Tesi di Voto Elettroniche [Droz]:

1. **Il voto elettronico è un approccio assurdo, perché il voto e le elezioni non sono semplici atti amministrativi** che devono essere ottimizzati, ma sono la sovranità dell'elettore. Il minimo dubbio sull'autenticità dei processi è intollerabile. Il voto elettronico risolve al massimo un piccolo problema, ma ne produce uno molto più grande: il calo di fiducia dei cittadini nell'istituzione della democrazia a causa dei dubbi sulla correttezza dei risultati.

2. **La guerra cibernetica esiste e non è una fantasia dei teorici della cospirazione**. Esiste una scena criminale globale a orientamento commerciale e una scena politico-strategica in cui le grandi potenze si assicurano l'ambizione di esercitare la propria influenza. Non esiste alcuna protezione contro i migliori di questi soggetti in un ambiente informatico tradizionale. (Internet Vrb/ Sistemi operativi principali / Browser). L'ingresso e l'uscita sono sotto il controllo del sistema operativo o del browser che può essere attaccato.
   Esempi :
   a) Stuxnet: Americani e israeliani manipolano con successo la produzione di centrifughe iraniane con attività cibernetiche. Dettagli speziati: (1) Gli impianti non erano nemmeno online su Internet. Le attività sono state svolte attraverso la logistica delle chiavette USB. (2) Senza la volontà politica penetrante degli israeliani, questo incidente non sarebbe mai stato di dominio pubblico.
   b) Wannacry: Gli hacker della scena criminale riescono a tenere sotto controllo 200.000 computer in un solo giorno. Lì si trattava di ricatto, con questo significa che uno avrebbe raggiunto anche ogni altro obiettivo della manipolazione dello schermo.
   c) Caso DFAE 2012-2014: un servizio di intelligence straniero riesce a estrarre dati sensibili dal servizio polacco, cosa che è rimasta inosservata per due anni ed è stata scoperta solo per caso. L'informatica dell'Amministrazione federale non è quindi più protetta di altre in Svizzera e all'estero.

3. **La crittografia utilizzata nella soluzione di e-voting può al massimo** garantire flussi di dati end-to-end, ma **non l'input/output del computer, né la sua disponibilità né la corretta comprensione del comportamento corretto dell'utente.**
   - Le manipolazioni sullo schermo tentano l'elettore di inviare il codice di conferma in anticipo o di astenersi dalla verifica, a seconda del suo comportamento di voto. Questi casi sono difficilmente individuabili. Appena arrivano i messaggi su di esso.
   - L'invio del codice di conferma può essere soppresso con codici dannosi che invalidano il voto. L'utente poteva notarlo (manca il codice di finalizzazione), ma riceve un messaggio rassicurante sullo schermo ed è soddisfatto**.**

4. **La sicurezza olistica nel centro IT non consiste solo nell'intelligenza della soluzione applicativa,** su cui BK richiama ripetutamente l'attenzione. Tutte le parti dell'IT centrale **dovrebbero** essere controllate per **verificarne la sicurezza**. Poiché questo deve essere sottoposto a un processo di rinnovo dinamico (altrimenti i contratti di manutenzione non possono essere eseguiti), in ***ogni Cantone e prima di ogni votazione*** dovrebbe essere effettuato un controllo di sicurezza completo. Ciò costerebbe **un'enorme quantità di denaro**. Le imprese cantonali non possono permettersi di farlo, ma non sono consapevoli della necessità di una tale difesa informatica. Tale riesame di sicurezza comprendeva, tra l'altro:

- Controllo di vulnerabilità di tutti i sistemi della sede centrale.
- Verifica aggiornata di tutti i sistemi e dei pacchetti software di e-voting della sede centrale.
- Controlli permanenti degli accessi e degli accessi e verifiche periodiche di tutti gli interventi su tutti gli impianti da parte di più responsabili, che si controllano a vicenda.

Inoltre, si dovrebbe fare quanto segue in un unico luogo:

- Votazione elettronica dell'applicazione di controllo del codice sorgente dopo ogni aggiornamento (4-12 settimane di lavoro)
- Il codice sorgente non è sempre stato pubblicato

5. **In caso di segnalazioni di attacchi informatici, la Confederazione e i Cantoni sono immediatamente sopraffatti.** Qualsiasi decisione del governo su come procedere diventerà arbitraria, in quanto non saranno disponibili informazioni sufficientemente precise. La fiducia nel funzionamento della democrazia può nascere solo da un conteggio chiaro e preciso.
   - Ogni messaggio ha un fattore di incertezza e un numero non comunicato. Il numero di casi non comunicati non può nemmeno essere stimato. Un singolo esame forense di un PC hackerato dura circa 1-2 settimane e un risultato negativo potrebbe anche essere dovuto ad un'attenta sfocatura di tutte le tracce.
   - Se si giunge alla conclusione da parte delle autorità che vi sono troppe poche segnalazioni per capovolgere il risultato, l'accusa di arbitrarietà è già in Aula a causa della mancanza di accuratezza nelle stime del numero di casi non segnalati.
   - Se si giunge troppo rapidamente a una conclusione da parte ufficiale, la votazione viene truccata e rieletta, viene anche mossa l'accusa di arbitrarietà, perché la parte perdente potrebbe trarne vantaggio.

Cognizione:

L'informatica di oggi non può essere protetta, ma la democrazia ha diritto a una protezione totale.

Conseguenze:

Il voto elettronico di oggi deve essere disattivato. Un riesame può essere preso in considerazione solo se le obiezioni di cui sopra sono obsolete.