E-Voting Thesen [Droz]:

1. **E-Voting ist ein unsinniger Ansatz, denn Abstimmungen und Wahlen sind nicht einfach Verwaltungsakte**, die optimiert werden müssten, es handelt sich hier um die Souveränität des Stimmbürgers. Da ist der kleinste Zweifel an der Authentizität der Vorgänge untolerierbar. E-Voting löst höchstens ein kleines Problem, produziert aber selbst ein viel Grösseres: Das schwindende Vertrauen des Bürgers in die Institution der Demokratie durch Zweifel an der Richtigkeit der Ergebnisse.

2. **Der Cyberkrieg existiert und ist keine Phantasie von Verschwörungstheoretikern**. Es gibt eine weltweite kriminelle Szene, die sich kommerziell ausrichtet und eine politisch-strategische, bei der sich Grossmächte ihre Ambitionen der Einflussnahme sichern. Gegen die besten dieser Akteure gibt es keinen Schutz in einer IT –Umgebung des Mainstreams. (Internet Vrb/ Mainstream Betriebssyteme / Browser). Input und Output untersteht der Kontrolle des allenfalls angegriffenen Betriebssystems oder Browsers.
   Beispiele :
   a) Stuxnet: Amerikaner und Israelis manipulieren die iranische Zentrifugenproduktion erfolgreich mit Cyberaktivitäten. Pikante Details: (1) Die Anlagen waren nicht einmal online am Internet. Die Aktivitäten erfolgten via Logistik von USB-Sticks. (2) Ohne den penetranten politischen Willen der Israelis wäre dieser Vorfall nie an die Öffentlichkeit gelangt.
   b) Wannacry: Hackern aus der kriminellen Szene gelingt es, 200 000 Computer an einem Tag unter Kontrolle zu bringen. Dort ging es um Erpressung, mit diesem Mittel hätte man auch jedes andere Ziel der Bildschirmmanipulation erreicht.
   c) EDA-Fall 2012-2014: Einem fremden Geheimdienst gelingt es, heikle Daten aus dem pol. Dept. abzusaugen und das blieb 2 Jahre unbemerkt und wurde nur per Zufall entdeckt. Die IT der Bundesverwaltung ist also keineswegs besser geschützt als andere im In- oder Ausland.

3. **Die bei der E-Voting Lösung eingesetzte Kryptologie kann** im besten Fall End-zu-End-Datenflüsse, aber **nicht den Input /Output des Computers, nicht dessen Verfügbarkeit und nicht das richtige Verständnis des Benutzers über das richtige Verhalten sichern**.
   - Manipulationen am Bildschirm verführen den Abstimmenden zur frühzeitigen Abgabe des Bestätigungscodes oder zum Verzicht auf die Verifikation, abhängig von seinem Wahlverhalten. Diese Fälle können kaum festgestellt werden. Meldungen darüber treffen nur zufällig ein.
   - Die Abgabe des Bestätigungscodes kann von Schadcodes unterdrückt werden und die Abstimmung so ungültig werden lassen. Der Benutzer könnte es zwar merken (fehlender Finalisierungscode), kriegt aber z.B. eine beschwichtigende Meldung auf dem Bildschirm und ist zufrieden.

4. **Die ganzheitliche Sicherheit in der IT-Zentrale** besteht nicht nur aus der Intelligenz der Applikationslösung, auf die immer wieder aufmerksam gemacht wird von der BK. Die gesamte zentrale IT **müsste** in allen Teilen bezüglich Sicherheit **überprüft werden**. Da diese einem dynamischen Erneuerungsprozess unterliegen muss (weil sonst die Wartungsverträge nicht erfüllt werden können), müsste man eine vollständige Sicherheitsprüfung ***in jedem***

Kanton und vor jeder Abstimmung durchführen. Das brächte **enorme Kosten**. Die Betriebe der Kantone können sich keine solche Cyberabwehr leisten, derer es bedürfte, sind es sich aber dessen nicht bewusst. Zu dieser Sicherheitsüberprüfung gehörten u.a.:

- Schwachstellen Check aller Systeme in der Zentrale.
- Aktualisierungscheck aller Systeme und der E-Voting Softwarepakete in der Zentrale.
- Permanente Zutritts- und Zugangskontrollen und periodische Kontrollprüfungen aller Eingriffe an allen Systemen durch mehrere Köpfe, die sich gegenseitig kontrollieren.

Ausserdem müsste man an einem Ort folgendes tun:

- Source Code –Überprüfung Applikation E-Voting nach jedem Update (4-12 Wochen Arbeit)
- Die Veröffentlichung des Source Codes ist immer nicht erfolgt

5. **Bei Auftreten von Meldungen über Cyberangriffe sind Bund und Kantone sofort überfordert**. Jede Regierungsentscheidung über das weitere Vorgehen wird ***willkürlich***, da man über keine genügend präzisen Erkenntnisse verfügen wird. *Das **Vertrauen*** in die Funktionsfähigkeit der Demokratie kann nur durch eindeutiges, genaues Zählen zustande kommen.
    - Jede Meldung hat sowohl einen Unsicherheitsfaktor als auch eine Dunkelziffer. Die Dunkelziffer ist nicht einmal annähernd abzuschätzen. Eine einzige gerichtstaugliche forensische Untersuchung eines gehackten PCs dauert ca. 1-2 Wochen und ein negatives Resultat könnte auch von einer sorgfältigen Verwischung aller Spuren herrühren.
    - Wird man auf behördlicher Seite zum Schluss kommen, es sind zu wenige Meldungen um das Resultat zu kippen, so ist der Vorwurf der Willkür bereits im Raum wegen der fehlenden Dunkelziffer-Schätzgenauigkeit.
    - Wird man auf behördlicher Seite zu schnell zum Schluss kommen, die Abstimmung ist manipuliert und neu wählen, so ist der Vorwurf der Willkür ebenfalls gegeben, denn es könnte ja davon die unterlegene Seite profitieren.

Erkenntnis:

Die heutige IT ist nicht schützbar, aber die Demokratie hat den Anspruch eines vollständigen Schutzes.

Konsequenzen:

Das heutige E-Voting muss abgeschaltet werden. Über eine Wiedererwägung kann erst nachgedacht werden, wenn die obigen Einwände obsolet sind.