Vernehmlassungsantwort

Anhang : Ausführliche Antwort 2.1 (E-Voting Bewilligung)

Zusammenfassender Kommentar

I.*Der Bundesrat regelt die Anforderungen an die Systeme für die elektronische Stimmabgabe und deren Betrieb*. Im Prinzip nichts gegen den Satz einzuwenden, aber die Erfahrung bei Cyberdedrohungen zeigt, dass solche einmal definierten Anforderungen bei weitem nicht den realen Bedrohungen auf Dauer genügen. Zertifizierungen der bisherigen Art sind wertlos, da sie nicht den höchsten Ansprüchen entsprechen, die es für die elektronische Stimmabgabe benötigte. An die Heimgeräte der Benutzer und das Internet im Allgemeinen werden gar keine Anforderungen gestellt, wohl weil eine Umsetzung davon juristisch und technisch schwierig wäre und die Kostenfolgen jemand zu tragen hätte. Die Sicherheit muss aber immer ganzheitlich konzipiert, realisiert, geprüft und permanent überwacht werden, denn das schwächste Glied bestimmt im Wesentlichen die Sicherheit. Den dafür notwendigen Aufwänden wird nirgendwo effektiv Rechnung getragen und es darf deshalb bezweifelt werden, dass sie geleistet werden würden. Der Bund, der als einziger dies könnte, hat sich schon vorsorglich aus diese Pflicht entlassen.(Erl. Pkt. 1.4)

Die Kantone kriegen (lediglich) die Auflage, *die erforderlichen Bestimmungen zu erlassen, damit die Sicherheit gewährleistet wird*. Sie sind dazu nicht in der Lage, denn es wird Unmögliches („nicht praktikabel") verlangt. Interessant ist dies im Zusammenhang damit, dass die Zertifizierungen für die Auswertungs-Systeme, die der Bund ausgibt, allein eben offenbar doch nicht zu genügen scheinen, denn das nicht vernachlässigbare Restrisiko gegen den Missbrauch müssen die Kantone mit Vorschriften abdecken. Falls es solche gäbe, müsste die Einhaltung derselben aber rigoros überprüft werden, was enorme Aufwände für die Kantone bedeutete. Der Bund lässt hier Spielraum: Wenn sie das nicht tun oder wenn es keine oder zu wenige Kontrollen gibt, geht es auf Kosten der Sicherheit. Dann stellt sich die Frage, wer trägt die Verantwortung für zu spät oder gar nicht aufgedeckte Missbrauchsfälle. Die Geschädigte ist die Gesellschaft als Ganzes. Das Vertrauen, das sie den Institutionen entgegenbringt darf nicht aufs Spiel gesetzt werden.

II. Das Gesetz müsste unbedingt dem obligatorischen Referendum unterstellt werden, denn es betrifft eine derart einschneidende Änderung der politischen Rechte und Verantwortungen, dass es eigentlich verfassungsrelevant[1] ist.

[1] Aufsatz „Über die Verantwortung, wenn etwas schiefläuft"
https://www.noevoting.ch/public/downloadable/Verantwortung_1.2.pdf

---

Das neue Gesetz mit dem neuen elektronischen Stimmkanal bietet offenbar Raum für eine E-Voting Lösung, wie sie heute zur Verfügung steht. Es ist deshalb abzulehnen und zwar im Einzelnen aus folgenden 5 Gründen:

1. Die Gesetzesänderung stellt eine demokratiefeindliche Erneuerung dar.

1a. Eine elektronische Erstellung und Auszählung von Stimmen ohne die Möglichkeit einer Nachzählung der Gesamtheit aller willentlich abgegebenen JA- und NEIN-Stimmen durch den Stimmbürger stellt für diesen - und das ist neu- einen intransparenten und daher nicht vertrauenswürdigen Prozess dar und widerspricht so den Anforderungen der Demokratie aus den Menschenrechten.

1b. Individuelle Verifizierbarkeit im Sinne der heutigen Implementation als Sicherung gegen Manipulation ist nicht demokratietauglich, weil sie unrealistische, zu hohe Ansprüche an den Einzelnen stellt. Es kann von diesem nicht erwartet werden, dass er erkennt, ob sein Gerät manipuliert wird. Und selbst wenn, kann er es nicht beweisen und keinen zählbaren Beitrag an die öffentliche Aufklärung liefern.

2. Privatisierung von hoheitlichen Staatsaufgaben wie Volksabstimmungen und Wahlen sind nicht zulässig. Auch wenn Kantone formell zuständig bleiben, verlieren sie die für die Sicherheit nötige technische Kompetenz an den Hersteller.

2a. Die Sicherstellung der Demokratie wird hiermit an Private und gar an ausländische Einflussnehmer (Scytl) ausgelagert werden. Ein privater Anbieter E-Voting kann die Sicherheit alleine nicht gewährleisten und eine hoheitliche Kontrolle bedingte viel mehr technische Kompetenz und Aufwand bei Bund und Kantonen als heute Ressourcen vorhanden.

2b. Der einzige Anbieter einer solchen E-Voting Anlage (Schweizerische POST) bietet keine Gewähr für Vergleichbarkeit und Plausibilisierung von Resultaten.

3. Das Gesetz verhindert nicht, dass es an Sicherheitsvorkehrungen gegen eine Manipulation des Ergebnisses und gegen den Bruch des Abstimmungsgeheimnisses mangelt. Es sind für die Öffentlichkeit keine geeigneten konkreten Kriterien sichtbar.

3a. Personenabhängige individuelle Verifizierbarkeit ist kein genügendes Cyberabwehr Dispositiv. Die sog. „universelle Verifizierbarkeit" der Schweizerischen POST erfüllt die Anforderungen dieses Begriffes nicht, sondern höchstens das ungenügende Regulativ der Bundeskanzlei mit dem Neu-Begriff "vollständige Verifizierbarkeit".

3b. Mit der ungesicherten Internet Infrastruktur des Stimmbürgers ist das Abstimmgeheimnis nicht zu wahren. Dieser kann nicht zuverlässig erkennen, ob er durch einen Schadcode Datenabfluss erleidet.

3c. Keine Planung ist möglich für Sicherheitskosten in der Zukunft. Eine für E-Voting notwendige permanente Sicherung der sich dynamisch ändernden Internet-Infrastruktur zentral, bei den Kantonen und lokal beim Benutzer würde mit grosser Wahrscheinlichkeit unvorhersehbare und inakzeptable Ressourcen verschlingen. Sie ist hier aber weder gefordert noch vorgesehen.

4. Die Bedarfsabklärungen sind mit falschen Vorzeichen versehen worden.

4a. Ungenügender Bedarf – wichtige Versprechungen als Grundlage für die Bedarfsabklärung für E-Voting sind nicht erfüllbar und widerlegt. Diese Erkenntnisse werden in der öffentlichen Kommunikation unterdrückt. Der Öffentlichkeit werden auch die Risiken nicht aufgezeigt und es wird auf unqualifizierte Umfragen abgestützt.

5. **Gefahr des Vertrauensverlustes selbst ohne fremde Einflussnahme auf die Ermittlung des Volkswillens**

5a. Der Vertrauensverlust in den demokratischen Prozess ist unter den heute gegebenen technischen Voraussetzungen am Internet ausgesprochen leicht möglich, selbst ohne die unter Ziff. 3 beschriebenen effektiven Risiken. Es reicht dafür aus, dass z.B. mit einem Defacement auf der Webseite selbst oder sogar nur auf dem lokalen Gerät des Benutzers der demokratische Prozess der Lächerlichkeit preisgegeben wird.

5b. Es ist mittlerweile durch diverse Beispiele international bekannt, dass Grossmächte, speziell solche mit wenig demokratischer Kultur, immer wieder versuchen, westliche Demokratien zu diskreditieren. Mit dem heutigen E-Voting-Konzept wird es ihnen besonders leicht gemacht.

Erläuterungen zu

1a	Spezifisch verhinderte JA- und NEIN- Stimmen, bei welchen die Manipulation vom Einzelnen nicht erkannt wurde, können nachträglich auf keine Art und Weise nachgezählt werden. Interessant ist, dass bei klassischen Stimmkanälen bis auf jeden Handgriff gesetzlich vorgeschrieben ist, wer was wie zu machen hat, damit alles korrekt abläuft. Bei den elektronischen Mitteln wird die Korrektheit einfach stillschweigend angenommen. In einer unzulässigen, stillschweigenden Beweislastumkehr wird jetzt offenbar verlangt, dass Inkorrektheiten vom Stimmbürger nachgewiesen werden müssten.
1b	Wie wird der Benutzer auf einen Cyber-Angriff reagieren[2]? Diese Abläufe sind zu wenig bedacht worden und deren Auswirkungen auf das politische Klima zu wenig berücksichtigt.
2a	Mit der Auslagerung von elektronischen Systemen - insbesondere in dieser Komplexität - in die Industrie, geht die **Hoheit über das Wissen und die Kompetenz für Betrieb und Weiterentwicklung aus der hoheitlichen Umgebung weg.** Die Sicherheit ist aber angewiesen auf vollständiges Wissen über Konzeption, Funktionalität, Architektur mit all ihren Schwachstellen und Gegenmassnahmen. Die Sicherheit wird jetzt implizit ausschliesslich den Experten der Industrie überlassen. Angesichts der Tatsache, dass selbst diese auf Experten im Ausland - nämlich die vom Hersteller - angewiesen sind, kann die Sicherheit auf gar keine Weise mehr hoheitlich gewährleistet werden. Es reicht nämlich nicht aus, Quellcode zu veröffentlichen. (vgl. Erfahrungen von norwegischen Experten). Zudem ist dies noch gar nicht erfolgt und es gibt nach wie vor keine Gewähr dafür, dass es überhaupt vollständig erfolgt. Erschwerend hinzu kommt, dass selbst wenn der Quellcode vollständig veröffentlicht würde, einem Bürger weder erlaubt ist noch zugemutet werden kann, sicherzustellen, dass dieser Quellcode ohne jede Veränderung auf den realen Abstimmungssystemen als effektives Programm - d.h. unverändert seit der Kontrolle, -und das für alle Zukunft- im Einsatz ist. Namentlich kann eine Manipulation des effektiven Programmes durch einen internen oder externen Angreifer so erfolgen, dass nicht einmal den Administratoren dies auffällt. Damit können wichtige Sicherheitsfunktionen aufgehoben werden bzw. Datenabflüsse erfolgen. Keine demokratisch legitimierte Wahlkommission hat eine Chance, so etwas zu entdecken, auch wenn anwesend bei der Stimmauszählung. Eine lückenlose Überwachung der Druckereien, die die Codes für die Stimmbürger herstellen, um **sicherzustellen, dass solche Codes nicht wie Passwörter von renommierten IT Unternehmen in aller Welt durchs Internet gestohlen** (swisscom, yahoo etc.) **oder durch Korruption von Beteiligten missbraucht werden können, würde ein Vielfaches dessen kosten, was die Kantone als Aufwand dafür vorgesehen haben**. Sie sind weder in der Lage (Ausstattung Sensorik) noch willens (Personalressourcen), einen solchen als unverhältnismässig angesehenen Sicherungsaufwand zu leisten. Es kann daher ohne rigorose Sicherungsmassnahmen vom Stimmbürger kein Vertrauen abverlangt werden, dass alle Stimmeingaben immer von authentischen Stimmbürgern stammen. Die lange Versuchsphase kann lediglich als Argument dafür verwendet werden, dass die zuständigen kantonalen Stellen jetzt Erfahrung mit den administrativen Abläufen besitzen. **Erfahrungen mit Cyberattacken und Sicherheitsproblemen haben sie keine**. Es fehlt an der Sensorik und an praktischen Beispielen. Zu klein war bisher in der Versuchsphase der Anreiz für einen Gegner, einzugreifen, so kann vermutet werden. Gleichzeitig wissen weder Bundeskanzlei noch Staatskanzleien mit Sicherheit, ob Eingriffe bisher erfolgt sind. Bisherige Cyberangriffe - z.B. auf den Rüstungskonzern RUAG - zeigen: raffinierte Angriffe können über Jahre unentdeckt bleiben. Selbst der Ursprung des Angriffs bleibt bei Angriffen staatlicher Akteure nicht selten komplett im Dunkeln.

[2] https://www.noevoting.ch/public/downloadable/arg_d/Szenario%20Manipulation.pdf

2b	Dies widerspricht der Forderung aus der gutgeheissenenen parl. Initiative 18.427. Dort heisst es: "Es müssen mindestens 2 E-Voting Systeme zur Verfügung stehen".
3a	Unstimmige Interpretation des absoluten Begriffes „Verifizierbarkeit" bei E-Voting CH aufgrund ungenügender Vorgaben für deren Umsetzung[3].
3b	Ein Trojaner auf dem System des Benutzers kann ungehindert die noch unverschlüsselte Dateneingabe am E-Voting an irgendeinen Ort der Welt kopieren. Das ist ein alltäglicher Vorgang in der Cyberkriminalität. Der Benutzer hat keine Chance, dies zu verhindern. Der Fall des CCC mit dem CHVote vom 3.11.2018 hat gezeigt, dass es sogar ohne Trojaner geht. Mit irgendwelchen Vorschriften an die Stimmbürger ist da nichts zu machen. Man kann lediglich die Wahrscheinlichkeit etwas reduzieren mit ein paar Vorsichtsmassnahmen. Aber ist damit dem Art. 6.1.b Genüge getan?
3c	Um Sicherheit im ganzen Prozess der Stimmabgabe und Resultatermittlung gewährleisten zu können, müsste man **sämtliche Schwachstellen des Gesamtsystems** unter Kontrolle haben. Davon sind wir mit der heutigen Lösung weit entfernt. Die Abbildung „Systemschwachstellen"[4] zeigt, wo überall durch eine geeignete Kombination von (a) Fehlverhalten von Mensch und Maschine, (b) Inkompetenz, (c) ungenügender Ressourcierung von Ausrüstung und (d) Sicherheitspersonal sowie durch (e) Korruption, mögliche Angreifer via Cyberkriminalität und Social Engineering hochskalierbar Einfluss in die Resultatermittlung nehmen könnten. Um solche Vorgänge lückenlos zu erkennen, müssten an allen diesen Schnittstellen automatisierte UND personelle Überwachungen eingesetzt werden, die sich gegenseitig kontrollieren müssten und dazu auch noch jeweils in der Lage sein, d.h. gleichartige Kompetenzen müssten mehrfach besetzt werden. Das ist heute in der IT ein nirgends praktizierter Ansatz, nicht einmal beim äusserst heiklen Nachrichtendienst, wie der vor einigen Jahren aufgetretene Fall gezeigt hat. Ausserdem müssten Versuche, Stimmen (insbesondere von Nichtwählern) zu kaufen oder zu verkaufen, entdeckt und geahndet werden können. Das ist mit den heutigen Möglichkeiten nahezu ausgeschlossen[5]. Leider verheisst auch die künftige Entwicklung nicht automatisch Gutes. Weil die Möglichkeiten immer komplexer und vielfältiger werden, sind die Angreifer schneller als die Verteidiger, denn sie müssen jeweils nur mit *einer* Methode überlegen sein, während die Verteidiger immer eine grösser werdende Angriffsfläche verteidigen müssen[6]. Der Kt. GE hat mit seiner Aufgabe des CHVote diese These implizit bestätigt. Die gegenüber realen Verhältnissen stark eingeschränkten **Intrusion Tests vom 24.2.19 bis zum 25.3.19** nehmen nur gerade 2 der 10 Schwachstellenbereiche[4] unter die Lupe und sind daher in keiner Weise geeignet, Prognosen über die künftige ganzheitliche betriebliche Sicherheit abzugeben. • Die gefundenen Fehlimplementationen bei der Quellcodeprüfung zeigen auf, dass sowohl der Betreiber POST nicht in der Lage ist, solches zu entdecken als auch den Prüfstellen jegliche nötige Kompetenz dafür fehlt. Zudem darf dieser „Erfolg" als Zufallstreffer gebucht werden, denn ohne das Engagement einer Einzelperson auf einem fremden Kontinent hätte man wohl den Quellcode als sicher eingestuft. • Da jedermann weiss, dass sich Quellcodes immer wieder ändern, müsste man ja, um wenigstens diese Schwachstelle zu sichern, solche Reviews periodisch durchführen. • Die Grundkonzeption dieses Intrusion Tests, basierend auf der Annahme,

[3] https://www.noevoting.ch/public/downloadable/arg_d/Verifizierbarkeit.pdf
[4] https://www.noevoting.ch/file/system
[5] Studie ETH: https://arxiv.org/abs/1903.00449
[6] https://www.noevoting.ch/public/downloadable/Zukunftsaussichten.pdf

	dass mächtige Institutionen der internationalen Cyberkriminalität uns bei der Entdeckung von Schwachstellen helfen würden, ist an Naivität nicht mehr zu überbieten. Die ansonsten bescheidenen Hinweise auf Unregelmässigkeiten legen Zeugnis ab von der Mittelmässigkeit der „Angreifer" und nicht von der Sicherheit des Systems.
4a	Bedarfserhebung mit falschen Versprechungen[7]
5a	Man stelle sich z.B. vor, dass während des Stimmabgabe-Vorgangs auf dem Bildschirm plötzlich das Bild des russischen oder amerikanischen Präsidenten erscheint mit einem passenden Spruch. Das würde blitzartig die Demokratie in eine Showveranstaltung diskreditieren, was u.U. auch von ausländischen Mächten erwünscht oder gesteuert sein kann. Aber selbst übermütige Jugendliche könnten auf eine solche Idee kommen und sie für lustig halten. Für einen solchen Eingriff braucht es relativ wenige Hacker Kompetenzen. Eine Sicherheitslücke auf Ebene des Webservers reicht. Solche Sicherheitslücken können überdies auf dem Schwarzmarkt eingekauft werden - mit Angriffscode dergestalt, dass ohne erhöhte Kenntnisse erfolgreich Angriffe ausgeführt werden können. Überdies können Sicherheitslücken in kriminellen oder staatlichen Kreisen vorliegen, die über Jahre auch in Schwarzmärkten unbekannt sind. Als paradigmatisch gilt der Fall Wannacry, wo eine dem amerikanischen Auslandsgeheimdienst NSA seit fünf Jahren (!) bekannte Sicherheitslücke mit dem Namen „Eternal-Blue" im Zentrum war, die von der NSA durch mutmassliche Inside-Akteure wiederum im Internet geleakt wurde. Dieser Code wurde von unbekannten Angreifern als Herzstück des Wannacry-Virus verbaut und hat sich sodann über Wochen in zahlreichen Firmen (einschliesslich Spitälern) verbreitet und Infrastrukturen lahmgelegt. Geheim gehalten, können solche Sicherheitslücken mitsamt Angriffscode gezielt dafür werden, kritische Infrastrukturen und auch E-Voting-Systeme anzugreifen und entsprechend auch gezielte Defacements auszuführen, die rein darauf bedacht sind, das Vertrauen in das politische System zu zerstören.

[7] https://www.noevoting.ch/public/downloadable/Bedarfserhebung.pdf