Bern University
of Applied Sciences

E-Voting = NSA-Voting?

Rolf Haenni

BFH-TI Beiratssitzung, 26.11.2013

Inhalt

- Vorgeschichte
- E-Voting an der BFH
- Warum braucht es E-Voting Forschung?
- Aktueller Diskurs
- Reelle Gefahren
- Verifizierbarkeit
- Schlusswort

Vorgeschichte

Vorgeschichte: Forschung

- Seit ca. 1989
- Teilgebiet de angewandten Kryptografie
- Zahlreiche Publikationen
- Internationale Konferenzen und Journals

Vorgeschichte: Praxis

- Seit ca. 2000
  - Wahlmaschinen (Holland, USA, Deutschland, Indien, etc.)
  - Internet-Voting (Estland, Schweiz, Norwegen, etc.)
  - Erfolge und Misserfolge
- Internet-Voting in der Schweiz seit 2002
  - Kanton Genf
  - Kanton Neuenburg
  - Kanton Zürich (heute AG, FR, GR, SG, SH, SO, TG)
  - Koordiniert durch die Schweizerische Bundeskanzlei
- Forschungsresultate kaum umgesetzt

Bern University
of Applied Sciences

E-Voting an der BFH

E-Voting Gruppe

- Research Institute for Security in the Information Society
- Gegründet 2008
- Leitung: Rolf Haenni (seit 2012, vorher Eric Dubuis)
- Mitglieder
  - Professoren: Eric Dubuis, Reto E. Koenig, Stephan Fischli
  - Assistierende: Severin Hauser, Philipp Locher (PhD)
  - Master-Studierende: Philémon von Bergen, Jürg Ritter
- Zahlreiche Publikationen
- 2 abgeschlossene, 1 nicht abgeschlossene Doktorarbeiten
- National und international gut vernetzt

Projekte

- FIDIS (EU FP6, 2004–2009)
- TrustVote (BFH, 2008–2009)
- SwissVote (Hasler-Stiftung, 2009–2012)
- VIVO (SNF, 2012–2014)
- UniVote (verschiedene Studierendenverbände, 2012–2013)
- UniVote 2.0 (Hasler Stiftung, Projektantrag eingereicht)

Veranstaltungen und Highlights

- Swiss E-Voting Workshop 2009, 2010, 2012 (2014)
- E-Voting PhD Days 2010, 2013
- Gründung des Swiss E-Voting Competence Centers 2011
- Meeting “ePower für die Schweiz”, 2011
- Konzeptpapier im Auftrag der Bundeskanzlei, 2012
- Apéro bei der Bundeskanzlerin Corina Casanova, 2012
- Fraktionssitzung der SP Schweiz, 2013
- VoteID 2015 in Bern

Warum braucht es E-Voting Forschung?

Vergleich zu E-Banking

- Verschiedene grundlegende Unterschiede
  - Kein Geheimnis gegenüber Bank
  - Verifizierung durch Kontobelege
  - Auswirkungen von Fehlern/Angriffen auf einzelne Kunden beschränkt
  - Keine Weitergabe an Dritte
- E-Voting ist um mehrere Grössenordnungen komplexer

Vergleich zu Papierwahlen

- Papierwahlen (Urne, Post) sind nicht perfekt
  - Fehler
  - Manipulationen
  - Family Voting
- Geringe Auswirkungen wegen dezentraler Auszählung
- Potentielle Verfälschung tolerierbar

Anforderungen E-Voting

- Korrektheit des Resultats
  - Jede wahlberechtigte Person kann wählen
  - Niemand kann doppelt wählen
  - Alle gültigen Stimmen werden gezählt
- Stimmgeheimnis und Anonymität
- Quittungsfrei (wegen Stimmenverkauf)
- Fairness
- Verfügbarkeit, Robustheit, Usability, Transparenz, Effizienz, Barrierefrei, etc.

Bern University of Applied Sciences

Aktueller Diskurs

Ereignisse der letzten Monate

- Doppelte Stimmabgabe in Genf (2012)
- NSA-Affäre (Sommer, 2013)
- Vortrag von S. Andrivet, Nuit du Hack (Paris, 2013)
- Gerichtsprozess “Richard Hill” in Genf (2012–2013)

Misstrauen gegenüber E-Voting wächst

Für Christoph Blocher zeigt die NSA-Debatte, dass die Risiken beim elektronischen Abstimmen zu gross sind. Mit dieser Ansicht ist er nicht allein. Die Hälfte der staatspolitischen Kommission will einen vorläufigen Stopp.

Iwan Städler

«Es gibt nichts Gefährlicheres in einer Demokratie, als wenn man das Vertrauen in Abstimmungen untergräbt», mahnt Christoph Blocher. Genau dies geschehe nun mit der vom Bundesrat geplanten Einführung des E-Votings. Die NSA-Affäre zeige, wie gefährlich das elektronische Übermitteln und Speichern von Daten sei, kritisiert der SVP-Vizepräsident in einem Interview mit der «Schweiz am Sonntag». Elektronische Abstimmungen könnten manipuliert und das Stimmgeheimnis könnte kaum gewährleistet werden.

Wenn das Virus abstimmt

Nicht nur der 73-jährige Konservative, der mit Computern seine liebe Mühe hat, hegt Bedenken. Auch der 41-jährige Balthasar Glättli, der auf Twitter und Facebook aktiv ist, mahnt zur Vorsicht. Der grüne Nationalrat hat vor einem Monat eine Motion eingereicht, die den Bundesrat zum Stopp der E-Voting-Versuche zwingen will - bis das elektronische Abstimmen sicher ist. Ausnahmen möchte Glättli nur für Auslandschweizer in Ländern mit unzuverlässiger Postzustellung machen. Fast hätte die staatspolitische Kommission sein Anliegen letzte Woche in Form einer Kommissionsmotion übernommen. Laut Glättli fehlte dafür nur eine einzige Stimme. Rund die Hälfte der Kommissionsmitglieder hält die Sicherheitsbedenken also für gravierend. Grund dafür ist nebst der NSA-Affäre auch die Erkenntnis eines Genfer Hackers. Dieser hat im Sommer demonstriert, wie man aus einem Ja ein Nein machen kann, ohne dass es der Stimmende merkt.

Ein Mann rubbelt in Winterthur den E-Voting-Code auf. Foto: Keystone

Der Schwachpunkt beim E-Voting ist der Computer des Stimmbürgers. Er kann mit einem Virus infiziert sein oder beim Abstimmen auf eine falsche Website umgeleitet werden. Das weiss auch der Bund. Es gebe aber keine Hinweise auf tatsächlich erfolgte Manipulationen, relativiert die Bundeskanzlei. Sie hält daher an ihren Ausbauplänen fest und will das E-Voting - nebst der brieflichen Stimmabgabe und dem Gang zur Urne - als «dritten Kanal» etablieren.

Vor allem die Auslandschweizer sollen rasch davon profitieren - ein Grossteil bereits bei den Parlamentswahlen 2015. Später möchte der Bund alle Schweizer Stimmberechtigten vom heimischen Computer aus wählen und abstimmen lassen. Schliesslich soll auch das elektronische Sammeln von Unterschriften für Initiativen und Referenden ermöglicht werden.

Mit der NSA-Affäre sinkt nun aber das Vertrauen in die elektronische Datenübermittlung - auch bei Blochers Parteikollege Lukas Reimann. Für den St. Galler SVP-Nationalrat ist ohnehin klar: «Innerhalb der Schweiz gibt es schlicht keinen Grund für E-Voting.» Auslandschweizern möchte er dagegen die Option offen halten - sobald sie sicher ist.

Reimann hat Glättlis Vorstoss zusammen mit 31 weiteren Nationalrätinnen und Nationalräten unterschrieben. Konkret verlangt die Motion, dass alle E-Voter überprüfen können, ob ihre Stimmabgabe korrekt angekommen ist. Dies ist technisch nicht ganz einfach, da gleichzeitig das Stimmgeheimnis gewahrt bleiben muss. Darüber hinaus wird ein Offenlegen des sogenannten Quellcodes der Programme verlangt. So könnte jedermann das System auf Schwachstellen und allfällige Hintertüren für Geheimdienste überprüfen.

Bevor weitere E-Voting-Versuche stattfänden, müssten diese Bedingungen erfüllt sein, so Glättli. «Ich bin nicht prinzipiell gegen das elektronische Abstimmen, aber die Sicherheit ist mir wichtiger als die Geschwindigkeit», betont der grüne Nationalrat. Denn das Vertrauen in korrekte Wahl- und Abstimmungsresultate sei zentral.

Ist Papier wirklich besser?

«Wer garantiert denn, dass die alte Methode mit den Abstimmungszetteln manipuliersicher ist», kontert CVP-Ständerat Filippo Lombardi, der auch im Vorstand der Auslandschweizer-Organisation sitzt. SP-Vizepräsidentin Jacqueline Fehr hält die Missbrauchsgefahr beim E-Voting ebenfalls für nicht grösser als beim Papier. Die Sensibilität für die Sicherheit sei mit der Geheimdienstdebatte bestimmt nochmals gestiegen. «Aber wir sollten nicht in die Steinzeit zurückkehren und die Projekte abbrechen», so Fehr. Vielmehr müsse man die Sicherheit weiter verbessern.

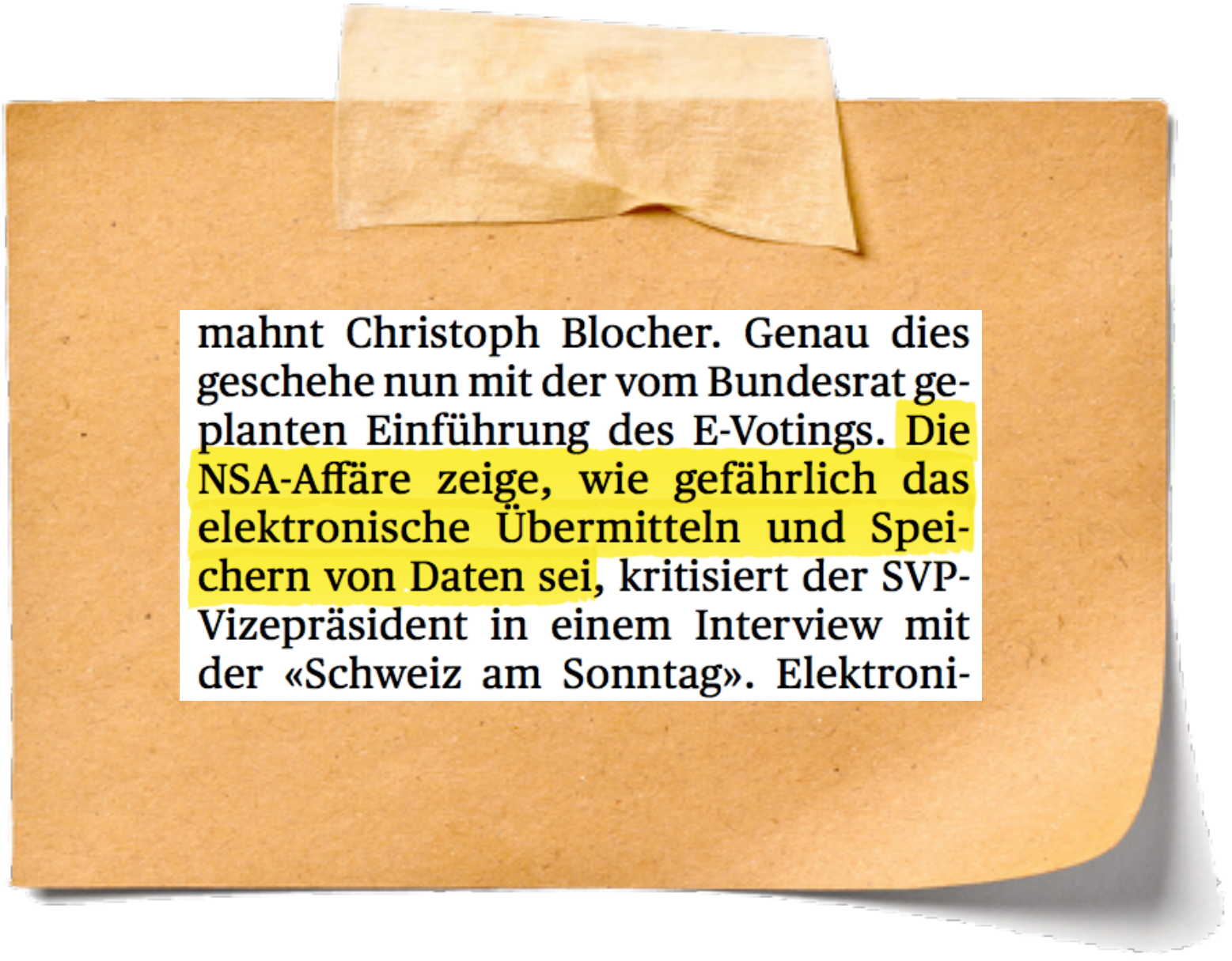
Diesen Weg will auch die Bundeskanzlei beschreiten und auf Systeme setzen, bei denen die Stimmenden verifizieren können, ob ihr Ja wirklich als Ja gezählt worden ist.

NSA-Affäre

Politiker wollen Snowden befragen

Die Schweiz will zusammen mit 21 anderen Ländern in der UNO eine Resolution gegen Internetspionage und Überwachung einbringen. Dies berichtet die «SonntagsZeitung». Gefordert werden Massnahmen gegen die Überwachung von Privatpersonen besonders im Ausland sowie gegen das Eindringen in Datenspeicher, das Persönlichkeitsrechte verletzt. Parlamentarier wollen zudem eine Anhörung des NSA-Whistleblowers Edward Snowden erwirken. «Am besten wäre, die Geheimdienst-Aufsicht GPDel lädt Snowden in die Schweiz ein. Zweitbeste Lösung wäre eine Befragung in Moskau», sagt Daniel Vischer (Grüne, ZH). Auch SVP-Nationalräte unterstützen eine Anhörung Snowdens, während Carlo Sommaruga (SP, GE) Snowden in Moskau besuchen will («Bund» vom Samstag). *(bzr)*

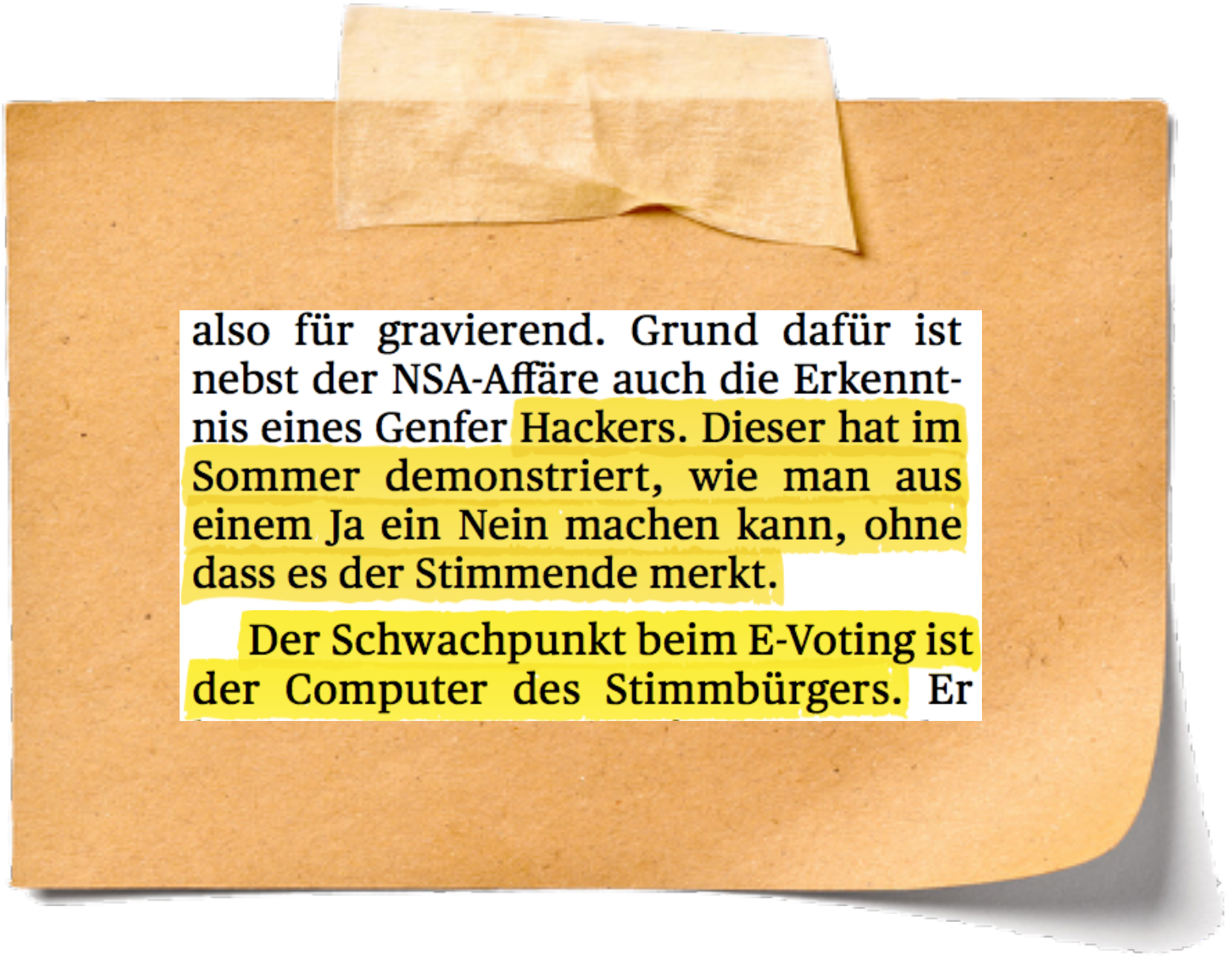
Montag, 4. November 2013 – Der Bund


mahnt Christoph Blocher. Genau dies geschehe nun mit der vom Bundesrat geplanten Einführung des E-Votings. Die NSA-Affäre zeige, wie gefährlich das elektronische Übermitteln und Speichern von Daten sei, kritisiert der SVP-Vizepräsident in einem Interview mit der «Schweiz am Sonntag». Elektroni-

Reelle Gefahren

Was kann die NSA?

- Mobiltelefon-Gespräche und SMS mithören
- E-Mail mitlesen
- Internet-Verkehr überwachen
- Cloud-Daten lesen (Dropbox, Google Drive, iCloud, etc.)
- Erstellen von Benutzer-Profilen


also für gravierend. Grund dafür ist nebst der NSA-Affäre auch die Erkenntnis eines Genfer Hackers. Dieser hat im Sommer demonstriert, wie man aus einem Ja ein Nein machen kann, ohne dass es der Stimmende merkt.
Der Schwachpunkt beim E-Voting ist der Computer des Stimmbürgers. Er

Was kann der Hacker?

- Gezielte Infizierung von Geräten mit Schadprogrammen
- Kontrolle über Geräte übernehmen (unbemerkt)
  - Zugangsdaten missbrauchen
  - JA/NEIN vertauschen
  - Stimme nicht abschicken
  - Stimmgeheimnis verletzen
- Gilt für PCs, Notebooks und Mobiltelefone

Was können die NSA und der Hacker nicht?

- Allgemein: Brechen moderner kryptografischer Verfahren
  - Starke Verschlüsselung brechen
  - Digitale Signaturen fälschen
  - Kryptografische Schlüssel “erraten”
- Speziell: Brechen von kryptografischen Wahl-Protokollen

Verifizierbarkeit

Konkret verlangt die Motion, dass alle E-Voter überprüfen können, ob ihre Stimmabgabe korrekt angekommen ist.

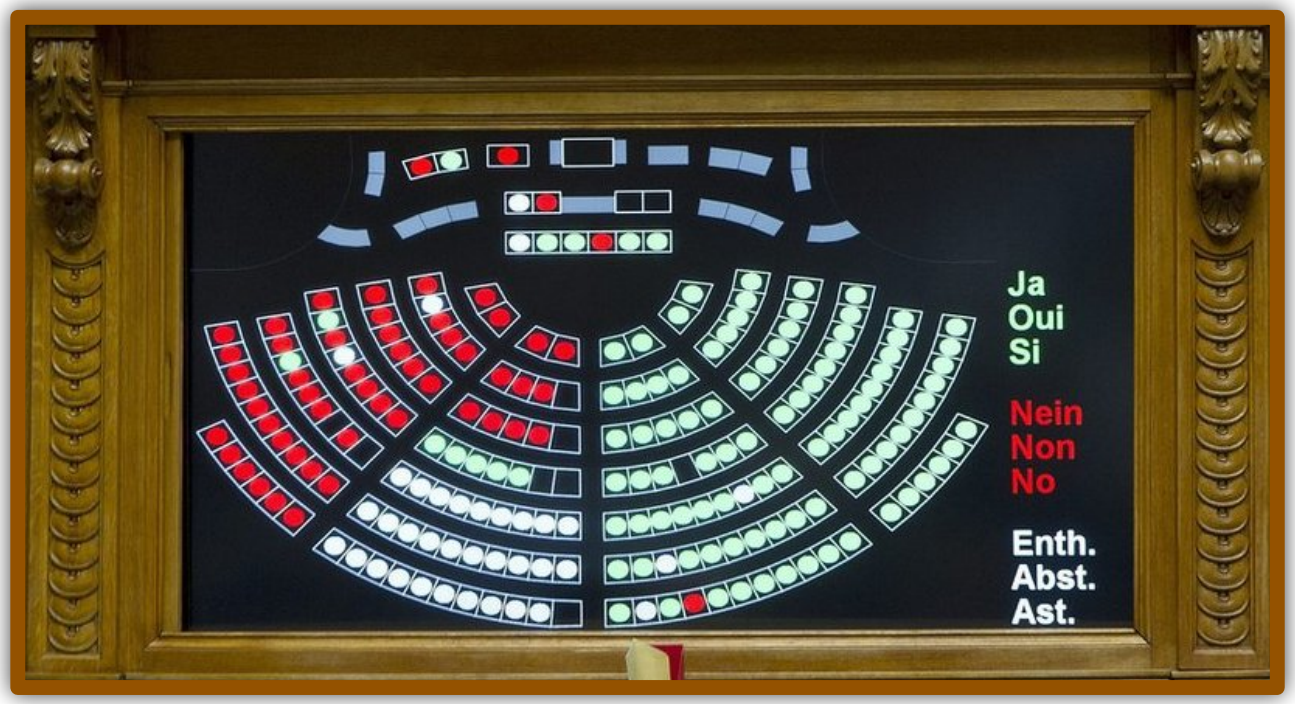
Diesen Weg will auch die Bundeskanzlei beschreiten und auf Systeme setzen, bei denen die Stimmenden verifizieren können, ob ihr Ja wirklich als Ja gezählt worden ist.

Verifizierbarkeit

- Die Wissenschaft fordert verifizierbare Systeme seit 20 Jahren
- Beispiel 1: Norwegisches Internet-Voting System
  - Individueller Bestätigungscode auf Stimmzettel
  - Schadprogramm (Hacker) kann diesen nicht erraten
- Beispiel 2: UniVote (Berner Fachhochschule)
  - Verschlüsselte Wahldaten werden veröffentlicht
  - Öffentlichkeit kann das Wahlergebnis nachzählen

Verifizierbarkeit (Forts.)

- Beispiel 3: Abstimmung im Nationalrat



- Schweizer Systeme der 1. Generation sind nicht verifizierbar

Schlusswort

Unsere Empfehlungen für die Schweiz

- Motto “Sicherheit vor Tempo” beibehalten
- Systeme der 2. Generation
  - Kryptographisches Wahlprotokoll
  - Individuelle Verifizierbarkeit
  - Transparenz
- Systeme der 3. Generation (vollelektronisch)
  - Individuelle und universelle Verifizierbarkeit
  - Vertrauenswürdige Hardware: Wahlkarte, Wahlgerät

Fragen?

http://e-voting.bfh.ch