanden ist. Diese sind also vollständig von hochkarätigen Vertretern der Wissenschaft bzw. Wirtschaft abhängig. Aber welche Interessen vertreten diese und verstehen jene sie denn auch richtig?

Das E-Voting selbst ist schon durch die ausgeklügelte Sicherheitstechnik auf Applikationsebene ausserordentlich komplex. Die Komplexität einer Manipulation scheint auf den ersten Blick noch viel komplexer und deshalb ausserhalb unseres Vorstellungsvermögens. Deshalb kann auch das Risiko nicht richtig beurteilt werden. Übersehen wird dabei aber, dass es genügt, die schwächsten Glieder der Sicherheit zu analysieren, um das Risiko zu beurteilen. Diese sind in diesem Dokument ausführlich genannt worden.

4.4 Die Freude am Neuen und die unerschütterliche Technikgläubigkeit

Wer möchte schon gegen den Strom schwimmen? Die Trendsetter setzen den Trend und sie haben immer Recht. Viele Leute finden das Neue immer besser als das Alte, vielleicht wenn es ihnen nicht so gut geht oder wenn sie am Anfang des Lebens stehen. Der enorme Einfluss, den die modernen Technologien ins Leben von jedermann gebracht haben, führt zu einer Abhängigkeit davon und oft richtet man auch sein Wertesystem danach aus. Natürlich ist unbestritten, dass diese Errungenschaften auch enorme Fortschritte ins Leben von jedermann gebracht haben.

Erst mit einer gewissen Reife erkennt man aber auch Risiken, die nur als abstraktes Konstrukt beschrieben sind und deren Folgen kaum direkt selbst erlebbar sind.

4.5 Die buhlenden Interessensvertreter

Auslandschweizer werden nicht müde, ihren Ansprüchen an ihrer Beteiligung zur politischen Willensbildung in der Schweiz Nachdruck zu verleihen. Weil die Post im Ausland nicht überall schnell genug ist, dass man rechtzeitig sich informieren, abstimmen und das Couvert zurückschicken kann, muss unbedingt das E-Voting her.

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

IT Vertreter können sich allenfalls lukrative Aufträge versprechen für Lieferung, Inbetriebnahme, Einsatz, Betrieb und Service einer solchen Anlage. Sie werden alles dafür tun, ihre Kompetenz auch in IT Sicherheit unter Beweis zu stellen und möglicherweise immer wieder versuchen, mit neuen Ideen zur partiellen Verbesserung von Teilproblematiken beizutragen.

All diesen Leuten kann nicht vorgeworfen werden, dass sie ihre eigenen Interessen vor diejenigen der Gesellschaft als Ganzes stellen. Von Behördenvertretern erwarte ich allerdings eine dezidiert entgegengesetzte Haltung.

4.6 Das fehlende Sicherheitsbewusstsein

Wenn man vor kriminellen Machenschaften warnt, so gibt es beim Normalbürger oft einen Reflex:
Dafür haben wir Polizei und Justiz! Damit müssen wir uns nicht in der Politik beschäftigen.

Man vergisst dabei aber, dass diese Instanzen ganz schlechte Karten haben, wenn es sich um organisierte Kriminalität handelt, noch schlechtere, wenn sich der grösste Teil dabei auf ausländischem Territorium abspielt. Sie haben gute Karten beim Erwischen der Parksünder und der Tempoübertreter, denn sie dürfen Parkplätze und Strassen einschränkungslos überwachen. Computer dürfen sie nicht überwachen, oder nur, wenn schon etwas Handfestes passiert ist. Aber wie kann man etwas feststellen, wenn wegen des Datenschutzes gar nicht „vorgängig“ überwacht werden darf? Im Kap. „Begünstigende Faktoren“ (des Risikos) sind die Erschwernisse für Polizei und Justiz beschrieben.

Zu glauben, dass Manipulationen an den Computern der Stimmbürger festgestellt werden könnten, wäre auch dann eine Illusion, wenn es diese Datenschutzbestimmungen nicht gäbe. IT Sicherheit zu Hause als Prävention zu fordern in dieser Situation ist zwar auch eine schöne Idee, hat aber ebenfalls keine Chance, da mit vernünftigem Aufwand nicht überprüfbar und allenfalls eben dem Datenschutz widersprechend.

4.7 Welche Gruppen von Leuten unterstützen E-Voting?

Ich möchte abschliessend zusammenfassend folgende Kategorien von Leuten unterscheiden, die das Projekt E-Voting unterstützen und jeweils mit einer eigenen Argumentation auftreten:

<table>
<tr><th>Gruppe</th><th>Deren Argumente</th><th>Gegenargumente</th></tr>
<tr><td rowspan="5">Internet-Ignoranten, Gutgläubige, Obrigkeitsgläubige, Technikgläubige</td><td>Was ist das, Cyberangriff?</td><td rowspan="5">Die Technologie des Cyberangriffs hat genauso Fortschritte erzielt wie die IT selbst. Der Kriminelle ist am längeren Hebel, er beachtet keine Regeln im Gegensatz zu unserem eigenen Staat.
Der Nachrichtendienst der Schweiz sieht in der Cyberbedrohung eine der dominanten Gefahren für die Schweiz. Die direkte Einflussnahme in Volksentscheide ist die effizienteste Manipulationsart.

Sicherheit ist nicht nur eine Technologiefrage. Der Mensch und das ganze Umfeld gehören dazu. Flexibilität und Bequemlichkeit widersprechen der Sicherheit im Kern.</td></tr>
<tr><td>Da ist bis heute nichts passiert, wieso soll da in Zukunft etwas passieren? Nicht einmal in Amerika konnte man einen Hackerangriff auf die Auszählung der Präsidentschaftswahlen 2016 nachweisen</td></tr>
<tr><td>Cyberangriffe sind nur ein theoretisches Risiko. Das wäre viel zu kompliziert und aufwendig. Man kann die Leute auch anders manipulieren.</td></tr>
<tr><td>Die Behörden werden schon schauen, dass das Zeug sicher ist.</td></tr>
<tr><td>Die IT Sicherheit wird immer besser. Im Moment gibt es zwar noch Probleme, aber die werden bald gelöst sein.</td></tr>
<tr><td>Beamte und Effizienzoptimierer</td><td>In Vernehmlassungen können interessierte Kreise Stellung nehmen
Lange Testphasen garantieren die Ausmerzung von Fehlern</td><td>Der unerschütterliche Glaube an die perfekte Methodik des Staatsapparates verbaut die Sicht auf gesamtgesellschaftliche Zusammenhänge bei der Bewertung von Risiken.</td></tr>
</table>

	Wir haben eine Verordnung, die das E-Voting steuert. Wir müssen die Verordnung befolgen und nicht sie in Zweifel ziehen. Es gibt einen politischen Weg, das zu bekämpfen, wenn man will. Ich bin nicht zuständig für die gesamtgesellschaftliche Beurteilung	Politische Entscheidungen werden in der Tat nicht vom Beamten, sondern auf der übergeordneten Ebene getroffen. Es fehlt aber oft am Verantwortungsbewusstsein der leitenden Beamten. Sie stellen ihre Meinung zurück hinter ihre Pflicht. Die Verbesserung der Effizienz scheint für sie das dominante Problem, das ihre Pflicht berührt.
	Endlich können wir das Ergebnis der Abstimmungen schnell und mit wenig Aufwand erbringen!	
Normalbürger und Technikfreaks als Profiteure	Auslandschweizer: Endlich können wir auch abstimmen! Das bisschen Risiko nehmen wir in Kauf! Generation Handy: Endlich schaut man auch einmal für uns! Vielleicht interessieren wir uns ja dann mehr für Politik.	Der Blick auf das eigene Wohl versperrt den Blick auf gesamtgesellschaftliche Zusammenhänge.
	IT Lieferanten: Das ist eine hochinteressante Technik. Wir hätten da noch so ein paar Ideen, welche Lösungen man da noch dazu verkaufen könnte…	
Utopisten und Progressive	Ihr seid einfach immer gegen das Neue: Hinterwäldler und Rückwärtsgerichtete! Gebt doch der Zukunft eine Chance!	Der unerschütterliche Glaube an das Neue versperrt die Sicht auf die enormen Risiken, die damit eingegangen werden. Man kann nicht alles einfach einmal ausprobieren und dann schauen wie es geht. E-Voting wird nie wieder wegzukriegen sein!
Elitaristen, „Weltbürger“	Das Volk kann komplizierte politische Vorlagen eh nicht richtig beurteilen. Wir sind für eine weltweite Standardisierung des Rechts. Da gibt es sowieso keinen Platz mehr für nationale Alleingänge. E-Voting ist deshalb gar kein Thema für uns.	Noch gilt die direkte Demokratie! Wenn so eine Weltordnung da wäre, müsste man die Demokratie abschaffen und nicht E-Voting einführen!
Fatalisten	Die Abstimmungen werden ja sowieso manipuliert durch Geld und Medien. Wenn jetzt auch noch durch Cyberkriminalität, so ist nicht viel mehr verloren.	Diese Haltung entbehrt der Wesentlichkeit bei Faktenlage. Zwar können Meinungen manipuliert werden, aber bisher ist die Auszählung der Meinungen wenigstens integer!

Nicht aufgeführt sind hier die potentiellen Nutzer der cyberkriminellen Machenschaften, denn sie selbst stellen wohl nur eine winzige Minderheit dar.

5 Fazit

Man hat den Eindruck, dass die Bundeskanzlei seit 2000 versucht, sich mit dieser Innovation in jahrelangen Testphasen ein Denkmal zu setzen. Zwar wird das verzögerte Tempo immer wieder auf die noch ungelösten Sicherheitsprobleme zurückgeführt, gleichzeitig ist aber der Bundesrat erfolgreich ermuntert worden, ein klares Bekenntnis zu E-Voting abzugeben.

Offenbar ist sich der Bundesrat trotz der vielen spektakulären Fälle von Cyberattacken, trotz der Enthüllungen von Edward Snowden immer noch nicht genügend bewusst, welche Risiken mit IT Systemen am Internet generell verbunden sind. Er glaubt vielleicht, dass wir in der Schweiz schon sicherere Systeme bauen als in der übrigen Welt. Oder er teilt den vielerorts verbreiteten Glauben, dass der Fortschritt der Technologien generell immer mehr Sicherheit bringen würde. Leider bestätigt die Gegenwart, dass dem nicht so ist. Die weltweite Kriminalität und die Machtpolitik der Grossmächte zeigen genau in die umgekehrte Richtung: Nur kleine Hacker werden immer mehr behindert, die grossen werden immer mächtiger.

Die Applikation „E-Voting" ist zwar wohl schon nach den letzten Erkenntnissen der IT Sicherheit gebaut. Die grösste Schwachstelle ist und bleibt aber der Computer des/(-r) Stimmbürgers/(-in) und sein Betriebssystem, über welche keine wichtigen Vorgaben verlangt und überprüft werden können, u.a. wegen des Datenschutzes. Der manipulierte Computer aber wird auch den User manipulieren! Wer folgt nicht den Anweisungen des Computers sondern denjenigen des Anleitungsbüchleins? Das verbleibende Risiko ist zwar nachweislich auch der Bundeskanzlei bekannt, durch den politischen Prozess wird aber die Verantwortung für die Folgen nicht dort wahrgenommen, sondern breit verteilt: Auf das Parlament, welches das Gesetz ja annehmen muss, auf die Kantone, die für den Einsatz des System und somit für die Korrektheit der Auszählungen ja zuständig sind, auf die Stimmbürger(-innen) selbst, die ja selbst schuld sind, wenn ihr Computer eine falsche Stimme erstellt und sie das nicht merken. Denn alles hängt konzeptgemäss an der sog. *Verifizierbarkeit,* d.h. an der Möglichkeit, dass der/die Stimmbürger/-in zweifelsfrei feststellen kann, ob die Stimme so abgegeben wurde, wie er wollte. Es wird nicht verlangt, dass er es tut, sondern nur, dass er es könnte. Man vergisst, dass wir alle davon abhängen, dass alle Stimmenden richtig gezählt werden und nicht nur jeweils die eigene.

Dieses Vorhaben ist für die Schweiz äusserst gefährlich: Wir steuern mit E-Voting der schleichenden Abschaffung der direkten Demokratie entgegen, dadurch dem Ende der stabilen politischen Ordnung, dadurch möglicherweise auch des erfolgreichen Wirtschaftsstandortes. Ich appelliere an die demokratische Verantwortung aller und rufe hiermit auf, diesem unseligen Vorhaben ein Ende zu bereiten!

6 Der Aufruf

Es hilft alles nichts: Wenn das Parlament nicht in der Lage sein sollte, ein Gesetz für die Einführung von E-Voting hochkantig abzuschmettern, so müssen wir als Stimmbürger uns wehren, bevor dieses Unding eine gefährliche Verbreitung erreicht hat. Wir brauchen ein Verbot für E-Voting, genauso wie es das Deutsche Verfassungsgericht beschlossen hat. (Deutschland ist ja auch nicht dafür bekannt, dass es keinen technologischen Fortschritt anstrebt)

- **Lehnen Sie dieses Gesetz beim Referendum ab!**
- **Wir wollen die direkte Demokratie behalten!**
- **Die Kantone behalten die Hoheit über die Auszählung der Stimmen!**
- **Die Stimmauszählung muss nachprüfbar bleiben!**
- **Wir haben genug von teuren, nicht durchdachten IT- Projekten beim Bund!**

Zum Autor:

Dipl. El.-Ing. ETH René Droz, 64, leitete 10 Jahre lang das militärische Computer Emergency Response Team in der Führungsunterstützung im VBS. Er verfügt über 28 weitere Jahre Berufserfahrung in Industrie und Verwaltung in den Bereichen Netzwerktechnik und IT Sicherheit.
Er ist heute pensioniert und setzt sich ehrenamtlich für politische Anliegen, die sein Fachgebiet betreffen, ein.