WorldWideWahl statt Wahllokal?

Welche Begriffe, Ideen, Konzepte der Informatik benötigt der informatische Laie, um das Thema Internetwahl technisch zu durchdringen?

Zusammenfassung In Estland dürfen die Bürger seit 2005 per Internet wählen, in der Schweiz wird die Einführung des Onlinekanals für 2023 angestrebt. Im Zusammenhang mit *remote electronic voting* (REV) stellen sich zahlreiche Fragen. Wir untersuchen, welche Aspekte von E-Voting in der Neuen Zürcher Zeitung sowie im Guardian zwischen 2000 und 2022 behandelt wurden, und arbeiten unter Hinzuziehung von Fachquellen zu REV-Systemen heraus, welche Begriffe, Ideen, Konzepte der Informatik der informatische Laie – wie es Schüler, Bürger, Politiker im Allgemeinen sind – benötigt, um das Thema Internetwahl technisch zu durchdringen. Der Fokus liegt auf den REV-Systemen Estlands und der Schweiz sowie der Gefahr durch trojanische Pferde auf den Rechnern der Wähler. Wir entwickeln Gedanken, die in der Presseberichterstattung Berücksichtigung finden sollten.

Schlüsselwörter Internetwahl, E-Voting, *remote electronic voting* (REV), Onlinewahl, Didaktik der Informatik

Arbeit zur Erlangung des ›B. Sc. Informatik für das Lehramt‹
der Freien Universität Berlin,

eingereicht von Matthias Kuhn
am 5. September 2022,

Erstgutachter: Prof. Dr. Ralf Romeike,
Zweitgutachter: N. N.

Inhaltsverzeichnis

1 Überblick

1.1 Motivation

Seit 2005 (Kommunalwahl) bzw. 2007 (Wahl des Landesparlaments) ist es den Wählern in Estland möglich, ihre Stimme via Internet abzugeben. Betrachtet man die Wahl des Landesparlaments, stieg der Anteil derjenigen in Estland, die ihre Stimme online abgeben, von 5,5 % auf 43,8 % (2019). [1]

Auch das Europäische Parlament dürfen Estlands Bürger auf diese Art wählen. Was heute laut EU-Recht eine Möglichkeit darstellt [2], kann morgen zu einer Richtlinie werden, die sämtliche EU-Mitgliedstaaten verpflichtet, bei nationalen Wahlen ebenfalls diesen Stimmkanal anzubieten, z. B. um Bürgern, die sich im Ausland aufhalten, die Teilnahme an der Wahl zu ermöglichen – auch eine Frage der Freizügigkeit innerhalb der EU [3].

Selbst wenn der Europäische Gerichtshof, sollte sich die Frage stellen, der Auffassung folgte, dass die Entscheidung über das Anbieten des Onlinekanals in der Hand der Nationalstaaten bleibt, würden Internetwahlen ein Thema, sobald westliche Länder dem Vorbild Estlands folgen. Interesse daran ist vorhanden: Im März 2019 waren Offizielle aus mehr als dreißig Ländern in Estland zugegen, um das System in Aktion zu erleben [4], und in einer ganzen Reihe von Ländern wurden bereits Versuche mit Onlinewahlen unternommen, z. B. in Großbritannien, in Norwegen, in der Schweiz.

Die Zunahme des Anteils der Briefwähler bei Bundestagswahlen von 4,9 % 1957 [5] auf 47,3 % 2021 [6] lässt erahnen, dass die Möglichkeit zur Stimmabgabe via Internet von vielen Wählern in Deutschland begrüßt werden würde. Bürger der USA, die im Ausland leben, haben 2020 eine Sammelklage eingereicht, um die Möglichkeit, per Internet an Wahlen teilzunehmen, zu erzwingen. [7]

1.2 Forschungsfragen

Internetwahlen werden auch in anderen Kontexten diskutiert: Leser-/Zuschauerabstimmungen, Hauptversammlungen von Aktiengesellschaften, Urabstimmungen vor Streiks etc. Wir interessieren uns einzig für Abstimmungen, mit denen die Wähler über die Zusammensetzung von Parlamenten entscheiden.

Das Presseecho, das Internetwahlen hervorgerufen haben, erstreckt sich von Begeisterung[1] bis zu scharfer Ablehnung[2]. In diesem Zusammenhang stellt sich die Frage:

F1 Welche Aspekte von Internetwahlen werden in der Presse behandelt? (wir beschränken uns auf Aspekte mit Informatikbezug)

Aus der Sicht der Didaktik der Informatik interessiert uns:

F2 Welche Begriffe, Ideen, Konzepte der Informatik benötigt der informatische Laie – wie es Schüler, Bürger, Politiker im Allgemeinen sind –, um das Thema Internetwahl technisch zu durchdringen?

Von der Beantwortung von Forschungsfrage F2 versprechen wir uns, dass die Bürger die Debatte über Internetwahlen nicht länger als *Schlagabtausch unter IT-Experten* [13] wahrnehmen müssen, und Hinweise darauf, welche Aspekte von Internetwahlen in der Presse bis jetzt unzureichend thematisiert wurden.

1.3 Methodik

Wenn wir von ›der‹ Presse sprechen, müssen wir eingrenzen. Gegenstand dieser Arbeit sind die Artikel zweier renommierter überregionaler Tageszeitungen, und zwar der Neuen Zürcher Zeitung (NZZ) und des Guardian.

Die NZZ empfiehlt sich, weil Internetwahlen in der Schweiz seit langem ein Thema sind – weil dem Schweizer Souverän angesichts der frequenten Abstimmungen, ungefähr vier pro Jahr [14], der direktdemokratische Schuh drückt – und für 2023 eine breitflächige Einführung von Internetwahlen geplant ist, der Guardian wegen der Erfahrungen, die Großbritannien mit Onlinewahlen und die die USA mit Wahlcomputern im Wahllokal gemacht haben.

Wir untersuchen Artikel, die das Stichwort *E-Voting* enthalten – in der NZZ ist das der gängige Terminus, im Guardian ebenfalls – und zwischen Januar 2000 und Mai 2022 erschienen; dies umfasst 343 Artikel der NZZ und 297 des Guardian. Bereinigt um die Artikel, in denen es nicht um Parlamentswahlen geht, blieben 320 und 219 Artikel auszuwerten.

[1] *technischer Quantensprung* [8] – *made the elections the most innovative since 18-year-olds were given the vote in 1969* [9]

[2] *E-Zauberlehrlinge* [10] – *Voting on paper might seem woefully old-fashioned in the 21st century, but one hour in Chaos Communications Congress will leave you very relieved if your country still votes the old way, and very concerned if it doesn't.* [11] – *E-Voting ist nicht nur absolut unnötig, es ist auch brandgefährlich. Ebenso gut könnten wir über die Abschaffung der direkten Demokratie abstimmen.* [12]

Es geht in dieser Arbeit nur am Rande um den Einsatz von Wahlcomputern im Wahllokal, der ebenfalls als *electronic voting* [15] bezeichnet wird. Auch der Einsatz von Stimmzettelscannern, der im weitesten Sinne noch dem E-Voting zugeordnet werden kann,[3] soll hier außen vor bleiben. Um abzugrenzen, übernehmen wir aus der Fachliteratur den Begriff *remote electronic voting* (so z. B. in [16]) und schreiben fortan typografisch ökonomisch REV.

Um Forschungsfrage F1 zu beantworten, unterziehen wir das Presseecho einer qualitativen Inhaltsanalyse nach Mayring [18].

Um Forschungsfrage F2 zu beantworten, arbeiten wir anhand von Zitaten aus den Artikeln Verständnisprobleme heraus und gehen mit Fachquellen zu REV-Systemen in die Tiefe. Wir legen den Schwerpunkt auf das System, das in Estland zum Einsatz kommt, und auf das System, das in der Schweiz zum Einsatz kommen soll. Wo es sinnvoll erscheint, werden Erfahrungen aus anderen Ländern herangezogen.

2 Forschungsfrage F1

In diesem Abschnitt wird die Frage behandelt:

F1 Welche Aspekte von Internetwahlen werden in der Presse behandelt? (wir beschränken uns auf Aspekte mit Informatikbezug)

Zu diesem Zweck unterziehen wir die Artikel der NZZ und des Guardian einer qualitativen Inhaltsanalyse (QIA) nach Mayring [18].

2.1 Kategorien für die QIA

Bei der Motivation und Definition der Kategorien für die QIA lassen wir uns von der Frage leiten: Welche Argumente werden pro REV angeführt und welche kontra?[4] Kodiert wird binär: ob die jeweilige Kategorie in dem Artikel adressiert wird, sei es stichwortartig, sei es dem Sinn nach; ausgewertet wurde durch menschliches Lesen. Die Kategorien sind im Folgenden fett hervorgehoben.

2.1.1 Zum Wesen von Risiken

Risiken lassen sich schwer quantifizieren und damit auch schwer vergleichen. Fragen nach und Aussagen zur Sicherheit eines Systems beziehen sich meist auf das Konzept **›Ein System ist entweder sicher oder nicht‹ (Sicherheit ist absolut)** oder auf das Konzept **›Diese Maßnahme ist sicherer als jene‹ (Sicherheit ist relativ).** Beim Zusammenspiel mehrerer Risiken stellt sich die Frage nach dem Gesamtrisiko, dem Risiko des **schwächsten Glieds**.[5]

2.1.2 Schutzziel Autorisierung

Zu den Grundsätzen von Wahlen in Demokratien gehört, dass der Wähler seine Identität nachweisen muss (Authentifizierung) und damit auch die Tatsache, dass er wählen darf – dass er volljährig ist; in manchen Ländern gelten weitere Voraussetzungen[6] –, und dass alle Wähler das gleiche Stimmengewicht haben, sprich: jeder maximal 1 Stimme abgeben darf, auch bei der Wahl zum Europäischen Parlament; vgl. den Fall des Bürgers zweier EU-Mitgliedstaaten Giovanni di Lorenzo [23]. Dies lässt sich mit **Autorisierung** der Stimmabgabe zusammenfassen.

Um zu dokumentieren, wer noch nicht gewählt hat bzw. wer bereits gewählt hat, muss ein Wählerverzeichnis geführt und aktuell gehalten werden. Es ist auch insofern von Bedeutung, als von dem Wahlkreis, in dem der Wähler wählt, abhängt, welche Kandidaten/Parteien zur Auswahl stehen.

2.1.3 Schutzziel Integrität der Stimme

Wie kann sich der Wähler bei REV sicher sein, dass seine Stimme so wie abgegeben **(Integrität der Stimme)** die elektronische Urne erreicht hat? Die Schweizerische Bundeskanzlei verlangt in dieser Hinsicht **individuelle Verifizierbarkeit:** *Der stimmenden Person wird die Möglichkeit gegeben zu erkennen, ob ihre Stimme, wie sie sie in die Benutzerplattform eingegeben hat, auf der Benutzerplattform oder auf dem Übertragungsweg manipuliert oder abgefangen worden ist; dazu erhält die stimmende Person einen Beweis, dass der vertrauenswürdige Systemteil … die Stimme so, wie sie die stimmende Person in die Benutzerplattform eingegeben hat, als systemkonform abgegeben registriert hat …* [24]

[3] *E-Voting … bei dem ein Teil des Wahlvorgangs elektronisch abgebildet wird* [16] – *Electronic voting systems are those which depend on some electronic technology for their correct functionality.* [17]

[4] Ein paar Kategorien verdanken wir [19].

[5] Dass das schwächste Glied maßgeblich ist, gilt bereits offline: Die Parteien fokussieren ihre Anstrengungen auf diejenigen US-Bundesstaaten, in denen ein knappes Rennen zu erwarten ist, die *Swing States* [20] oder, zutreffender, *Battleground States* [21].

[6] In 48 von 50 Bundesstaaten der USA dürfen Häftlinge nicht wählen; in einigen Bundesstaaten betrifft dies auch Ex-Häftlinge. [22]

2.1.4 Schutzziel Vertraulichkeit der Stimme

Zu den Grundsätzen von Wahlen in Demokratien, die diese Bezeichnung verdienen, gehört, dass sich der Wähler frei entscheiden kann, wem – Kandidat bzw. Partei – er seine Stimme anvertraut. Das setzt voraus, dass er sich niemandem gegenüber rechtfertigen muss. Daher muss die **Vertraulichkeit der Stimme** garantiert sein.[7]

Interessant für das Gebiet ›Informatik und Gesellschaft‹ ist, **welche Auswirkungen ein Bruch der Vertraulichkeit der Stimme haben könnte.**

2.1.5 Schutzziel Integrität der Urne

Alle abgegebenen Stimmen müssen berücksichtigt werden, und es dürfen nur autorisiert abgegebene Stimmen in die Zählung eingehen **(Integrität der Urne).** Die Schweizerische Bundeskanzlei verlangt zu diesem Zweck **universelle Verifizierbarkeit:** *Zur universellen Verifizierung erhalten die Prüferinnen und Prüfer*[8] *einen Beweis der korrekten Ergebnisermittlung; der Beweis bestätigt, dass das ermittelte Ergebnis folgende Stimmen berücksichtigt: 1. alle systemkonform abgegebenen Stimmen, die durch den vertrauenswürdigen Systemteil registriert wurden; 2. ausschliesslich systemkonform abgegebene Stimmen; 3. alle Teilstimmen gemäss des im Rahmen der individuellen Verifizierung generierten Beweises.* [24] Individuelle plus universelle Verifizierbarkeit wird in der Schweiz als **vollständige Verifizierbarkeit** bezeichnet.

2.1.6 Schutzmittel

Ein naheliegendes Angriffsziel sind die Server des REV-Systems; sie benötigen **physischen Schutz:** Schlösser am Gerät, gesicherte Räume. Der **Zugriff** darf **nur durch autorisierte Personen** erfolgen.

Ein Geheimnis lässt sich schützen, indem es so zerlegt wird, dass zur Rekonstruktion das Zusammenwirken mehrerer Personen erforderlich wird; man kennt das von Tresoren, die eine zeitgleiche Betätigung mehrerer Schlüssel erfordern. Bei REV muss der Schlüssel zum Entschlüsseln der abgegebenen Stimmen vor dem Zugriff Unbefugter geschützt werden, und er darf nicht vor der Zeit zur Anwendung kommen.

Die Vertraulichkeit der Stimme lässt sich durch **Verschlüsselung** gewährleisten, ebenso die Integrität der Stimme. Die Authentizität der Stimme kann durch eine **digitale Signatur** nachgewiesen werden.

2.1.7 Technische Machbarkeit eines Informatiksystems

Ist es nur eine Frage der Zeit, bis sicheres REV zur Verfügung steht **(technisch machbar)?** Oder ist sicheres REV **vielleicht technisch gar nicht machbar?** Diese Frage zu beantworten ist nicht trivial, denn: *There is such a complex interaction between the different requirements that such systems may be required to meet … in general, that it is not yet clear whether a universally acceptable solution exists.* [17] Mit *complex interaction* ist gemeint, **dass bestimmte Schutzziele miteinander in Konflikt stehen.**

2.1.8 Bedienbarkeit von Informatiksystemen

Das Kumulieren oder Panaschieren können REV-Systeme dem Wähler sehr erleichtern; wie das aussehen könnte, beschreibt [26]. Ansonsten ist der Umgang mit einem REV-System komplizierter als Lokalwahl oder Briefwahl. Von der **Bedienbarkeit** der Software hängt ab, ob nicht nur der digital native, sondern auch der digital naive Wähler in der Lage ist, seine Stimme wie gewünscht abzugeben.

2.1.9 Verfügbarkeit von Informatiksystemen

Seine Stimme abzugeben kann, z. B. wenn man stundenlang anstehen müsste, bereits offline ein Problem darstellen. Ein Beispiel sind die Wahlen im September 2021 in Berlin [27]; sie haben ein Nachspiel, das bis heute nicht abgeschlossen ist [28]. Bei REV ist die **Verfügbarkeit** durch technisches Versagen und durch Überlastungsattacken (*Denial-of-Service*-Attacken) bedroht.

2.1.10 Wirkung von Informatiksystemen

Bei Wahlen können ungültige Stimmen entstehen, in Deutschland 1. durch Stimmzettel, die nicht zum Wahllokal passen, 2. wenn der Wähler das Wahlverfahren verletzt (Beispiel Bundestagswahl: je 1 Stim-

[7] Südwestrundfunk/Westdeutscher Rundfunk berichten über die Volkskammerwahl in der DDR 1986: *Um mit Ja zu stimmen, wurden die Stimmzettel gefaltet und in die Urne geworfen. Wer die Wahlkabine benutzt macht … deutlich, dass er abweichend vom Wahlvorschlag abstimmen möchte. Er macht sich verdächtig! Er weiß nicht, ob und welche Folgen sein Verhalten haben kann. Von 196 Wahlberechtigten im Wahlbezirk 7 in Wernigerode benutzt nur ein Wähler die Kabine. Bei der Stimmenauszählung zeigt sich, dass auf einem Stimmzettel ein Name gestrichen ist.* [25]

[8] *Prüferinnen und Prüfer = Personen, die im Auftrag des Kantons den korrekten Ablauf des Urnengangs prüfen* [24]

me für den Kandidaten im Wahlkreis und für eine Partei), 3. wenn der Wähler den Stimmzettel unterschreibt, persönliche Informationen preisgibt, Kommentare anbringt etc. [29, 30] Wenn, z. B. bei einer Kommunalwahl, kumuliert/panaschiert wird, ist Punkt 2 ein wesentlicher Grund für das Entstehen ungültiger Stimmen. Bei den Nationalratswahlen in der Schweiz 2011 waren gegen drei Prozent der im Inland brieflich abgegebenen Stimmen ungültig. [31] Ungültig sind ferner Stimmen, die zu spät eintreffen; dies betrifft vor allem den internationalen Postweg; die Auslandschweizer machen hier regelmäßig schlechte Erfahrungen [32].

Mit dem Einsatz eines Informatiksystems wird die Hoffnung verbunden, **dass sich ungültige Stimmen verhindern lassen** [33, 14], z. B. dadurch, dass die App den Wähler darauf hinweist, dass sein Stimmverhalten einen ungültige Stimme zur Folge hätte [34].

Darüber hinaus verspricht man sich vom Einsatz eines Informatiksystems, **dass bei der Auszählung keine Fehler mehr vorkommen;** weil Streit über den aus der handschriftlichen Kennzeichnung des Stimmzettels hervorgehenden mutmaßlichen Wählerwillen nicht entstehen kann [35]; weil Stimmen weder verloren gehen können [36] noch auf dem falschen Stapel landen noch falsch addiert werden können [37].

Ferner wird erwartet, dass die Auszählung schneller vonstattengeht als per Hand, in Sekunden [38] oder Minuten [39, 40] statt Stunden oder Tagen. Andererseits sind bei REV viel weniger Personen in die Durchführung der Wahl involviert als bei Wahl im Wahllokal. Wenn es einer von ihnen gelänge, in die Wahl einzugreifen, könnte sie Manipulationen *automatisieren und auf Knopfdruck tausend- oder millionenfach ablaufen lassen* [41]. Diese Skalierung – im Positiven wie im Negativen – ist typisch, wenn Informatiksysteme zum Einsatz kommen. Wir erfassen für die QIA nur **die Skalierung des Manipulationsrisikos.**

2.1.11 Code von Informatiksystemen

Bei Informatiksystemen wird früher oder später auf den **Quellcode** rekurriert. Prominent ist die Frage nach einer **Veröffentlichung des Quellcodes.**

Mit der Komplexität von Informatiksystemen gehen Defekte einher, die zu **funktionalen Fehlern *(bugs)*** führen können. Zur Qualitätssicherung dienen **Softwaretests** ohne Berücksichtigung des Quellcodes *(blackbox testing),* darunter **Intrusionstests,** und **Softwareinspektion** (Einblick in den Quellcode, mit der Möglichkeit zum *whitebox testing*). Von einer **Zertifizierung** verspricht man sich Bestätigung der Qualität des Systems durch Fachleute.

2.1.12 Transparenz von Informatiksystemen

Informatiksysteme, mindestens Teile von ihnen, verhalten sich wie eine *Blackbox*. Selbst wenn der Quellcode öffentlich zugänglich ist, wird *blackbox testing* eine wichtige Rolle spielen.

Bei Lokalwahl können Wähler, die dies wünschen, vorstellig werden und, auch wenn sie in technischer Hinsicht Laien sind, die einzelnen Schritte nachvollziehen: zu Beginn ist die Urne leer; jeder Wähler bekommt nur 1 Stimmzettel; wer gewählt hat, wird im Wählerverzeichnis abgehakt; die Stimmen werden korrekt sortiert und korrekt addiert; die Ergebnisse der Wahllokale werden veröffentlicht und korrekt zum Gesamtergebnis zusammengeführt.

Es ist bis jetzt ungeklärt, wie Wahlbeobachter bei REV **ohne besondere Sachkenntnis die Abläufe nachvollziehen können** sollen. So kam das National Institute of Standards and Technology (USA) in einem Bericht von 2011 zu dem Schluss: *Because of the difficulty of validating and verifying software on remote electronic voting system servers and personal computers, ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution.* [42, 43]

2.1.13 Angriffe auf Informatiksysteme

Wenn Angriffe thematisiert werden, ist in der Presse meist von **›Manipulation‹, ›manipulier…‹** die Rede. In diesem Zusammenhang stellt sich die Frage: **Werden Manipulationen erkannt?** Angreifer – mit ihnen und ihren Motiven beschäftigen wir uns in Abschnitt 5.1 – werden in den Artikeln zumeist als **›Hacker‹ (›hacken‹, ›gehackt‹)** bezeichnet. Der Angriff kann von außen erfolgen (Intrusion) oder durch einen **Innentäter.** Angriffspunkte sind **Schwachstellen der Software *(exploits)*** oder absichtlich eingerichtete **Hintertüren.** Angriffsmittel ist für gewöhnlich **Schadsoftware *(malware),*** genauer: **trojanische Pferde**. Es braucht Bewusstsein dafür, **dass Sicherheit ein Wettlauf ist** und der Schutz des Systems permanent weiterentwickelt werden muss.

Wir unterscheiden in dieser Arbeit nicht zwischen versuchten/erfolgreichen Angriffen auf ein bestimmtes REV-Systemeinerseits und demonstrierten Angreifbarkeiten andererseits, sprechen übergreifend von **Lücken** in dem System.

2.2 Ergebnisse der QIA (Beantwortung von Forschungsfrage F1)

Anzahl NZZ-Artikel (von 320), in denen es um folgende Themen geht (Fortsetzung)

Beim Einsatz eines REV-Systems kann es nicht zu ungültigen Stimmen kommen
11

Annahme: Sicheres REV ist technisch machbar
9

Schutzmittel digitale Signatur
9

Bedienbarkeit eines REV-Systems
9

Softwareinspektion
8

Softwaretests
7

Papierstimmzettel-Auszählung ist ohne besondere Sachkenntnis nachvollziehbar
7

Schadsoftware *(malware)*
7

Schwachstellen *(exploits)*
7

funktionelle Fehler *(bugs)*
7

Zielkonflikte bei Schutzzielen
6

Gedanke: Sicheres REV ist technisch vielleicht gar nicht machbar
5

Ausspähen von Informationen *(phishing)*
5

Maßstab der Sicherheit eines Systems ist das schwächste Glied
4

Es geht um den Quellcode (aber nicht um Offenlegung des Quellcodes)
4

Angriff durch einen Innentäter
4

Gefahr menschlicher Fehlleistungen
4

Auswirkungen eines Bruchs der Vertraulichkeit der Stimme
4

Sicherheit ist ein ständiger Wettlauf
3

Angriff durch eine Hintertür
3

Anzahl NZZ-Artikel (von 320), in denen es um folgende Themen geht (Fortsetzung)

Zugriff erhalten nur autorisierte Personen
3

Der Zugriff ist so geregelt, dass mehrere Personen zusammenwirken müssen
2

trojanische Pferde
1

Ein Informatiksystem ist eine *Blackbox*
1

Bei Auszählung durch ein REV-System sind Fehler ausgeschlossen
1

Anzahl Guardian-Artikel (von 219), in denen es um folgende Themen geht

Autorisierung des Wählers
51

›Manipulation‹, ›manipulier…‹
39

Verfügbarkeit des REV-Systems
29

›Hacker‹, ›hacken‹, ›gehackt‹
26

Schutzziel Integrität der Urne
25

Schutzziel Vertraulichkeit der Stimme
23

Bedienbarkeit eines REV-Systems
16

Beim Einsatz von Informatiksystemen skaliert das Manipulationsrisiko hoch
13

Sicherheit ist relativ
13

Ein bestimmtes REV-System ist entweder sicher oder unsicher (Sicherheit ist absolut)
12

Es wird über Lücken in einem bestimmten REV-System berichtet
12

Schadsoftware *(malware)*
11

Werden Manipulationen erkannt?
10

Anzahl Guardian-Artikel (von 219), in denen es um folgende Themen geht (Fortsetzung)

Softwaretests
9

Offenlegung des Quellcodes
9

Bei Auszählung durch ein REV-System sind Fehler ausgeschlossen
9

Zertifizierung als Voraussetzung für den Einsatz eines REV-Systems
8

funktionelle Fehler *(bugs)*
8

Gedanke: Sicheres REV ist technisch vielleicht gar nicht machbar
7

Schutzziel physischer Schutz der Server
7

Beim Einsatz eines REV-Systems kann es nicht zu ungültigen Stimmen kommen
7

Schutzmittel Verschlüsselung
6

Annahme: Sicheres REV ist technisch machbar
6

Schutzmittel digitale Signatur
6

Schutzziel Integrität der Stimme
6

Zielkonflikte bei Schutzzielen
5

Angriff durch einen Innentäter
4

trojanische Pferde
3

Softwareinspektion
3

Papierstimmzettel-Auszählung ist ohne besondere Sachkenntnis nachvollziehbar
3

Auswirkungen eines Bruchs der Vertraulichkeit der Stimme
3

Sicherheit ist ein ständiger Wettlauf
2

Es geht um den Quellcode (aber nicht um Offenlegung des Quellcodes)
2

Anzahl Guardian-Artikel (von 219), in denen es um folgende Themen geht (Fortsetzung)

Intrusionstests
2

Eine Manipulation der Stimme lässt sich durch individuelle Verifizierbarkeit aufdecken
2

Ein Informatiksystem ist eine *Blackbox*
2

Ausspähen von Informationen *(phishing)*
1

Der Zugriff ist so geregelt, dass mehrere Personen zusammenwirken müssen
1

Angriff durch eine Hintertür
1

Schwachstellen *(exploits)*
1

Gefahr menschlicher Fehlleistungen
1

3 E-Voting nach Ländern

In diesem Abschnitt werden das REV-System, das in Estland zum Einsatz kommt, und das REV-System, das in der Schweiz zum Einsatz kommen soll, beschrieben. Weil die Themen REV und Wahlcomputer im Wahllokal Schnittmengen besitzen, gehen wir auch auf die Entwicklung in Deutschland ein.

Die Darstellung richtet sich nicht an den informatischen Laien – die Ideen, Begriffe, Konzepte, die man zum Verständnis benötigt, werden im Rahmen der Beantwortung von Forschungsfrage F2 in Abschnitt 4 herausgearbeitet.

3.1 REV in Estland

Estland bietet seinen Wählern seit 2005 (Kommunalwahl) bzw. 2007 (Landesparlament) bzw. 2009 (Europäisches Parlament) die Möglichkeit, die Stimme per Internet abzugeben [1], vom zehnten bis zum vierten Tag vor dem klassischen Wahltag. [44] Estlands REV-System, das von der Firma Cybernetica entwickelt wurde, funktioniert wie folgt [44, 45, 46]:

Für jede Wahl wird eine App, die IVCA *(i-Voting Client Application)*, welche für Windows, macOS und Linux erhältlich ist [47], neu zusammengestellt. Der Wähler lädt diese Wahl-App von der Website `www.valimised.ee` herunter. Die Wahl-App enthält den öffentlichen Schlüssel *(public key, PK)*, mit dem die Stimmen bei dieser Wahl zu verschlüsseln sind. Das Schlüsselpaar öffentlicher/geheimer Schlüssel wird durch ein Hardware-Sicherheitsmodul *(Hardware Security Module)* erzeugt [3, S. 64]. Das Geheimnis des privaten Schlüssels wird auf sieben Mitglieder des Wahlkomitees sowie zwei Mitglieder des Wahlbüros verteilt [48].

Der Wähler authentifiziert sich gegenüber dem Stimmensammel-Server *(collection server)* mit der Smartcard, über die alle Bürger Estlands verfügen; sie wird mit dem Rechner durch ein Kartenlesegerät verbunden. Alternativ leistet seit 2007 eine spezielle SIM-Card fürs Smartphone dieselben Dienste. [3] Auf der ID-Card ist ein privater Schlüssel für digitale Signaturen hinterlegt; eine PKI-Infrastruktur steht in Estland zur Verfügung. Zum digitalen Signieren ist eine PIN einzugeben.

Passend zum Wahlkreis wird der Wahl-App die Liste der Kandidaten/Parteien übermittelt. Die Wahl-App erzeugt eine Zufallszahl r und verschüsselt mit der Kombination (PK, r) die, so funktioniert es intern, Identifikationsnummer [46] des Wunschkandidaten und beglaubigt den elektronischen Stimmzettel durch die digitale Signatur des Wählers. [46] Die kryptografischen Operationen finden auf der ID-Card statt [49] bzw. auf dem Smartphone.

Es folgt offline ein Weiterverarbeitungs-Server *(processor server)*, auf den die verschüsselten und signierten Stimmen, so ist es vorgesehen, mit einer DVD übertragen werden. Der Weiterverarbeitungs-Server berücksichtigt, dass jeder Wähler nur 1 Stimme abgeben darf, entfernt also alle vom Wähler abgegebenen Stimmen außer der letzten (oder alle, nämlich dann, wenn der Wähler zusätzlich offline gewählt hat), gruppiert die verschlüsselten Stimmen nach Wahlkreisen, entfernt die digitalen Signaturen, anonymisiert also die verschlüsselten Stimmen, verschlüsselt die Kryptogramme ein zweites Mal (Umverschlüsseln, *re-encryption*) und mischt sie (beides hat das Ziel, sie von der Reihenfolge des Eingangs beim Stimmensammel-Server zu entkoppeln), bevor sie an den Zähl-Server *(counting server)* weitergegeben werden, der, wenn von den neun Schlüsselträgern mindestens fünf zugegen sind [48] und ihren Teil des Geheimnisses beisteuern, mit dem wieder zusammengesetzten privaten Schlüssel die Stimmen entschlüsselt und die Auszählung vornimmt.

2011 gab ein Vorfall, den wir auf Seite 31 f. beschreiben, Anlass dazu, die Annahme, dem Rechner des Wählers dürfe vertraut werden, zu überdenken. [50] In der Folge hat Estland sein REV-System erweitert. Seit 2013 [51] kann der Wähler mit einer Verifizierungs-App *(Individual Verification Application)*, die auf ein Smartphone oder Tablet herunterzuladen ist, überprüfen, ob seine Stimme so, wie er sie abgegeben hat, die Urne erreicht hat. Zu diesem Zweck zeigt die Wahl-App nach der Stimmabgabe einen QR-Code an, der die Zufallszahl r enthält sowie eine Quittungsnummer *(vote identifier)*, die die Wahl-App vom Stimmensammel-Server zurückbekam. [46] Mit diesem QR-Code kann sich die Verifizierungs-App die abgegebene Stimme bestätigen lassen. Der Stimmensammel-Server übermittelt der Verifizierungs-App das Kryptogramm K der abgegebenen Stimme ohne die digitale Signatur des Wählers [49] sowie die Liste der Kandidaten/Parteien. Die Verifizierungs-App berechnet nun für jeden Kandidaten c das Krytogramm K', das sich ergeben hätte, wenn der Wähler für c gestimmt und den Stimmzettel mit (PK, r) verschlüsselt hätte, vergleicht K' mit K und gibt den Namen desjenigen Kandidaten aus, bei dem Übereinstimmung festgestellt wird. [44] Die Möglichkeit der Verifizierung steht für 30 min und 3 Zugriffe zur Verfügung [49]. Als Schutz gegen Zwang und Stimmen(ver)kauf besteht die Möglichkeit, seine Stimme mehrmals abgeben; es zählt die zuletzt bzw. die im Wahllokal abgegebene Stimme.

Springall et al. haben 2013 eine Wahl in Estland begleitet und das System im Labor nachgestellt. In ihrem Bericht, den wir in dieser Arbeit an den passenden Stellen aufgreifen, diskutieren sie mögliche Angriffe und schildern haarsträubende Fehlleistungen, die sie beobachtet haben. Sie zogen das Fazit: *We conclude that there are multiple ways that … attackers … could successfully attack the Estonian I-voting system. For these reasons, we recommend that Estonia discontinue the I-voting system.* [49]

Estland hat darauf reagiert. Um robuster gegenüber dem Faktor Mensch zu werden [50], wurde das System 2017 um Ende-zu-Ende-Verifizierbarkeit *(end-to-end verifiability)* erweitert [44], die Möglichkeit, zu überprüfen, dass die Beziehung zwischen den gespeicherten Stimmen und dem Wahlergebnis bestimmte Eigenschaften hat [50]: dass die Stimmen wohlgeformt sind *(anyone is able to check that valid ballots do not contain over-votes or negative votes)*, dass die Stimmen wie erfasst gezählt wurden *(anyone is able to check that all the recorded ballots have been tallied correctly)*, dass die Stimmen konsistent sind *(anyone is able to check that the voters and the general public have the same view of the election records)*, dass die Stimmen authentisch sind *(anyone can check that any cast ballot has a corresponding voter who can perform check No. 3 [erfasst wie abgegeben])*; genau dies werde üblicherweise unter universeller Verifizierbarkeit verstanden [50].

3.2 REV in der Schweiz

Die folgende chronologische Darstellung basiert auf [52, 53]: In der Schweiz fanden zwischen 2004 und 2019 mehr als 300 Versuche mit REV statt. 2010 kamen drei verschiedene REV-Systeme zum Einsatz: 1. das System des Kantons Neuenburg, man stützte sich auf Software der Firma Scytl [54], 2. das System des Consortiums Vote électronique, zu dem neben anderen der Kanton Zürich gehörte, man stützte sich auf Software der Firma Unisys [55], 3. das System des Kantons Genf, eine Eigenentwicklung [56].

Neben dem Internetkanal ermöglichte Zürich zeitweise das Wählen per SMS oder interaktivem TV; Wählen per SMS wurde 2007 eingestellt. [57]

2015 kamen in der Schweiz erstmals Systeme mit individueller Verifizierbarkeit zum Einsatz. Das Consortium entschloss sich 2015, sein REV-System nicht weiterzuentwickeln; die Kosten wären nicht mehr vertretbar gewesen. [58] 2016 trat mit der Schweizerischen Post, deren REV-System sich ebenfalls auf Software der Firma Scytl stützte, ein neuer Akteur

auf. Im Juni 2019 stellte der Kanton Genf sein System wegen der hohen Kosten, die mit einer Weiterentwicklung verbunden wären, ein. [59, 60] Mit Weiterentwicklung ist in beiden Fällen keine allgemeine Weiterentwicklung gemeint, sondern die Weiterentwicklung in Richtung Verifizierbarkeit. Die Bundeskanzlei verlangte für die Zulassung eines REV-Systems für die Erfassung von mehr als 50 % aller Stimmen vollständige Verifizierbarkeit. [61, 62]

Im März 2019 wurden Mängel bei der individuellen Verifizierbarkeit im System der Post bekannt; seit Juli 2019 kam das System nicht mehr zum Einsatz. Die NZZ berichtete, die Post setze auf ein neues System, das sie ab 2020 anbieten wolle. [63] Die Post plant, dass die Kantone das neue System im Laufe des Jahres 2023 einsetzen können. [64]

Wir stellen das System dar, wie die Schweizerische Post es anpreist [65, 14, 66]: Wie in Estland, so ist auch in der Schweiz REV ein zusätzlicher Abstimmungskanal; dieser Kanal ist insbesondere für Abstimmungen der direkten Demokratie von Interesse. Das System basiert auf dem Austausch von Codes *(Returncodes)* zwischen Wähler und Wahl-Server. Jeder Wähler erhält mit der Post eine Wahl-und-Wähler-individuelle Codeliste. Die Codes werden offline berechnet. Die Post unterstützt die Kantone bei der Vorbereitung der Unterlagen für die Wähler; die Kantone lassen die Unterlagen von zugelassenen Druckpartnern produzieren.

Der Wähler gibt auf der Website für die Wahl eine PIN ein (*Start Voting Key [SVK],* 24 Zeichen), um die Autorisierung für die Stimmabgabe zu bekommen; welcher Wähler sich mit diesem SVK autorisiert, weiß der Onlineteils des Systems nicht.

Der Wähler trifft nun, abhängig vom Modus der Wahl (Kumulieren? Panaschieren?), eine Auswahl; ihm bleiben bis zu fünf Versuche, um eine gültige Auswahl zusammenzustellen [67]. Jedem Klartextnamen ist eine kleine Primzahl zugeordnet [14]; die Folge der den ausgewählten Kandidaten zugeordneten Zahlen wird als Produkt kleiner Primzahlen in einer einzigen Zahl codiert, vor der Übermittlung verschlüsselt und digital signiert. Das System antwortet mit einem Auswahlbestätigungscode (*Choice Return Code [CC],* 4 Ziffern) für jeden Kandidaten. Diese Codes kann das System berechnen [14]; Näheres zu diesem interessanten Punkt folgt auf Seite 24. Der Wähler überprüft, ob die Auswahlbestätigungscodes mit den Auswahlbestätigungscodes übereinstimmen, die auf seiner Codeliste neben den Kandidaten abgedruckt sind. Falls nein, bricht er den Wahlvorgang ab. Falls ja, gibt er einen Stimme-abgeben-Code (*Ballot Casting Key [BCK],* 9 Ziffern) ein. Das System antwortet mit einem Stimme-erhalten-Code (*Vote Cast Return Code [VCC],* 8 Ziffern). Unterbrechung plus Wiederaufnahme des Wahlvorgangs ist möglich. Sobald der Wähler seine Auswahl abgeschickt und im Gegenzug die Auswahlbestätigungscodes erhalten hat, lässt sich die Auswahl auf dem Onlinekanal nicht mehr ändern. Solange der Wähler seine Auswahl noch nicht mit dem BCK-Code bestätigt hat, kann er auf einem anderen Kanal noch für jemand anderen stimmen. Jedenfalls kann er seine Stimme exakt ein Mal abgeben. [65]

Die Weiterverarbeitung erfolgt offline. Die verschlüsselten Stimmen durchlaufen mehrere Mischer, in denen sie partiell entschlüsselt, d. h. umverschlüsselt werden; das Geheimnis des privaten Schlüssels ist wie in Estland auf mehrere Personen verteilt. [14] Es folgt die Auszählung.

Das System der Post bietet individuelle Verifizierbarkeit (die Auswahlbestätigungscodes) plus universelle Verifizierbarkeit. Die Schweizerische Bundeskanzlei verlangt dies: *Es ist sichergestellt, dass jede Manipulation, die zu einer Verfälschung des Ergebnisses führt, unter Wahrung des Stimmgeheimnisses erkannt werden kann (vollständige Verifizierbarkeit). Dies gilt als gegeben, wenn die Anforderungen an die individuelle und an die universelle Verifizierbarkeit erfüllt sind.* [24] Lewis et al. weisen darauf hin, dass die Post eine zusätzliche Annahme zugrunde legt: *The Swiss sVote voting system claims to offer a form of verifiability, called 'complete verifiability', which aims at offering the same guarantees as universal verifiability under the extra assumption that at least one of the components on the server-side, i.e., the people running the voting system, behaves honestly … (universal verifiability offers guarantees even if all server-side components are malicious.)* [68]

3.3 Wahlcomputer in Deutschland

1998 wurde im Schlussbericht der Enquete-Kommission des Deutschen Bundestages ›Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft‹ vorgeschlagen, dass *bei Bundestagswahlen … das Angebot gemacht werden [sollte], künftig in Ergänzung zur Urnen- und Briefwahl … auch per Internet zu wählen* [69]. Bei der Bundestagswahl im September 2005 gaben etwa 2,5 Millionen Wähler in 2 100 von insgesamt 80 000 Wahllokalen ihre Stimme an Wahlcomputern der Firma Nedap ab. [70, 16]

Einsprüche anlässlich der elektronischen Stimmabgabe wurden vom Wahlprüfungsausschuss des Deutschen Bundestages, d. h. einer Mehrheit in diesem Ausschuss – in aller Regel handelt es sich bei der Mehrheit um die Regierungsmehrheit –, im November 2006 zurückgewiesen. [71]

In der Folge musste sich das Bundesverfassungsgericht mit Wahlprüfungsbeschwerden befassen. Das Bundesinnenministerium lehnte es unter Berufung auf Betriebsgeheimnisse ab, Unterlagen, die die Firma Nedap der Physikalisch-Technischen Bundesanstalt für die Prüfung der Baumuster überlassen hatte, oder Prüfberichte der Physikalisch-Technischen Bundesanstalt der interessierten Öffentlichkeit zugänglich zu machen. [72] Kurz und Rieger zeigten 2007 zahlreiche Möglichkeiten auf, die Wahlcomputer der Firma Nedap zu manipulieren. [73] Im März 2009 erging ein Urteil des Bundesverfassungsgerichts. Den Kern dieses Urteils bildet die Anforderung: *Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können.* [72][9] Volkamer et al. fassen das Urteil wie folgt zusammen: *Hierin wird entschieden, dass die Zertifizierung des Wahlgerätes nicht ausreicht, und es werden Verifizierungsfunktionen gefordert, die den Wählern die Möglichkeit geben, sich von der Integrität des Wahlergebnisses zu überzeugen.* [74]

Eine Eidgenössische Volksinitiative, elektronische Verfahren zur Stimmabgabe zu verbieten, wobei die Möglichkeit vorgesehen war, das Verbot aufzuheben, *wenn gewährleistet ist, dass mindestens die gleiche Sicherheit gegen Manipulationshandlungen wie bei der handschriftlichen Stimmabgabe besteht, namentlich wenn unter Wahrung des Stimmgeheimnisses … die Teilergebnisse der elektronischen Stimmabgabe eindeutig und unverfälscht ermittelt sowie nötigenfalls in Nachzählungen ohne besondere Sachkenntnis zuverlässig überprüft werden können* (E-Voting-Moratorium, [75]), scheiterte im November 2020 im Sammelstadium [76]. Die NZZ fasste die Befürchtungen der Befürworter von REV wie folgt zusammen: *Eine Gruppe von Politikern und Netzaktivisten will eine Volksinitiative lancieren, mit der E-Voting faktisch verunmöglicht würde.* [77]

Erwähnenswert ist an dieser Stelle: Der Komplex Manipulation durch Wahlcomputer wurde von Andreas Eschbach in ›Ein König für Deutschland‹ [78], erschienen im September 2009, in Form eines Romans aufgearbeitet, mit umfangreichen Fußnoten, in denen im Detail der Frage nachgegangen wird, wie sich welche Manipulation technisch realisieren lässt.

4 Forschungsfrage F2

In diesem Abschnitt wird die Frage beantwortet:

F2 Welche Begriffe, Ideen, Konzepte der Informatik benötigt der informatische Laie – wie es Schüler, Bürger, Politiker im Allgemeinen sind –, um das Thema Internetwahl technisch zu durchdringen?

Wir entwickeln den Kanon der Begriffe, Ideen, Konzepte, den wir zur Beantwortung von F2 für erforderlich halten, anhand von Zitaten aus den Artikeln und anhand von Vorkommnissen, zu denen es beim Einsatz von REV-Systemen kam. Die Antworten zu Forschungsfrage F2 sind fett hervorgehoben.

Eine Anmerkung: Wenn man der Deutung folgt, dass ›Informatik‹ ein Kofferwort gebildet aus ›Information‹ plus ›Mathematik‹ ist, dann ergibt es keinen Sinn, näher zu unterscheiden, bei welchen Konzepten es sich mehr um Konzepte der Mathematik handelt.

4.1 Technisches Versagen

Falls das System ausfällt, kann eine REV-Wahl mit vergleichsweise geringem Aufwand wiederholt werden. Es gibt aber auch subtiles technisches Versagen, und zwar Versagen von Speicher. **Bitflips** [79], also dass ein **Bit,** das eine 0 enthielt, plötzlich eine 1 enthält bzw. umgekehrt, können z. B. – das ist keine Esoterik; für diese Entdeckung wurde Hess 1936 der Physik-Nobelpreis verliehen – durch kosmische Strahlung verursacht werden; weitere Ursachen für Bitflips sind denkbar.

Speicherfehler treten zwar selten auf, aber häufiger, als man dachte: *We observe DRAM error rates that are orders of magnitude higher than previously reported, with 25,000 to 70,000 errors per billion device hours per Mbit and more than 8% of DIMMs affected by errors per year* [80]. Alterungseffekte spielen eine Rolle: *Age severely affects … error rates: one should expect an increasing incidence of errors as DIMMs get older, but only up to a certain point, when the incidence becomes almost constant … The age when errors first start to increase and the steepness of the increase vary per platform, manufac-*

[9] In der Drucksache, in der die Einsprüche abgehandelt werden [71], und im Urteil des Bundesverfassungsgerichts [72] sind die Argumente beider Seiten, der Befürworter wie der Gegner von Wahlcomputern, ausführlich dargestellt.

turer and DRAM technology, but is generally in the 10–18 month range. [80]

Die Verteilung der Mandate ändert sich im Allgemeinen nicht, wenn bei einer Nachzählung herauskommt, dass 1 Stimme einem anderen Kandidaten/einer anderen Partei zuzuordnen ist. Dazu müsste der Bitflip allerdings im letzten Bit der zugeordneten Speicherzelle aufgetreten sein. Tritt er z. B. im ersten Bit einer sechzehn Bit breiten Speicherzelle auf, erhöht sich die Zahl um 32768 – oder die Zahl wird negativ (!). Zum Verständnis benötigt man das Konzept der **Binärzahlen.**

Wenn die elektronische Stimme aus der Id(entifizierungsnummer) des Kandidaten besteht, führt ein Bitflip dazu, dass entweder die Id eines anderen Kandidaten entsteht oder eine Id, die keinem Kandidaten zugeordnet ist (ungültige Stimme). Bei der Wahl des Landesparlaments 2011 in Estland musste 1 elektronische Stimme für ungültig erklärt werden. [81] Hierfür kommen zwei Erklärungen infrage. Die komplizierte beschreiben wir auf Seite 30. Die einfachere: Es kam zu technischem Versagen.

Bei einem unplausiblen Ergebnis – Summe der Stimmen passt nicht; eine negative Zahl von Stimmen; etc. – kann also trotz Einsatz eines Informatiksystems eine Nachzählung der elektronischen Stimmen, bei der man ja eigentlich kein anderes Ergebnis erwartet, erforderlich werden.

4.2 Designentscheidungen

4.2.1 Struktur des Internets

In der NZZ liest man, zu den Sicherheitsaspekten eines transparenten REV-Systems gehöre der *Erhalt der Daten auf Schweizer Gebiet* [82]. Sicherlich kann man die Server auf Schweizer Gebiet betreiben. Es lässt sich jedoch nicht garantieren, dass die Kommunikation der Schweizer Bürger mit den Servern auf Schweizer Gebiet ausschließlich über Server geleitet *(gerootet)* wird, die sich ebenfalls auf Schweizer Gebiet befinden. Hier fehlt es an Verständnis betreffend ***Rooting* bzw. die Struktur des Internets.**

4.2.2 Bedienbarkeit von Informatiksystemen

Wir betrachten einige Vorkommnisse, die mit der Bedienbarkeit von REV-Systemen zu tun haben:

Estland. *Three people turned to the ... help-desk with the following problem: the IVCA GUI was too large to fit onto their computer screen and two candidates on the bottom of the list were hidden by the Windows task-bar.* [81]

Schweiz. Bei evoting.zh.ch bekam ein Problem, *wer zuerst den Stadtrat und erst später das Parlament wählen wollte. Wer die erste Wahl mit der Eingabe des geforderten PIN-Codes und des Geburtsdatums abschloss, hatte keinen zweiten Zugriff zum E-Voting-System mehr.* [83]

USA. *In most cases, voters cast ballots by pressing a big red button labelled ›vote‹. But some versions of the system require touching a ›confirm vote‹ box on the screen to complete the ballot. It is alleged officials hid this fact from voters and would then 'correct' and confirm the ballot after the voter had left. The officials have pleaded not guilty. Matt Blaze, a security researcher at the University of Pennsylvania, writes in his blog that if this were a strategy, it's a pretty elegant attack, exploiting little more than a poorly designed, ambiguous user interface, printed instructions that conflict with actual machine behaviour, and public unfamiliarity with equipment that most citizens use at most once or twice each year. And once done, it leaves behind little forensic evidence to expose the deed.* [84]

Die Beispiele illustrieren: **Die Bedienbarkeit eines REV-Systems** ergibt sich nicht von selbst, aus der zu erfüllenden Aufgabe, sondern **erzwingt, wie jede Rechner-Benutzer-Schnittstelle, Designentscheidungen.** Ondrisek formuliert als Anforderungen an die Benutzerschnittstelle u. a. *Darstellung des Stimmzettels auf einer Bildschirmseite, ohne Scrollen* und *adäquate Darstellung des Ablaufes der Stimmabgabe (›Weiter‹-, ›Zurück‹- und ›Abbrechen‹-Buttons, etc.), vor der endgültigen Abgabe kann der Stimmzettel nochmals kontrolliert und geändert werden* [16].

4.2.3 Zielkonflikte bei Schutzzielen

Beim Design jedes Informatiksystems treten Zielkonflikte auf, die Kompromisse erfordern. Bezug zur Informatik haben bei REV:

- Sicherheit versus Bedienbarkeit [85, S. 14]
- Sicherheit versus Nachvollziehbarkeit der Technik durch Auditoren [44]
- Sicherheit versus Komplexität der Implementierung [81]
- individuelle Verifizierbarkeit versus Schutz des Wählers vor Zwang und Schutz der Wählergemeinschaft vor Stimmen(ver)kauf [86]
- Vertraulichkeit der Stimme versus Dokumentation der Autorisierung der Stimme [79, 87]; deswegen

ist REV fundamental anders gelagert als Onlinebanking, wo die Transaktionen ja nachvollziehbar sein müssen [88]

- Sicherheit (abstrakt wählen mit Wahl-und-Wähler-individuellen Tabellen, in denen sogar die Namen der Kandidaten/Parteien codiert sind) versus – sowohl in Estland [46] als auch in der Schweiz [89] – Anschaulichkeit (die Namen der Kandidaten/Parteien erscheinen auf dem Bildschirm des Wählers)[10]

4.3 Code

4.3.1 Quellcode *(source code)*

Es ist noch immer kein Allgemeingut, was es mit dem Quellcode eines Informatiksystems auf sich hat. In der NZZ wird vom *Herzstück der E-Voting-Software* [90] gesprochen, im Guardian von *software secrets*[11] [91]. Die Bundeskanzlei bietet folgende Erklärung: *Beim Quellcode handelt es sich um den Text eines Computerprogrammes. Er wird von Menschen geschrieben, ist für Menschen lesbar und beschreibt die Funktionsweise des Computerprogrammes.* [92] Durch das Wort *beschreibt* kann jedoch der Eindruck entstehen, der Quellcode sei so etwas wie eine Dokumentation.

Bessere **Vergleiche, die einem Laien illustrieren, was ein Quellcode ist,** sprechen von dem *in Programmiersprache verfassten Bauplan eines Systems* [60], *der DNA des E-Voting-Systems* [82]. Die reale Ausführung eines Baus kann allerdings vom Bauplan abweichen. (Wenn man von einem Schaltplan spräche, hätte man dasselbe Problem.) Die DNA kodiert – Epigenetik – nur einen Teil der Konfiguration der lebenden Zelle.

In welchem Zusammenhang stehen Quellcode und Informatiksystem? Der Quellcode ist die Formulierung des Algorithmus in einer Hochsprache. Er wird von einem Compiler in **Maschinensprache** übersetzt bzw. von einem Interpreter in die Sprache einer virtuellen Maschine übersetzt. Entscheidend ist: **Das Programm, das zur Ausführung kommt, führt lediglich die Anweisungen aus, die im Quellcode formuliert sind; das und nichts anderes tut es.**

Dem Laien stellt sich die Frage, warum nicht direkt in Maschinensprache programmiert wird. Antwort: **Eine höhere Programmiersprache erlaubt das Programmieren auf einem höheren Abstraktionsniveau.** Das Programmieren wird dadurch für den Menschen erheblich komfortabler, ja erst möglich; Gleiches gilt für das Nachvollziehen des Programms. Ein detailliertes Beispiel, das den Unterschied illustriert, findet sich bei [93].

4.3.2 Sicherheit durch Geheimhaltung/ Verschleierung *(security by obscurity)*

In der NZZ wird gewarnt: *Es erscheint mir … blauäugig, den Quellcode eines E-Voting-Systems zu veröffentlichen … Wohlwollende Hacker können zwar mit dem Quellcode auf Schwachstellen aufmerksam machen; bösartige erhalten aber ein unschätzbar wertvolles Hilfsmittel zur Manipulation!* [94] In die gleiche Richtung deutet die Konnotation des Satzübergangs in folgendem Zitat: *Anfang 2019 setzte die Post ihr E-Voting-System den Angriffen der Hacker weltweit aus und legte den Quellcode … offen. Rasch fanden Experten gravierende Sicherheitslücken.* [90] Ähnlich liest sich: *Die Post unterzog dieses System einem öffentlichen Intrusionstest. 3000 internationale Hacker bissen sich an ihm nach Angaben der Post die Zähne aus. Im Quellcode wurden allerdings schwere Fehler entdeckt.* [63]

Auf der anderen Seite wird in der NZZ zu Recht darauf hingewiesen: *Im Sicherheitsbereich ist es verführerisch und entspricht leider einer verbreiteten Praxis, dass man die Sicherheit eines Systems dadurch zu erhöhen versucht, dass man seine Funktionsweise verschleiert, möglichst komplex gestaltet und grundsätzlich nicht offenlegt* [88] (*security by obscurity*, Begriff z. B. in [73]).

Es ist zu kurz gedacht, wenn die Intrusionstests der Post in der NZZ als *Eigentor für den Anbieter* [95] bezeichnet werden. Intrusionstests, bei denen jedermann mitmachen kann,[12] sind vielmehr ein wichtiges Mittel, um im **Wettlauf von (neuartigem) Angriff und Maßnahmen gegen diesen Angriff** ein System zu verbessern.

Den Quellcode nicht zu veröffentlichen, mag den Aufwand für Angreifer erhöhen. **Der Maschinencode lässt sich dennoch** – das Ziel: das Programm leichter nachvollziehen zu können – **in hochsprachlichen Code zurückverwandeln *(Reverse Engineering),*** und dafür gibt es Werkzeuge, d. h. Hilfsprogramme.

[10] Heiberg et al. thematisieren diese Abwägung: *The IVCA is executed in the malicious environment … One possible solution is to use a blind voting scheme … where for each voter personalized candidate numbers (codes) are generated. Codes can later be re-unified by the tabulation process for tally. The voter gets his codes through some pre-channel and uses computer to enter and send the code for the desired candidate … The problems with this protocol are … (iii) most of the people will not find this system usable.* [81]

[11] Das passt insofern, als der Guardian berichtet: *E-voting machine companies refuse to open up their software for public viewing.* [91]

[12] Die Post stellt für die Meldung unbekannter Schwachstellen Belohnungen in Aussicht (*Bug-Bounty*-Programm), unbefristet. [96]

Estland ergreift Maßnahmen, um eine Rückübersetzung/Interpretation des ausführbaren Codes zu erschweren: *The executable is obfuscated using the UPX packing tool. Strings, public keys, and other resources are hidden by XORing*[13] *them with the output of a linear congruential generator*[14]. [49] Man ist sich dort aber durchaus bewusst, dass Angreifer den ausführbaren Code der IVCA dennoch aufboren können: *It is hoped that a 7-day i-voting period is short enough to avoid reverse engineering of the IVCA, designing and implementing robust and stealthy malicious code, distributing and activating it on a large scale.* [81] Für Profis wie Springall et al. stellt eine komprimierte ausführbare Datei aber keine große Hürde dar: *These measures did not significantly complicate the construction of our attacks. We used the UPX application with the* `-d` *switch to unpack the binary and used the IDA Pro disassembler and Hex-Rays decompiler to reverse the portions necessary for our attacks.* [49] Erneut zeigt sich: Sicherheit ist ein ständiger Wettlauf.

4.3.3 Zertifizierung eines Informatiksystems

Eine vertrauensbildende Maßnahme kann darin bestehen, dass ausgewählten Personen Einsicht in den Quellcode gewährt wird, gegebenenfalls nach Abgabe einer Verschwiegenheitserklärung. **Auch bei einer Zertifizierung durch Fachleute können jedoch Dinge übersehen werden,** selbst bei Zertifizierung durch eine namhafte Firma wie KPMG [97]. Und wenn die Hersteller von Wahlcomputern den Zertifizierungsbericht unter Verschluss halten [91], ist diese Vorgehensweise sicherlich nicht geeignet, das Vertrauen in die Zertifizierung zu stärken.

Letztlich wird bei Zertifizierung das Autoritätsargument bemüht: *Manch einer mag darauf vertrauen, dass die elektronischen Abstimmungssysteme durch Experten betreut werden, die ihr Handwerk verstehen und die Fälschungssicherheit garantieren.* [98] Eigentlich müsste die vierte Gewalt beim Hinweis auf Zertifizierung im Interesse der Öffentlichkeit nachhaken: *Wer* hat darüber entschieden, *welche (wie qualifizierten und wie hoch bezahlten?) Fachleute* das System *in welcher Hinsicht* und *in welchem Umfang* prüfen?

Abschließend sei ein **Interessenkonflikt** angesprochen: Der Zertifizierer ist auf kommende Aufträge angewiesen; es spricht sich aber herum, wenn er einem zahlenden Kunden das Zertifikat verweigert.

4.3.4 Veröffentlichung des Quellcodes

In der NZZ wird unter einer **Veröffentlichung des Quellcodes** verstanden, *dass die verwendete Programmiersprache publik gemacht wird und jedermann, der sie versteht, die getroffenen Sicherheitsmassnahmen nachvollziehen und überprüfen kann.* [99] Ersteres ist falsch. Es geht darum, **dass der Algorithmus, d. h., die Summe von Anweisungen, die das Programm ausmachen, öffentlich einsehbar wird.**

Die Intention, die hinter einer Veröffentlichung des Quellcodes steht, wird meist korrekt beschrieben: ***Durch die Publikation erhalten Drittpersonen die Möglichkeit, die Sicherheit des Systems zu überprüfen.*** [100] – *so people can identify both intentional and unintentional flaws …* [101]

Die Bundeskanzlei schreibt vor (mittlerweile; die Vorschrift wurde nach etwa sechzehn Jahren Versuchen mit REV eingeführt [102]): *Der Kanton sorgt dafür, dass … offengelegt werden: a. der Quellcode der Software des Systems …* [24] Das Beispiel Estland zeigt, dass nicht zwingend der gesamte Quellcode offengelegt wird. [49]

Fehlerfreiheit lässt sich leider auch durch eine Veröffentlichung des Quellcodes nicht garantieren. So wurde in einem Bericht der Firma Synopsis von 2020 festgehalten, dass 91 % der *Open-Source*-Komponenten, die in 99 % der kommerziellen Software Verwendung finden, Code enthalten, der überholt ist und als nicht mehr sicher gilt. [103, 79] An dieser Stelle die Anmerkung, dass eine Veröffentlichung des Quellcodes nicht das Gleiche ist wie, den Quellcode unter eine *Open-Source*-Lizenz zu stellen.

Eine Veröffentlichung des Quellcodes dürfte, wenn sich Fachleute an Hochschulen mit ihm befassen möchten und dafür nicht auf die Bewilligung eines Drittmittelantrags angewiesen sind, **einer Zertifizierung durch wenige Fachleute überlegen sein.** Dennoch **ist es nicht trivial, Quellcode nachzuvollziehen.** Allein der Code, der auf den Wahlservern in Estland läuft, umfasst 17 000 Zeilen und enthält viele Abhängigkeiten von externer Software. [104, S. 32 ff.] [49] Die Firma Cybernetica schätzt den Aufwand, eine App für Android und iOS zu entwickeln, auf zwischen 8 000 und 11 000 Personenstunden. [65] Der Quellcode des norwegischen REV-Systems, eines Systems, an dessen Bau wie beim System der Schweizerischen Post die Firma Scytl beteiligt war

[13] Bitweise Entweder-oder-Verknüpfung, also 0 XOR 0 = 0, 0 XOR 1 = 1, 1 XOR 0 = 1, 1 XOR 1 = 0. Beispiel: `00001101` XOR `10101010` = `10100111` (verknüpft werden Bits, die an der gleichen Position stehen).

[14] Ein Kongruenzgenerator erzeugt nach einem bestimmten Verfahren Zahlen, deren Verteilung zufällig aussieht.

[86] und das ebenfalls auf dem Austausch von Codes zwischen Wähler und Wahl-Server basierte, umfasste 211 500 Zeilen Code [105].

Davon ab **ist es mühsam, Quellcode nachzuvollziehen, wenn** – dies wird in [106] beanstandet – **die Dokumentation zu wünschen übrig lässt.**

4.3.5 Funktionelle Fehler im Code *(bugs)*

Ariane 5 (1996), Y2k (1. Januar 2000), Knight Capital (2012), Boeing 737 max (ab 2018): die Liste der Softwarefehler, die es in die Schlagzeilen geschafft haben, weil mit ihnen Millionen- oder Milliardenschäden verbunden waren, ist lang.

Ondrisek und Purgathofer geben zu bedenken: ***Dem Stand der Technik entsprechend ist nichttriviale Software … niemals hundertprozentig fehlerfrei.*** *Diese Einsicht zählt zu den wenigen von allen anerkannten Wahrheiten unserer Branche. In komplexer Software werden immer Fehler sein – unbeabsichtigt oder beabsichtigt –, die niemals gefunden werden. Hierbei ist zu bedenken, dass nicht-trivial fast schon kein ausreichender Begriff mehr ist, um die Komplexität moderner Systeme zu beschreiben; um nur ein paar der möglichen Fehlerquellen anzusprechen, wären da außer dem Sourcecode … die verwendeten Code-Bibliotheken … das Betriebssystem … das Internet als Übertragungskanal selbst.* [79]

Man könnte meinen, dass ein entdeckter Defekt nur noch behoben zu werden braucht. 2019 kam allerdings heraus, dass die Korrektur einer Lücke im System der Post, die von Forschern der Berner Fachhochschule bereits 2017 entdeckt und gemeldet worden war, nicht vollständig umgesetzt worden war. [61]

4.4 Logik

4.4.1 Zusammenspiel mehrerer Risiken

Mit einer Vielzahl von Angriffsszenarien korrespondiert eine Vielzahl von Vorkehrungen gegen Angriffe. So ist in [107] von *diverse[n] Barrieren … die eine Manipulation fast unmöglich machen,* die Rede.

Interessant wird es, wenn man sich fragt, wie all die Sicherheitsvorkehrungen zusammenspielen. Droz hält fest: *Es genügt, die schwächsten Glieder der Sicherheit zu analysieren, um das Risiko zu beurteilen.* [85] Simons und Jones weisen darauf hin: *Most complex software systems have an abundance of vulnerabilities, with attackers needing to exploit just one.* [108] **Sicherheit ist also wie eine Kette: Maßgeblich ist das schwächste Glied.**

4.4.2 Zur Natur wissenschaftlicher Erkenntnis

Aus Beobachtungen lassen sich induktiv Naturgesetze verallgemeinern, dachten Naturwissenschaftler jahrhundertelang – bis Einstein zeigte, dass Newtons Gravitationsgesetz, das sich in der Himmelsmechanik hervorragend bewährt hatte (die Vorhersage der Planeten Uranus, Neptun, Pluto ermöglicht hatte), lediglich einen Spezialfall korrekt darstellt, nämlich nicht zu große Massen bei Geschwindigkeiten deutlich kleiner als der Lichtgeschwindigkeit.

Angesichts dieses Versagens der Induktion **kann wissenschaftliche Erkenntnis,** wie Popper gezeigt hat [109], **nur gewonnen werden, indem man Hypothesen aufstellt** (nicht irgendwelche Hypothesen, sondern Hypothesen, die nützlich sind) **und sich bemüht, diese zu falsifizieren.** Lässt sich die Hypothese falsifizieren – **ein einziges Gegenbeispiel genügt** –, so beschreibt sie zumindest diesen Fall nicht korrekt; die Hypothese ist dann in ihrer Allgemeingültigkeit nicht haltbar, sie muss so verfeinert werden, dass der Fall, in dem sie versagt hat, anders, nämlich korrekt beschrieben wird. Besteht die Hypothese den Test – Naturwissenschaftler nennen ihn ›Experiment‹; tatsächlich ist jedes Experiment eine Frage an die Natur –, ist ihre Korrektheit damit nicht etwa bewiesen, es ist lediglich ihre Nützlichkeit untermauert.

Poppers Erkenntnis hat weitreichende Auswirkungen: **Man kann durch *blackbox testing*, d. h. Testen des Verhaltens der Software ohne Einblick in den Quellcode, nicht beweisen, dass die Software korrekt funktioniert – man kann lediglich zeigen, dass sie für bestimmte Eingaben korrekt funktioniert.** Durch intensives Testen kann man plausibel machen, dass Software korrekt funktioniert. Wie funktioniert das? Der Tester unterteilt den Testraum willkürlich in Äquivalenzklassen – z. B. Randfälle, kleine Eingaben, große Eingaben, widersinnige Eingaben – und deckt beim Testen sie alle ab. Hinter den Äquivalenzklassen steht die Annahme, dass sich die Software für alle Eingaben der – darum dieser Begriff – Äquivalenzklasse gleich, nämlich entweder richtig oder falsch, verhält.

Softwaretests können vom Arbeitsaufwand her nicht beliebig umfangreich werden. **Man muss** also **damit rechnen, dass einige Fehler, die in komplexen Situationen auftreten, durch *blackbox testing* nicht gefunden werden.** Ob die mangelhafte Korrektur, die in der linken Spalte angesprochen wurde, aufgefallen wäre, wenn der Quellcode nicht öffentlich einsehbar gewesen wäre, ist jedenfalls fraglich.

Die Grenzen der Aussagekraft von *blackbox testing* gelten insbesondere für den Test auf Schadverhalten. Ein Wahlcomputer kann sich unauffällig verhalten, wenn er am ›falschen‹ Tag betrieben wird (Wahlen finden in Deutschland sonntags statt). Ein Wahlcomputer kann sich unauffällig verhalten, wenn er ›zu kurz‹ in Betrieb war (in Deutschland öffnen die Wahllokale von 8 bis 18 Uhr). Ein Wahlcomputer kann sich unauffällig verhalten, wenn ›zu wenige‹ Stimmen erfasst wurden (in Deutschland werden in einem Wahllokal typischerweise tausend Stimmen erfasst). Ein Wahlcomputer kann sich unauffällig verhalten, wenn die zeitlichen Abstände zwischen den Stimmabgaben ›zu kurz‹ sind. All dies würde auf eine Testwahl hindeuten.[15] – Dennoch kann der Wahlcomputer über ›Zusatzfunktionen‹ **(Hintertüren)** verfügen, die sich z. B. durch das Drücken unsichtbarer Tasten (Berührbildschirm) oder durch das Drücken von Tasten in einer bestimmten Reihenfolge (*Knock*-Attacke [110, 16]) auslösen lassen, oder dadurch, dass ein Dutzend Wähler nacheinander in einer vereinbarten Reihenfolge für bestimmte Splitterparteien stimmt[16]. Weitere Strategien bzw. Angriffspunkte skizzieren Feldman et al. [110].

In den USA wurde in der Software eines Wahlcomputers eine *Knock*-Vorrichtung entdeckt: *According to Harris, a manipulation technique she found in Diebold's AccuVote central vote tabulator is able to read totals from an untraceable bogus vote set within its software. ›By entering a two-digit code in a hidden location, a second set of votes is created; and this set of votes can be changed in a matter of seconds, so that it no longer matches the correct votes,‹ she has said.* [91, 111] Hätte sich diese Präparation durch intensives *blackbox testing* aufdecken lassen? Das ist sehr unwahrscheinlich. Simons und Jones halten fest: *In general, no amount of testing can be relied on to reveal the presence of a back door.* [108]

Inwieweit sind die Bedenken im Hinblick auf die Integrität von Wahlcomputern auf REV übertragbar? Estlands System funktionierte bis 2013, vor der individuellen Verifizierbarkeit, nicht anders als ein solcher Wahlcomputer: Stimme abgeben und hoffen, dass bei Erfassung und Zählung alles seine Richtigkeit hat.

Wegen der zahlreichen Manipulationsmöglichkeiten wird die Sicherheit von Wahlcomputern mittlerweile vom Ende her aufgezäumt: Neuere Wahlcomputer produzieren einen Ausdruck der Stimme, die der Wähler abgegeben hat, den der Wähler überprüfen kann (*voter-verified paper audit trail,* VVPAT); die Ausdrucke werden für Nachzählungen aufgehoben, die bei statistischem Vorgehen Aussagen über die Korrektheit des Wahlergebnisses erlauben (*risk-limiting audits,* RLAs) [110, 112].

Allerdings müssen die Wähler bei VVPAT auch mitspielen (können): *Eine Studie der Universität Michigan zeigte … dass nur etwa 40 % der Testpersonen ihren ausgedruckten Stimmzettel auch überprüften, nur knapp 6 % taten das so gründlich, dass sie darauf Fehler entdeckten. In manchen Fällen wird das Resultat als QR-Code abgebildet, was eine Kontrolle ohnehin unmöglich macht.* [113] Volkamer et al. geben in diesem Zusammenhang zu bedenken: *Es ist aus soziologischer Sicht problematisch, dem Wähler zu erklären, dass die Korrektheit und Integrität der durchgeführten Wahl davon abhängt, dass die Wähler von der individuellen Verifizierbarkeit Gebrauch machen.* [74]

Stand 2020 arbeiten in den USA nur noch 0,5 % der gesetzgebenden Körperschaften mit Wahlcomputern ohne VVPAT. [114] Ob es in einer betriebswirtschaftlich durchdrungenen Welt den Steuerzahlern vermittelbar ist, dass viel Geld ausgegeben wird für Nachzählungen, die, wenn sie vorgeschrieben sind und ernsthaft betrieben werden, genau deswegen, weil es sie gibt, wahrscheinlich nie jemals einen Grund zur Beanstandung der Wahl zutage fördern werden, steht auf einem anderen Blatt. Man muss an dieser Stelle aber sehen: Durch RLAs spart man viel Geld, das sonst in Bemühungen zur Erhöhung der Sicherheit der Wahlcomputer gesteckt werden müsste.

Durch REV, warnt der CCC-CH, werden Nachzählungen faktisch abgeschafft. [43] Das erklärt die intensiven Bemühungen sowohl in Estland als auch in der Schweiz um Verifizierbarkeit.

Die Grenzen der Aussagekraft von *blackbox testing* gelten auch für Intrusionstests. Heiberg wird in der NZZ wiedergegeben, *die Beobachter [Springall et al.] hätten nicht beweisen können, dass das zentrale System [in Estland] gehackt werden könnte.* [77] Der Guardian berichtet aus Indien: *In 2017, the Election Commission invited parties to prove they could hack the voting machines – none were able to do so.* [115] Wenn ein Einbruch *einem* Angreifer nicht gelingt, lässt sich daraus aber keine Aussage ableiten, dass dies *keinem* Angreifer gelingen könne. Droz gibt zu bedenken, dass

[15] Bekanntlich hatten die Pkws bestimmter Hersteller erkannt, wenn sie einem Abgastest unterzogen wurden, und verhielten sich, was den Ausstoß von Schadstoffen angeht, anders als auf der Straße.

[16] Die ersten Bits, die durch das Wahlverhalten übermittelt werden, könnten die ›Zusatzfunktion‹ triggern, die letzten zum Programmieren des gewünschten Ergebnissen dienen. Splitterparteien zu wählen, erhöht den Informationswert (Neuigkeitswert) der Bits.

der Angegriffene von dem Angriff schlicht nichts gemerkt haben könne. [85, S. 18] Eine weitere mögliche Erklärung: Die konkrete Wahl war für Angreifer nicht interessant. [116] Überhaupt: Warum sollten Angreifer die Einführung von REV durch Angriffe torpedieren, anstatt zu warten, bis REV in mehreren Ländern, womöglich flächendeckend, etabliert ist? Anfangs wird bestimmt sorgfältiger hingeschaut als später, wenn REV selbstverständlich geworden ist.

Die NZZ gibt zu bedenken: *Alles, was es … braucht, ist ein unerwartetes oder knappes Resultat. Wenn es dazu kommt, liegt die Beweislast für dessen Korrektheit bei den Behörden. Und diese werden lediglich sagen können, dass es keine Hinweise auf einen Angriff gebe.* [117] Das trifft es. **Man kann** nämlich **nicht beweisen, dass ein System *nicht* gehackt worden ist – man kann lediglich beweisen, *dass* ein System gehackt worden ist.** Marques bringt die wissenschaftstheoretischen Überlegungen, die wir angestellt haben, auf den Punkt: *Es gibt schlicht keine Möglichkeit, zu garantieren, dass das System nicht manipuliert wird.* [118]

4.4.3 Rekursion

Kritische Prozesse werden in Estland auf Video aufgezeichnet; diese offiziellen Videoaufzeichnungen haben Springall et al. in ihre Sicherheitsanalyse einbezogen. Wir sprechen die Videoaufzeichnungen an, weil sie ein anschauliches Beispiel für **das Problem der Rekursion** darstellen. Wie man es aus Filmen über raffinierte Banküberfälle kennt, stellt sich bei Videoaufzeichnungen die Frage nach der Authentizität, insbesondere der Vollständigkeit; berühmt ist das Bild des Tresorraums, in dem scheinbar nichts passiert. Man bräuchte Aufzeichnungen, die die Authentizität (insbesondere die Vollständigkeit) der offiziellen Videoaufzeichnungen belegen. Weiters bräuchte man Aufzeichnungen, die die Authentizität (insbesondere die Vollständigkeit) der Aufzeichnungen, die die Authentizität (insbesondere die Vollständigkeit) der offiziellen Videoaufzeichnungen belegen. Und so weiter, und so fort. Wir werden dem Problem der Rekursion noch in anderen Zusammenhängen begegnen.

4.4.4 Beweise und die Annahmen, auf denen sie beruhen

Wenn der Quellcode öffentlich zugänglich ist und genügend viele Fachleute ihn anschauen, bleiben Hintertüren schwerlich verborgen. Tatsächlich **lassen sich durch Softwareinspektion bzw. *whitebox testing* am Quellcode Eigenschaften der Software, z. B. Korrektheit, beweisen.** Solche Beweise sind aufwendig – die Post liefert dazu ein 134-seitiges Dokument [67] –, aber möglich; sie sind aber selbst für Informatiker nicht ohne Weiteres zu verstehen. Die Schweizerische Post schreibt: *This report demonstrates that the protocol provides strong security guarantees under a challenging threat model.* [67] Man beachte: Dem Beweis liegt ein Bedrohungsszenario zugrunde. Die Annahmen lauten: *Die folgenden Systemteilnehmenden dürfen als vertrauenswürdig gelten: Setup-Komponente; Druckkomponente; eine von vier Kontrollkomponenten pro Gruppe* [24]. *Wenn* diese Annahmen als erfüllt gelten dürfen, *dann* kann die Post vollständige Verifizierbarkeit und die Vertraulichkeit der Stimme garantieren (wir setzen voraus, dass ihr Beweis keine Fehler enthält). Ist aber auch nur eine dieser Annahmen nicht erfüllt, wird sich die Garantie schon nicht mehr aufrechterhalten lassen (andernfalls hätte die Post dem Beweis umfangreichere Annahmen zugrunde gelegt als nötig). **Ein Beweis ist** also **nur so gut wie die Annahmen, die ihm zugrunde liegen.**

Ähnlich ist es zu sehen, wenn die Post wirbt: *Alle Informationen, die während der Stimmabgabe übermittelt werden, sind anonymisiert und mit einer End-zu-End-Verschlüsselung geschützt. Nur die kantonalen Wahlbehörden können das Resultat in der elektronischen Urne auswerten. Rückschlüsse von der Stimme auf den/die Stimmberechtigte/n sind an keiner Stelle möglich.* [119] Entscheidend ist, dass die Information, welchem Wähler welche Codeliste zugesandt wurde, in den Druckzentren verbleibt. Der CCC-CH gibt zu bedenken, dass Geheimdienstkomplexe einer Großmacht wie den USA in der Lage sind, die Computer bzw. Drucker in den kantonalen Druckzentren zu unterwandern. [43]

Ein vernünftiger Gutachter muss manche Annahmen einfach als gültig hinnehmen – wie ein Statiker auch nicht erwarten kann, dafür bezahlt zu werden, dass er untersucht, ob der Untergrund, auf dem das Ulmer Münster steht, dieses Gewicht wirklich tragen kann. Deswegen ist ein Angriff auf die Fundamente verlockend. Die New York Times berichtet von einem solchen Angriff: *Classified N.S.A. memos appear to confirm that the fatal weakness, discovered by two Microsoft cryptographers in 2007, was engineered by the agency. The N.S.A. wrote the standard.* [120]

Wir betrachten einige Zitate aus der NZZ: *… hat der Bundesrat … noch stärkere Sicherheitsanforderungen zum Schutz vor Manipulationen … beschlossen* [121] – *individuelle Verifizierbarkeit … bedeutet, dass jeder Bür-*

ger überprüfen kann, ob seine Stimme eingetroffen und korrekt gezählt worden ist; somit kann er allfällige Manipulationsversuche erkennen [62] – *... wenn ein System mit universeller Verifizierbarkeit zur Verfügung steht ... haben die Stimmenden und die Wahlbehörden jederzeit die volle Kontrolle ... und können Manipulationen zweifelsfrei erkennen* [13]. In den Formulierungen schwingt die Konnotation mit, gemeint seien alle Manipulationen. Jeder Manipulation muss aber ein bestimmtes Angriffsszenario zugrunde liegen. Gegen das Konzept der universellen Verifizierbarkeit z. B. ließe sich einwenden: *Selbst ein lückenloses Protokoll auf dem Server kann Stimmen, welche schon manipuliert auf dem Server ankamen (oder unterdrückt wurden), nicht als manipuliert erkennen.* [122] **Da jeder Manipulation denknotwendig ein Angriffsszenario zugrunde liegt, folgt, dass es unmöglich ist, ein System gegen jede Manipulation zu wappnen; denn dafür müsste man alle Manipulationsmöglichkeiten a priori kennen.** Deswegen ist der unbestimmte Plural *Manipulationen,* egal ob er mit oder ohne ein Adjektiv davor verwendet wird, problematisch.

Durch Softwareinspektion bzw. *whitebox testing* lassen sich, wie wir gesehen haben, einige Grenzen von *blackbox testing* überwinden. **Doch was,** fragt Ondrisek, **wenn Quellcode, der alle Reviews übersteht, von einem bösartigen Compiler compiliert wird?** Das Ergebnis ist ein manipuliertes Programm, obwohl der Quellcode authentisch ist. [16] Ein bösartiger Compiler lässt sich mit erstaunlich wenig Aufwand konstruieren. [123] Das Ganze lässt sich eine Ebene weiter denken: Was, wenn der Quellcode des verwendeten Compilers integer ist, dieser Quellcode aber von einem bösartigen Compiler compiliert wurde? Wir begegnen hier erneut dem Problem der Rekursion.

4.5 Schutzmittel

4.5.1 Beschränkung des Zugriffs

Das kleine Einmaleins beim IT-Schutz besteht in der **Aufteilung der Zuständigkeiten und Verantwortlichkeiten.** Gritzalis formuliert als Entwurfsprinzip von REV-Systemen: *Only the ab-so-lu-tely necessary entities should have logical and/or physical access to the voting system. Adequate segregation of duties must be enforced between the authorised personnel.* [124] Die Bundeskanzlei stellt die Anforderung: *Es darf kein logischer Zugriff auf oder physischer Zugang zu vertrauenswürdigen Komponenten oder Datenträgern mit kritischen Daten möglich sein, ohne dass eine andere Person dies bemerkt, beispielsweise indem sie für die Gewährung des Zugriffs mitwirken muss (strenges Vieraugenprinzip).* [24] Springall et al. beobachteten 2013 in Estland, dass, obwohl für Updates/Backups das Vieraugenprinzip vorgeschrieben war, ein einzelner Mitarbeiter diese Aufgabe ausführte. Damit hing die Sicherheit der Wahl von der Integrität eines einzigen Mitarbeiters ab.

Ein bekanntes Mittel, um den Zugriff nichtautorisierter Personen zu verhindern, besteht in der Einrichtung eines **Passwortregimes**. Dann muss man dieses aber auch ernsthaft betreiben. Springall et al. beobachteten, dass Wahlmitarbeiter für die Videoaufzeichnung sichtbar Passwörter eintippten, darunter *Root*-Passwörter der Wahlserver, und sich der Videoaufzeichnung die Log-in-Daten für das WLAN der Wahlmitarbeiter entnehmen ließen. [49] Simons und Jones berichten von einem Intrusionstest am REV-System von Washington D.C.: *From the start, his team [Halderman] had control of the network infrastructure for the pilot project. The team used the default master password from the owner's manuals, which had not been changed, for the routers and switches, thereby gaining control of the infrastructure ...* [108]

Von Dokumenten kennt man es, dass nicht einfach Zugriff gewährt wird oder nicht, sondern **Zugriff in einer festgelegten Tiefe,** z. B. auf den Stufen VS-Vertraulich, Geheim, Streng geheim. Analog dazu sind auf dem Rechner nicht mit jedem Benutzerkonto dieselben Rechte verbunden. Administratoren besitzen die umfangreichsten Rechte. Springall et al. beobachteten, dass sich die Wahlmitarbeiter als *Root* einloggten; dies widerspreche der guten fachlichen Praxis, weil es den Schutz gegen menschliche Fehlleistungen senkt und viele Angriffe vereinfacht. [49]

Zur Beschränkung des Zugriffs gehört das **Entziehen der Zugriffsrechte** bzw. das **Verunmöglichen des Zugriffs.** In der Dokumentation zu Estlands REV-System [44] liest man: *At the end of the process, the private key is deactivated* und *Thereafter [Bekanntgabe des finalen Ergebnisses der Wahl] the private key is exterminated, and the personalised and encrypted votes become unusable*. Ob die Verben *deactivate, exterminate* beim informatischen Laien die richtigen Assoziationen auslösen? Besser ist die deutsche Übersetzung in [3, S. 64]: *In Estland wird der private Schlüssel nach Ablauf der Zeit für Wahleinsprüche zerstört.* Wie – ob die Speicherstelle, die den Schlüssel enthält, x-fach mit zufälligen Bitmustern überschrieben wird oder das Hardware-Sicherheitsmodul unter KSK-Geleitschutz zu einem Hochofen eskortiert und dort terminiert wird –, soll uns hier nicht interessieren.

4.5.2 Einbeziehung eines weiteren Kanals

Die Schweizer Wähler, auch die Auslandschweizer, erhalten die Codelisten mit der Post. Manche halten das für unpraktikabel und fordern, alle Dokumente sollten online versandt werden. [125] Die NZZ berichtete 2018, eine Expertengruppe erarbeite ein Konzept dafür, wie diese sogenannte Dematerialisierung in der Praxis umgesetzt werden könne, gibt aber zu bedenken, hier drohe sich die Katze in den Schwanz zu beißen: Je stärker die Stimmabgabe des Bürgers dematerialisiert werde, desto schwieriger werde es, die Korrektheit der Stimmabgabe zu überprüfen. [126] Appel bringt auf den Punkt, warum die Codes per Post versendet werden: *If the Swiss Post e-voting system might possibly be secure, it's only because of the out-of-band communication channel that is completely out of reach of the voter's computer. That is: a sheet of paper sent through the mail, to the voter.* [127] Die Zwei-Faktor-Authentifizierung beim Onlinebanking hat denselben Hintergrund: **Ein Angreifer müsste beide Kanäle kontrollieren; das erschwert Angriffe erheblich.**

Der weitere Kanal kann auch seriell einbezogen werden: **wenn,** wie in Estland und der Schweiz, **Daten zur Weiterverarbeitung mit einem Medium auf einen nicht ans Internet angeschlossenen Rechner übertragen werden *(air gap).***

4.5.3 Zerlegung von Geheimnissen *(secret sharing)*

Der Guardian berichtete aus Großbritannien: *Swindon's e-votes are held in a data centre in Slough. The file is encrypted, and holds only the vote and a 10-digit personal identification number (Pin), randomly generated for this election – voters used it to log on to their chosen system. The file linking Pins to voters' names and addresses is held in Swindon.* [34]. Es ging offensichtlich darum, **die Verknüpfung von Daten** zu **verhindern.**

Ein Geheimnis, das schwer wiegt, ist **das Geheimnis des Schlüssels zum Entschlüsseln der abgegebenen Stimmen;** besonders schwer wiegt dieses Geheimnis, weil REV nicht einen Tag lang, sondern tagelang, wochenlang angeboten wird. Um zu verhindern, dass Stimmen vorzeitig entschlüsselt werden [14] – bereits dieser Informationsvorsprung würde eine Manipulation der Wahl ermöglichen, und zwar durch taktisches Wählen mit einem wegen dieses Wissens höheren Stimmengewicht –, **wird** dieses Geheimnis in Estland wie in der Schweiz **auf mehrere Mitglieder der Wahlkommission verteilt.** [48, 14]

Wätjen illustriert das Vorgehen wie folgt: *Beim secret sharing wird ein Geheimnis auf mehrere Personen einer Gruppe verteilt. Keiner von ihnen kennt das gesamte Geheimnis, sondern nur einen Teil davon. Aus diesen Teilen (shares) kann dann das vollständige Geheimnis zurückgewonnen werden. Eine typische … Anwendung ist eine Karte, die den Weg zu einem Piratenschatz beschreibt. Sie wird … in einzelne Stücke zerrissen und … verteilt, sodass sich der Schatz nur von allen gemeinsam finden lässt.* [128] *Verteilen* ist ein ungünstiges Wort, weil es an das Verteilen von Kopien an mehrere Personen erinnert. *Teilen* ist ebenfalls ungünstig, weil etwas Immaterielles zu teilen bedeutet, dass jeder im Besitz der ganzen Information ist. *Zerlegen* trifft es besser.

Mathematik erlaubt es, die Teil-Geheimnisse so anzulegen, dass sich das ursprüngliche Geheimnis selbst bei Ausfall eines oder mehrerer Geheimnisträger rekonstruieren lässt *(threshold secret sharing).* Auch dies lässt sich mit einer klassischen Analogie illustrieren: Pergamente, die jedes nur einen Teil der Informationen enthalten, werden übereinandergelegt und gegens Licht gehalten, wie in ›Tim und Struppi: Das Geheimnis der Einhorn‹.

Technisch passiert im System der Post übrigens genau das Gegenteil: Der geheime Schlüssel wird nicht aus den Teilen, die die Mitglieder der Wahlkommission halten, zusammengesetzt, sondern das Schlüsselpaar öffentlicher/geheimer Schlüssel wird aus den Passwörtern dieser Personen abgeleitet. [14]

4.5.4 Verschlüsselung

Kann man schützenswerte Informationen sicher vor neugierigen Augen über das Internet versenden? Im Guardian findet sich die Einschätzung: *The internet has never been a very safe way to send any kind of information.* [129] Es bleibt offen, ob der Autor noch nie etwas von Verschlüsselung gehört hat oder ob er meint, dass sich jede Verschlüsselung von einem Hacker, der schnell tippen kann, nach wenigen Minuten brechen lasse. Dem ist nicht so. **Verschlüsselung ist, sofern bestimmte Voraussetzungen erfüllt sind, sicher.**

Wie darf sich der Laie Verschlüsselung vorstellen? Purgathofer hält den **Vergleich** mit der **Verwendung eines Briefumschlags** für ausreichend. [130]

Seit Ende der 70er-Jahre sind **Verschlüsselung und Entschlüsselung mit zwei Schlüsseln, von denen einer veröffentlicht wird, ein zentrales Thema. *Public-Key*-Kryptografie** funktioniert wie folgt: Wenn Anja Bruno eine Nachricht schicken möchte, bringt sie Brunos öffentlichen Schlüssel in Erfah-

rung, verschlüsselt die Nachricht damit und sendet das Kryptogramm. Mit seinem privaten = geheimen Schlüssel, den nur er kennt, kann Bruno und nur Bruno die Nachricht, die mit seinem öffentlichen Schlüssel verschlüsselt wurde, entschlüsseln. **Weil unterschiedliche Schlüssel benutzt werden, wird auch von asymmetrischer[17] Verschlüsselung gesprochen.**

Von Bedeutung ist unserer Meinung nach, unter welchen Voraussetzungen Verschlüsselung sicher ist, also **wie lange ein Angreifer bräuchte, um die Verschlüsselung mit Rechengewalt *(brute force)*** zu brechen, mit heutiger Technik und in einer vernünftigen Zeitspanne, nach der die entschlüsselte Information noch einen Wert hat.[18]

Welcher Zusammenhang zwischen der Länge des Schlüssels und der Zeit zum Brechen der Verschlüsselung besteht, hängt davon ab, welches Verschlüsselungsverfahren genau zum Einsatz kommt. In Estland wurden die Stimmen von 2005 bis 2017 mit dem RSA-Verfahren (1978, [131]) verschlüsselt [81, 50]; die Id des gewählten Kandidaten wurde zusammen mit *(padding)* einer 160 Bit breiten Zufallszahl r mit dem öffentlichen Schlüssel *PK,* Schlüssellänge 2048 Bits, RSA-verschlüsselt. [49] Die Zufallszahl r verhindert, dass, wenn zwei Wähler für denselben Kandidaten stimmen, die Kryptogramme identisch ausfallen [44]; wenn das so wäre, könnte ein Angreifer ein Mal für jeden Kandidaten stimmen und erhielte dadurch einen vollständigen Satz Kryptogramme, mit denen er jede abgegebene Stimme, die von nun an in seine Hände gelangt, abgleichen könnte – mit der Vertraulichkeit der Stimme wäre es vorbei.

Im System der Schweizerischen Post werden die Stimmen mit dem ElGamal-Verfahren (1985, [132]) verschlüsselt, in Estland seit 2017 ebenfalls [50, 46]. Auch hier wird eine Zufallszahl r erzeugt, sie tritt jedoch in einer anderen Bedeutung auf: als Parameter für das ElGamal-Verfahren. [46, 44] Das Ziel ist das gleiche: sicherstellen, dass sich die Kryptogramme aller abgegebenen Stimmen voneinander unterscheiden.

Missverständlich ist folgende Beschreibung in der Dokumentation zu Estlands System: *NB! The randomness [r] used to encrypt one vote can be used to decrypt only that vote. To decrypt several different votes, the private component of the vote secrecy key pair is needed.* [46] Tatsächlich lässt sich das Kryptogramm K auch bei Kenntnis von r nicht entschlüsseln; vielmehr berechnet die Verifikations-App für jeden Kandidaten c das Krytogramm K', das sich ergeben hätte, wenn der Wähler für c gestimmt hätte und diese Stimme mit dem Parameter r verschlüsselt worden wäre, vergleicht K' mit K und gibt bei Übereinstimmung den Namen dieses Kandidaten aus. Es wurde also nichts entschlüsselt, es wurde stattdessen jede denkbare Stimmabgabe mit dem Parameter r verschlüsselt und das entstandene Kryptogramm mit dem zu bestätigenden Kryptogramm verglichen.

In der Schweiz erhält der Wähler für jeden Kandidaten, den er gewählt hat (Kumulieren/Panaschieren!), einen Bestätigungscode. Man fragt sich, woher das REV-System wissen soll, welche Kandidaten der Wähler gewählt hat, wenn dem System die Auswahl der Kandidaten doch verschüsselt zugeht und das Entschüsseln, wie es immer heißt, erst am Ende der Wahl und nur unter Mitwirkung mehrerer Schüsselträger durchgeführt werden kann. Die Lösung: Das System errechnet die Bestätigungscodes auf der Basis des ihm übermittelten Kryptogramms. Das ist möglich, wenn die Stimme mit einem Verschüsselungsverfahren verschlüsselt wurde, welches homomorph ist, d. h. die mathematische Gestalt erhält; bei RSA bzw. ElGamal ist das der Fall. Homomorphe Verschüsselung wird z. B. in [133] dargestellt.

Die Sicherheit des RSA-Verfahrens beruht darauf, dass es für eine gegebene Zahl n, die das Produkt zweier unbekannter großer Primzahlen p und q ist, praktisch unmöglich ist, p und q zu ermitteln. [128] Die Sicherheit des ElGamal-Verfahrens beruht auf der Schwierigkeit, den diskreten Logarithmus einer sehr großen Zahl y modulo (Rechnen mit Kongruenzen/Restklassen) einer sehr großen Primzahl p in vernünftiger Zeit zu bestimmen, also aus gegebenem $y = g^x \bmod p$ den Exponenten x zu bestimmen. [128]

Wätjen rechnet vor, dass, um eine 512-Bit-Verschlüsselung durch Berechnung des diskreten Logarithmus zu berechnen, der – Stand 2018 – schnellste Supercomputer 176 Sekunden, bei 1024 Bit 42 Jahre, bei 2048 Bit 50 Milliarden Jahre bräuchte. [128, S. 12 f.] Das ist gemeint, wenn es heißt, es sei *mathematically impossible* [134], zu entschlüsseln, für wen der Wähler gestimmt hat. Rivest, einer der Autoren des RSA-Verfahrens, verschüsselte 1977 einen kurzen Text mit einer Zahl n von 428 Bits (129 Dezimalstellen) und veröffentlichte ihn als Rätsel, mit einem Lö-

[17] und nicht etwa *asynchroner,* wie es in [17] heißt

[18] Im Falle der Enigma mussten die Nachrichten binnen weniger Stunden entschlüsselt werden können. Wer in einem Staat lebt, in dem er davon ausgehen darf, dass Sippenhaft nicht in Erwägung gezogen werden wird, kann die vernünftige Zeitspanne nach unten abschätzen durch die Lebenszeit, die er noch zu erwarten hat.

sungsanreiz von einigen Dollars. Er hielt eine Zeit von 40 Quadrillionen ($40 \cdot 10^{24}$) Jahren für notwendig, um den Text zu dechiffrieren. [128, S. 78] Es ist also nicht mathematisch unmöglich; wenn nur die gegenwärtige Mathematik zur Verfügung steht, scheitert es aber an der Lebenszeit der Beteiligten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt ab 2023 RSA-Schlüssellängen von 3000 Bits. [135] Die Frist deutet darauf hin, **dass kürzere Schlüssel nicht mehr sicher sind.** Dafür gibt es zwei Gründe: **Zum einen nimmt die Rechenleistung zu;** das Außerkrafttreten des Mooreschen ›Gesetzes‹, wenn die Miniaturisierung an physikalische Grenzen stößt, wurde jüngst durch technische Durchbrüche bei der EUV-Lithografie erneut in die Zukunft verschoben. Darüber hinaus lässt sich Rechenarbeit auf zahlreiche Rechner verteilen.

Zum anderen werden in der Mathematik noch Fortschritte erzielt. So wurde Rivests 1977 für absolut sicher gehaltenes Kryptogramm bereits 1994 dechiffriert. [128] Die Erfinder des RSA-Verfahrens schrieben selbst: *Since no techniques exist to prove that an encryption scheme is secure, the only test available is to see whether anyone can think of a way to break it.* [131] Wir dürfen hoffen, dass an Kryptografie hinreichend viele Personen forschen und von denen, die Durchbrüche erzielen, wenigstens einige bei einem Arbeitgeber beschäftigt sind, der es ihnen erlaubt, ihre Ergebnisse zu veröffentlichen.[19,20] Es ist daher vernünftig, anzunehmen: ***Once the method has withstood all attacks for a sufficient length of time it may be used with a reasonable amount of confidence.*** [131]

Wenn eine Verschlüsselung, die heutzutage sicher ist, in naher Zukunft womöglich doch gebrochen werden kann, dann sind im Hinblick auf die Verschlüsselung der Stimmen von Wählern besondere Anforderungen zu stellen. Es genügt nicht, wenn der Schüssel zum Entschlüsseln der Stimmen nach der Wahl sicher entsorgt wird, bei der Wahl der Länge des Schlüssels muss der Fall berücksichtigt werden, dass Angreifer die Kryptogramme der Stimmen abfangen, d. h. sie beim Durchleiten kopieren, um sie zu entschlüsseln, wenn dies eines Tages technisch möglich ist. Gibson et al. fassen das wie folgt zusammen: ***Everlasting privacy is a privacy property*** *that withstands the explosion of computational resources over time,* ***allowing votes to remain private even after the cryptographic parameters of their time can be easily brute-forced.*** [17] Warum die Information, für wen welcher Wähler gestimmt hat, auch Jahre nach der Wahl noch schützenswert ist, legen wir in Abschnitt 5.2.3 dar.

Übrigens ist auch beim Thema Verschüsselung Sicherheit durch Geheimhaltung eine schlechte Idee. Beutelspacher et al. halten fest: ***Man muss grundsätzlich davon ausgehen, dass sowohl Ver- als auch Entschlüsselungsfunktion bekannt sind (Kerckhoffsches Prinzip).*** [136, S. 6] Schon bei der Enigma war es nicht gelungen, den Algorithmus geheim zu halten.

4.5.5 Digitale Fingerabdrücke (*Hash*-Funktionen)

Wie ein Video durch ein Standbild repräsentiert werden kann, so kann ein digitaler Fingerabdruck – gemeint ist: ein Text fester Länge, ein Bild fester Größe – ein Dokument beliebiger Länge repräsentieren. Wenn der Fingerabdruck eine feste Größe hat, andererseits aber von beliebig langen und damit beliebig vielen verschiedenen Dokumenten ein Fingerabdruck dieser festen Länge berechnet werden kann, folgt, **dass manche Dokumente denselben Fingerabdruck besitzen.**

Die Raffinesse der ***Hash*-Funktion** $h(x)$, die den Fingerabdruck der Nachricht x berechnet, besteht darin, dass schon aus einer winzigen Änderung von x ein völlig anderer Fingerabdruck resultiert (Lawineneffekt). Dadurch wird es praktisch unmöglich, für den gegebenen Fingerabdruck $f = h(x)$ eine andere Nachricht y zu finden, die denselben Fingerabdruck besitzt, also $f = h(x) = h(y)$, sprich: die Nachricht zu fälschen. Details dazu finden sich auf [137].

Um die Authentizität einer Software zu überprüfen, kann man einen Fingerabdruck der Software berechnen und diesen mit einem an vertrauenswürdiger Stelle veröffentlichten Fingerabdruck vergleichen. Estland Wähler finden eine Anleitung zur Überprüfung der Wahl-App auf [47].

Was aber, wenn das Programm zur Berechnung digitaler Fingerabdrücke durch ein bösartiges Alter ego ersetzt wurde, das sich, angesetzt auf die Wahl-App, die Berechnung ›spart‹ und einfach behauptet, sie habe den bekannten Fingerabdruck? Ein bösartiges Fingerabdruck-Programm lässt sich mit sehr wenig Aufwand programmieren; es braucht nur ein paar Zeilen Code, die, je nachdem, von welcher Datei der Fingerabdruck berechnet werden soll, eine Unterscheidung vornehmen und Aufrufe ansonsten an das unter anderem Namen weggespeicherte integre Ori-

[19] GCHQ-Mitarbeiter Cocks hatte zwei Jahre eher dieselbe Idee wie Rivest, Shamir, Adleman (RSA). [128, S. 77]
[20] Im Falle der Enigma kam erst Jahrzehnte später ans Licht der Öffentlichkeit, dass die Verschlüsselung gebrochen worden war.

ginal weiterleiten. An der Dateigröße lässt sich ein bösartiges Fingerabdruck-Programm nicht zuverlässig erkennen. Und wenn es mit Sorgfalt gemacht ist, wird ein bösartiges Fingerabdruck-Programm auch Anfragen zu seinem eigenen Fingerabdruck manipulieren. Wir begegnen hier erneut dem Problem der Rekursion; Ondrisek illustriert sie wie folgt: *So finden wir uns vor einem Turm aus Schildkröten, jede auf dem Rücken der vorigen, ohne jemals einen Boden zu finden, der uns tatsächliche Sicherheit garantiert.* [79]

4.5.6 Digitale Signaturen

Wie kann man bei elektronischer Kommunikation sicher sein, dass der Absender ist, wer er zu sein behauptet (Authentifizierung), dass die abgegebene Stimme von dem Wähler kommt, der zur Abgabe der Stimme autorisiert wurde? Sind digitale Signaturen, wie die NZZ schreibt, *eine Art elektronischer Ausweis, der die Identifizierung der beteiligten Personen sicherstellt* [138]? Von einem Ausweis zu sprechen, ist sicherlich ungeeignet. Die Metapher der Unterschrift passt besser. Unterschriften, das weiß jeder, lassen sich aber fälschen, nachahmen (gegen eine Kopie der Unterschrift spricht, dass dann der Druck auf das Papier fehlt).

Wie funktioniert eine digitale Signatur? Die NZZ erklärt: *die digitale Unterschrift ... das heisst ein jedem Einzelnen unverwechselbar zugeteilter elektronischer Schlüssel. Der öffentliche Teil dieses Schlüssels wird dann in eine Art Telefonbuch aufgenommen – auch dieses kann elektronisch sein –, welches erlaubt, jeden Schweizer elektronisch eindeutig zu identifizieren.* [10] Es geht jedoch nicht um Identifizierung der Person, sondern um Authentifizierung eines Dokuments.

Wenn von einem *öffentlichen Teil* die Rede ist, assoziiert man zu Recht asymmetrische Kryptografie. Problematisch ist die Formulierung *zugeteilter elektronischer Schlüssel.* Man fragt sich: Wer teilt den Schlüssel zu? Kennt der Zuteiler den Schlüssel, genauer: den geheimen Teil, genauer: den geheimen Schlüssel des Schlüsselpaars (seine Existenz wird durch die Formulierung *der öffentliche Teil* angedeutet)?

Es bleibt festzuhalten, **dass bei der Erzeugung des Schlüsselpaares kein Dritter involviert ist.** Digitale Signaturen funktionieren wie Verschlüsselung, nur andersherum: **Zur digitalen Signatur verschlüsselt der Sender die Nachricht mit seinem geheimen Schlüssel** statt mit dem öffentlichen Schlüssel des Empfängers. **Der Empfänger entschlüsselt das Kryptogramm mit dem öffentlichen Schlüssel des Senders. Nur der Sender kann diese Nachricht so verschlüsselt haben, dass sie nach der Entschlüsselung einen vernünftigen Text ergibt** [128], ergo ist der Sender der, der er zu sein vorgibt, und **der Sender kann die Urheberschaft an der Nachricht nicht abstreiten. Die digitale Signatur ist damit sowohl nachrichten- als auch senderabhängig.**

Zwei technische Anmerkungen zur digitalen Signatur: Erstens. **Aus aus mathematischen Gründen,** um Fehler bei der Entschlüsselung zu vermeiden [128, S. 80], **benutzt jeder Kommunikationsteilnehmer für das Signieren bzw. prüfen einer Signatur ein anderes Schlüsselpaar als für Ver- bzw. Entschlüsselung von Nachrichten.** Zweitens. Zur digitalen Signatur wird nicht die Nachricht selbst, sondern ein digitaler Fingerabdruck der Nachricht verschlüsselt. Dafür gibt es zwei Gründe: a) Die digitale Signatur großer Datenmengen durch ein *Public-Key*-Kryptosystem ist zeitaufwendig. [128, S. vii] b) Unter Umständen ist es möglich, einzelne Blöcke der Signatur zu entfernen und trotzdem einen vernünftigen Klartext zu erhalten; man erhielte also eine gültige Signatur für einen abgekürzten, eventuell sinnentstellten Text [128, S. 93], z. B. eine kürzere Liste von Gegenständen, Personen, Buchungen etc.

Zurück zur Metapher des Telefonbuchs: Ein Anruf. Im Anzeigefeld des Telefons des Angerufenen erscheint die Nummer des Anrufers. Der Angerufene versucht durch Suche in einem elektronischen Telefonbuch herauszufinden, wer ihn anruft. Vom Anschluss des Anrufers aus könnte aber auch jemand anders anrufen (dass die Stimme gleich klingt, obwohl jemand anders anruft, schieben wir auf Nicht-HD-Telefonie) – so wird das nichts mit der Nichtabstreitbarkeit. Und es geht beim Zugriff auf den öffentlichen Schlüssel einer anderen Person auch nicht um das Nachschlagen einer Information, sondern um das Ausleihen eines Werkzeugs, mit dem die Überprüfung – nämlich das erfolgreiche Entschlüsseln – vorgenommen werden kann.

Wünschenswert wäre eine **Metapher für digitale Signaturen,** die den Zweck digitaler Signaturen, die Authentizität nichtabstreitbar zu belegen, auf den Punkt bringt. Eine Möglichkeit besteht darin, die Analogie zur Briefwahl herauszuarbeiten: *In online voting, the inner envelope is an encrypted vote and the outer envelope is a digitally signed document.* [46] Diese Metapher verwischt allerdings den Unterschied zwischen Verschlüsselung und digitaler Signatur, zwischen dem Schutz der Integrität der Nachricht einerseits und dem Nachweis der Authentizität andererseits. Vielleicht sollte man sich digitale Signatu-

ren so vorstellen: Der Absender lässt sich zusammen mit dem Dokument, das er senden möchte, hochauflösend fotografieren und nimmt für dieses Foto eine einzigartige Pose ein – den sterbenden Schwan, einen Moonwalk; der Phantasie sind keine Grenzen gesetzt – und orchestriert einen komplizierten Schattenwurf auf das Dokument, der es nahezu unmöglich macht, dieses Foto zu fälschen. Die Pose müsste sich von Foto zu Foto unterscheiden.[21]

Von digitalen Signaturen machen sowohl Estlands REV-System als auch das REV-System der Schweizerischen Post ausgiebig Gebrauch: Die Komponenten der Systeme kommunizieren grundsätzlich mittels digital signierter Nachrichten. [104, S. 13] [14]

Ein Problem wurde bis jetzt noch nicht behandelt, und zwar: **Woher weiß der Empfänger, dass der öffentliche Schlüssel des Senders authentisch ist?** Antwort: Jemand hat ihn digital signiert. Und woher weiß man, dass die Signatur authentisch ist? Jemand anderer hat sie digital signiert. Und so weiter, und so fort; wir treffen erneut auf das Problem der Rekursion. Es entsteht ein sogenannter Zertifizierungspfad, der muss irgendwo enden muss; er endet bei einer Instanz, der man letztlich vertrauen muss, der Stammzertifizierungsinstanz *(root certification authority)*. Zertifikate sind ausführlich dargestellt in [139, 140]. Dieser Zertifizierungspfad ist gemeint, wenn von einer **Infrastruktur für die öffentlichen Schlüssel (*Public-Key*-Infrastruktur, PKI-Infrastruktur)** gesprochen wird. Damit die Vertrauenswürdigkeit von Zertifikaten überprüft werden kann, ist in jedem Browser eine Liste von Zertifikaten vertrauenswürdiger Zertifizierungsstellen hinterlegt.

Wie digitale Signaturen Texte beglaubigen können, so können sie – man kann jede Bitfolge auch als einen Text interpretieren – belegen, dass eine Software (eine App, ein Treiber, eine Firmware etc.) **authentisch ist.** Zu diesem Zweck wird ein digitaler Fingerabdruck der Software digital signiert. Ein Beispiel mit Details: Der Fingerabdruck von Estlands Wählerverzeichnis wird mit der *Hash*-Funktion SHA-256 gebildet und mit einem 2048 Bit langen RSA-Schlüssel digital signiert. [46] Die Bundeskanzlei stellt die Anforderung: *Vor der Installation einer Software ist für sämtliche Programme anhand einer offiziellen vertrauenswürdigen Grundlage zu prüfen, ob es sich bei den Dateien um die korrekte und unverfälschte Version handelt.* [24]

4.5.7 Mischnetze

Aus der Reihenfolge des Eingangs der Stimmen, die geloggt wurde oder geloggt worden sein kann, lassen sich möglicherweise Rückschlüsse auf die Identität der Wähler ziehen – die Vertraulichkeit der Stimme wäre gefährdet.

Deswegen werden die Stimmen, wenn sich in Estland ein Auditor von der Korrektheit der Entschlüsselung bzw. des Zählvorgangs überzeugen möchte, zuvor einem Mischvorgang unterzogen [44]. Weil sich die Kryptogramme der abgegebenen Stimmen voneinander unterscheiden, vgl. Seite 24, reicht es nicht, die Kryptogramme zu mischen. Daher werden die Stimmen in Estland, ohne dass sie zuvor entschlüsselt worden wären, neu verschüsselt, umverschlüsselt. [45]

In der Schweiz ist das Geheimnis des privaten Schlüssels bekanntlich auf mehrere Mitglieder der Wahlkommission verteilt. Die Kryptogramme der abgegebenen Stimmen, sie wurden mit dem öffentlichen Schlüssel für diese Wahl verschlüsselt, werden in der Schweiz durch mehrere Mischer geschickt. Nacheinander, mit jedem Mischvorgang einer, werden die Stimmen mit den Teilen, aus denen sich der gesamte geheime Schlüssel zusammensetzt, teilentschlüsselt; man darf sich das vorstellen wie das Schälen einer Zwiebel [65]. Eine Bemerkung wert ist, dass, wenn die mit dem gemeinsamen öffentlichen Schlüssel erstellten Kryptogramme in mehreren Schritten entschlüsselt werden, die Teilnehmer ihren geheimen Schlüssel dabei niemandem gegenüber offenlegen. [66] Die Kryptogramme, die entstehen, lassen keinen Zusammenhang mit den ursprünglichen Kryptogrammen erkennen [66].

Voraussetzung für das **Umverschlüsseln der Stimmen** ist, dass sie mit einem homomorphen Verfahren verschlüsselt wurden [44], hier: ElGamal mit öffentlichem Schüssel für mehrere Empfänger. [66] Wir begegneten der Eigenschaft der Homomorphie bereits auf Seite 24 im Zusammenhang mit der Berechnung der Auswahlbestätigungscodes auf der Basis der Kryptogramme.

Wie wird sichergestellt, dass die übergebenen Stimmen gemischt werden und nichts anderes mit ihnen gemacht wird, die Gelegenheit des Mischens nicht dazu genutzt wurde, Stimmen unter den Tisch fallen zu lassen und als Ersatz dafür Stimmen für einen Kandidaten von des Angreifers Gnaden unterzumischen? Antwort: Man benutzt **Mischverfah-**

[21] Offline finden solche Fotos Verwendung, wenn Geiselnehmer die Geisel zusammen mit einer Tageszeitung als Zeitstempel abbilden, um zu beweisen, dass diese Person in ihrer Hand war und an diesem Tag lebte.

ren, nach deren Anwendung sich überprüfen lässt, ob korrekt gemischt worden ist; wie das funktioniert, dazu kommen wir im nächsten Abschnitt. Die Post benutzt Mischnetze nach Bayer/Groth (2012) [66, 141], in Estland wird ein Mischnetz nach dem Verificatum-Protokoll verwendet [46, 142].

4.5.8 Beweise, die keine Informationen preisgeben *(zero-knowledge proofs, ZKPs)*

Universelle Verifizierbarkeit verlangt, dass jeder Schritt nachvollziehbar/überprüfbar ist. Randbedingung: Die Vertraulichkeit der Stimme muss gewahrt bleiben. Diese kleine Quadratur des Kreises leisten **Beweise, die keine Informationen preisgeben *(zero-knowledge proofs, ZKPs),*** auch ›kenntnisfreie Beweise‹ oder ›Null-Wissen-Beweise‹ genannt.

Wie kann jemand beweisen, dass er ein Geheimnis kennt – z. B. das Geheimnis, wie die Stimmen gemischt wurden bzw. dass sie gemischt und nur gemischt wurden –, ohne dieses Geheimnis zu verraten? Beutelspacher et al. illustrierten das an einem Problem, welches im 16. Jahrhundert gelöst wurde: die Lösungen der kubischen Gleichung $x^3 + ax^2 + bx + c = 0$ zu finden. Wer für jede solche Gleichung die Lösung kennt, kann dies **interaktiv, durch eine Folge von Fragen und Antworten beweisen:** Die Frage könnte z. B. lauten: Welche Lösungen hat die kubische Gleichung, wenn $a = 1$, $b = 2$, $c = 3$ ist? Die Antwort bestünde dann der Menge der Zahlen $\{x_i\}$, die die kubische Gleichung mit den gegebenen Koeffizienten lösen. Wenn der Geheimnisträger für genügend viele Fragen die richtige Antwort präsentieren kann (und schneller antworten kann als Konkurrenten, die die Lösung durch Raten finden), so wird man ihm glauben, dass er im Besitz einer Formel ist, die es ihm ermöglicht, die Lösung jeder dieser Gleichungen zu berechnen.

ZKPs sind üblicherweise interaktiv, sie lassen sich aber in eine nichtinteraktive Form transformieren. [67] Auch für **nichtinteraktive Beweise, die keine Informationen preisgeben *(non-interactive zero-knowledge proofs, NIZKPs),*** gibt es Vorbilder: Wissenschaftler haben in der Vergangenheit Anagramme (Sätze, in denen sie die Buchstaben umgestellt, d. h. permutiert haben) benutzt, um ihre Priorität einer Entdeckung zu dokumentieren, ohne ihren Konkurrenten die Möglichkeit zu geben, die Forschung am Gegenstand aufzunehmen und darin schneller als sie zu Ergebnissen zu kommen. So wird Huygens zugeschrieben, er habe 1656 die Buchstabenfolge AAAAAAA CCCCC D EEEEE G H IIIIIII LLLL MM NNNNNNNNN OOOO PP Q RR S TTTTT UUUUU veröffentlicht und drei Jahre später in einem Buch die Lösung bekanntgegeben: *Annulo cingitur, tenui plano, nusquam cohaerente, ad eclipticam inclinato,* zu Deutsch: *Er [der Planet Saturn] ist von einem Ring umgeben, welcher dünn und flach ist, nirgends mit ihm zusammenhängt und gegen die Ekliptik geneigt ist.* [143]

Im Guardian waren ZKPs leider kein Thema, in der NZZ finden sich nur indirekte Erwähnungen wie *dass der Betreiber der E-Voting-Plattform Manipulationsversuche aufgrund von mathematischen Beweisverfahren feststellen kann* [144] oder *vollständig verifizierbar … was eine kryptologische Überprüfung des Abstimmungsresultats bedeutet* [59]. Ein informatisch Vorgebildeter hätte sich zumindest Stichworte gewünscht, die es ihm erlauben, sich in die Grundlagen der Verifizierbarkeit einzuarbeiten.

Estland hat die Verschlüsselung 2017 von RSA auf ElGamal umgestellt, um NIZKPs zu ermöglichen, die beweisen, dass korrekt gemischt wurde, dass korrekt entschüsselt wurde, dass korrekt gezählt wurde [44, 46, 50]. In der Schweiz beweisen NIZKPs, dass die Bestätigungscodes mit der verschlüsselten Auswahl korrespondieren, dass zwei Kryptogrammen derselbe Klartext zugrunde liegt, dass korrekt entschlüsselt wurde [14, 66].

Auch ZKPs basieren auf Annahmen. Wir kommen damit zu der Lücke im System der Post, die bereits 2017 gefunden wurde und deren Korrektur, wie sich 2019 herausstellte, nicht vollständig durchgeführt worden war. Sie entstand wie folgt: *The two cryptographic errors in the Swisspost/iVote/Scytl e-voting system … were misalignments of a primitive's properties with its protocol assumptions. In the case of the shuffle proof, a trapdoor commitment scheme was used in a protocol that was proven secure only under the assumption that the trapdoor was not known to the prover. In the case of the non-interactive ZKPs for equality of discrete logs, the problem was adaptive vs static security—a statically secure primitive was used in a protocol in which the adversary could adapt the input.* [112] Die Folgen des Fehlers: *An authority who knows the trapdoor values … [can] generate a shuffle proof transcript that passes verification but actually alters votes … substitute votes for which it knows the randomness used to generate the encrypted vote.* [68] Es handelte sich nicht um einen Fehler im Bayer/Groth-Verfahren, sondern um einen Fehler in der Implementierung durch die Firma Scytl. [68] Tatsächlich waren es zwei Fehler; es war nicht nur die universelle Verifizierbarkeit fehlerhaft, sondern auch die individu-

elle. [145] **Die Implementierung eines Verfahrens in Software muss so erfolgen, dass die Annahmen, auf denen das Verfahren basiert, erfüllt sind.** Der Fall unterstreicht: In komplexer Software lassen sich Fehler nicht ausschließen.

Wichtig ist noch eine Anmerkung zum Wesen von ZKPs: **Es handelt sich bei ZKPs/NIZKPs um probabilistische Verfahren.** [67] Wenn ein Schüler auf eine Prüfungsfrage die richtige Antwort gibt, weiß der Lehrer nicht, ob es Können war oder ob der Schüler die richtige Antwort geraten hat. Kann der Schüler aber auf verschiedene Prüfungsfragen in Folge die richtige Antwort geben, wird es jedoch unwahrscheinlich, dass er stets richtig geraten hat.

Genauso **ist mit jedem ZKP eine Wahrscheinlichkeit verbunden, dass der Beweis gilt.** Entsprechend muss sich die Bundeskanzlei festlegen, welche Irrtumswahrscheinlichkeiten sie bei den ZKPs zu akzeptieren bereit ist. Bei der individuellen Verifizierbarkeit verlangt sie eine Irrtumswahrscheinlichkeit von weniger als 0,1 %. Was eine Abweichung des Wahlergebnisses vom korrekten Wahlergebnis um mehr als 0,1 % angeht, verlangt sie eine Irrtumswahrscheinlichkeit von unter 1 %. [24]

Diesen probabilistischen Charakter der Beweiskraft von ZKPs muss man im Blick behalten, wenn es heißt, *mit universeller Verifizierbarkeit … haben … die Wahlbehörden jederzeit die volle Kontrolle über die abgegebenen Stimmen und können Manipulationen zweifelsfrei erkennen* [13] oder *beim System der Post könne zu 100 % eruiert werden, ob und wann es bei der Stimmabgabe zu Manipulationen gekommen sei* [146]. **Tatsächlich lässt sich die Wahrscheinlichkeit, dass eine Manipulation unbemerkt bleibt, auf beliebig kleine Werte drücken.**

Zur Überprüfung der ZKPs/NIZKPs, die bei der Verarbeitung der Kryptogramme der abgegebenen Stimmen erzeugt werden, kommt in Estland wie in der Schweiz eine Audit-App zum Einsatz. Bei diesen Apps stellt sich wiederum das Problem der Authentifizierung.

4.6 Angriffe

4.6.1 Ausspähen von Informationen *(phishing)*

Der Guardian berichtete im Zusammenhang mit Wählen per Telefon in Florida 2004 über folgende Angriffe [147]:

An automated voice had some surprising news: did he know that he could now cast his presidential vote by phone, and could do so right now, using the keypad? Mr Sasser's suspicion that somebody was trying to trick him into thinking he was casting a vote – presumably so that he wouldn't cast a real one – was far from unique.

James Scruggs … remembers a similar unease about the young woman who phoned him at home, insistently offering to collect his absentee ballot to ensure its safe delivery.

Then there was the elderly woman who called the local elections office last week to register her husband for an absentee vote. According to office staff, as she hung up she made a point of thanking them: she wouldn't have thought to get in touch about her husband, she said, if it hadn't been for their helpful call the night before, when someone had taken her own details, assuring her that she was now registered and would receive a ballot. But the elections office makes no such calls.

Angriffe, die auf **das Ausspähen von Informationen *(phishing)*** abzielen, können nicht nur per Telefon, SMS oder E-Mail initiiert werden, sondern auch von bösartigen Apps oder Websites ausgehen.

4.6.2 *Man-in-the-middle*-Angriff[22]

Wenn eine Verbindung nicht sicher ist, kann sich zwischen Sender und Empfänger ein Betrüger einschalten, der gegenüber dem Sender vorgibt, der Empfänger zu sein, gegenüber dem Empfänger, der Sender zu sein. Eine Illustration dafür, wie ein *Man in the middle* seine Position ausnutzen kann, findet man in ›Asterix bei den Goten‹: Der Dolmetscher, der zwischen dem gallischen Druiden und dem gotischen Befehlshaber vermittelt, übersetzt nicht eins zu eins, sondern manipulativ (mit dem Ziel, seine eigene Haut zu retten). Wie ein Angreifer mit einem ***Man-in-the-middle*-Angriff** verschlüsselte Kommunikation unterwandern kann, ist schülergerecht beschrieben in [148]; dieser Angriff illustriert, wofür digitale Signaturen benötigt werden.

Wenn digitale Signaturen nach dem Stand der Technik verwendet werden, darf man davon ausgehen, dass ein *Man-in-the-middle*-Angriff ausgeschlossen ist – *wenn.* Der Guardian berichtete 2015: *While the iVote website itself is secure, Melbourne University security specialist Vanessa Teague discovered … that it loaded javascript from a third-party website that was 'vulnerable to an attack called the FREAK attack'. 'The*

[22] Wir tun uns schwer damit, hierfür im Deutschen einen treffenden Begriff zu finden. ›Mittelsmann-Attacke‹ trifft es nicht, weil Mittelsmänner absichtlich eingesetzt werden. ›Stille-Post-Attacke‹ trifft es nicht, weil der Sender bei stiller Post weiß, dass er nicht direkt mit dem Empfänger kommuniziert.

implication is that an attacker who controls some point through which the user's traffic is passing could substitute that code for a code of the attackers' choice,' she said. In layman's terms, a hacker could intercept a vote for party A and turn it into a vote for party B without alerting the voter or the NSW [New South Wales] Electoral Commission. [149]

Bei der FREAK-Attacke, erläutert heise online, *handelt es sich um ein Relikt aus den 90er Jahren, als die US-Regierung die Nutzung von starker Kryptografie zugunsten der NSA einschränkte. Wenn ein Server diese Export-Ciphers unterstützt, kann ein Angreifer durch Manipulation des Verbindungsaufbaus einen Rückfall auf die schwache Verschlüsselung mit einem unsicheren 512-Bit-Schlüssel erzwingen … Neben dem Server muss aber auch der Client die Export-Cipher unterstützen, sonst sei der Angriff nicht realisierbar.* [150] Verschlüsselung ist, wie das Beispiel noch einmal vor Augen führt, nur sicher, wenn die Schlüssel genügend lang sind; Gleiches gilt für digitale Signaturen.

Ein *Man-in-the-middle*-Angriff kann erklären, wie es dazu kommen konnte, dass in Estland eine ungültige Stimme in der Urne landete: *In the case of cell phone based digital identity – Mobile-ID – only the VFS [Vote Forwarding Server = Stimmensammel-Server] is authenticated; the voter identification follows from the Mobile-ID protocol and cannot be used on the HTTPS level … This opens the possibility for a man-in-the middle attack where the user's certificate store is compromised with the attacker's CA certificate and an intercepting HTTPS proxy using a certificate signed by attacker's CA is installed between the IVCA and the IVS [I-voting system]. The proxy modifies the original candidate list sent to the IVCA so that it contains invalid candidate numbers … The user does not notice the invalidity of the candidate numbers and casts a vote which is correctly formatted and encrypted by the IVCA and forwarded to the VFS by proxy. This type of intentionally invalidated i-vote would have been falsely identified as a bug in the IVS after the i-vote decryption.* [81]

Bei sicherer Verschüsselung ist ein *Man-in-the-middle*-Angriff, wie gesagt, ausgeschlossen. Wenn es diese technische Möglichkeit gibt, muss sie aber auch konsequent genutzt werden. Springall et al. beobachteten 2013 in Estland, dass Software von einer öffentlichen Website über eine unsichere HTTP-Verbindung heruntergeladen wurde; auf diese Weise hätte ein Angreifer durch einen *Man-in-the-middle*-Angriff Schadsoftware einschleusen können. [49]

4.6.3 Schadsoftware *(malware)*

Eine Folge der Existenz von sicherer Verschüsselung/digitaler Signatur ist, dass Angreifer versuchen, Daten vor der Verschlüsselung abzugreifen. **Man muss davon ausgehen, dass ein signifikanter Anteil aller privaten Rechner mit Malware infiziert ist** [86]; Purgathofer spricht von 25 % aller privaten Rechner [130], Ondrisek sogar von bis zu 50 %. [79]

Wie gelangt Schadsoftware auf private Rechner? Es kommen viele Wege infrage: jemand hat im Anhang einer E-Mail eine Datei angeklickt, die mit einem Makrovirus infiziert war; jemand hat einen auf dem Parkplatz gefundenen USB-Stick angeschlossen, der dort absichtlich ›verloren‹ wurde; jemand ist bei einer Recherche alle Treffer durchgegangen und hat dabei eine Website mit Schadsoftware angesurft (*Drive-by*-Attacke [151]); oder durch eine Schwachstelle im Betriebssystem, über die bisher nur potentielle Angreifer etwas wissen [152], für die bisher kein Update zur Verfügung steht oder die auf dem Rechner des Wählers bisher nicht durch ein Update behoben wurde. Zahlreiche weitere Wege sind denkbar.

Es ist, schon um die Komplexität des Systems so klein wie möglich zu halten, ratsam, das REV-System mit so wenig Software und Hardware wie möglich auszustatten. [124] Springall et al. beobachteten in Estland, dass Mitarbeiter die Auslieferung der Wahl-App auf einem Rechner vorbereiteten, auf dem privat verwendete Software lief; auf diese Weise hätte Schadsoftware auf die Rechner aller Wähler gelangen/eingebracht werden können. [49]

Es schützt nicht, den Auszähl-Server nicht mit dem Internet zu verbinden, wenn, wie Springall et al. aus Estland berichten, offizielle Ergebnisse, anstatt wie vorgeschrieben auf eine DVD gebrannt zu werden, mit einem USB-Stick, auf dem sich private Dateien befanden, übertragen werden; so hätte Schadsoftware auf den Server übertragen werden können. [49]

Inwiefern stellt Schadsoftware eine Gefahr dar? Ein großer Teil der Schadsoftware bringt Fähigkeiten von **Tastaturspionen *(keylogger)*** bzw. **Bildschirmspionen *(screenlogger)*** mit (Oberbegriff ***spyware***). Um es mit Orwells Worten auszudrücken: ***Big Brother is watching you.*** heise online dekliniert an einer Sicherheitssoftware durch, was Onlinebanking in einer kompromittierten Umgebung bedeutet: Gegen Tastaturspione helfen simulierte Tastenanschläge und virtuelle Tastaturen. Simulierte Tastenanschläge kann eine Schadsoftware als solche erkennen, wenn sie die Anschläge nach der erzeugenden Quelle aufschlüsseln

lässt. Virtuelle Tastaturen kann sie durch Bildschirmfotos ausspähen. Zwar stellt Microsoft Windows eine Programmierschnittstelle bereit, die das Kopieren des Fensterinhalts unterbindet; diese Funktion lässt sich aber umgehen. [153] Und so weiter, und so fort; Sicherheit ist ein ständiger Wettlauf.

Tastatur- und Bildschirmspione stellen Spezialfälle von **trojanischen Pferden** dar, **Programmen, die, und sei es zusätzlich, etwas anderes tun als das, was man von ihnen erwartet.**[23]

Ein trojanisches Pferd kann so gestaltet sein, dass es die Oberfläche eines anderen Programms imitiert. Der Benutzer glaubt, mit der gewünschten App, der gewünschten Website zu interagieren; tatsächlich tätigt er seine Eingaben auf der Oberfläche des trojanischen Pferdes. Das trojanische Pferd kann sich mit den *abgephishten* Informationen – genau darum ging es auch bei den *phishing*-Angriffen auf Telefonwähler, Seite 29 – gegenüber dem Originalprogramm, der Originalwebsite als der Benutzer ausgeben (*Man-in-the-middle*-Angriff). Das erklärt, warum die Anbieter von Onlinebanking davon abgekommen sind, die Kunden mit Listen von Transaktionsnummern auszustatten, und stattdessen auf eine Zwei-Faktor-Authentifizierung, also eine zusätzliche Authentifizierung auf einem unabhängigen Kanal, mit einem unabhängigen Gerät setzen.

Bekommt der REV-Wähler auf dem Bildschirm die Namen der Kandidaten/Parteien zu sehen, kann ein trojanisches Pferd unter gewissen Voraussetzungen die Stimme des Wählers einem Kandidaten von des Angreifers Gnaden zuschlagen. Heiberg et al. berichteten 2011 aus Estland: *Student P. sent an e-mail to the NEC [National Electoral Committee] and three major newspapers claiming that he had written a prototype of an election rigging malware …The presentation pointed out that a malicious piece of software controlling both input and output interfaces on a client computer was a threat to the IVCA as it was capable of manipulating the voter to believe that he has voted for candidate c_1, although the malware actually voted for candidate c_2.* [81]

Student's attack, wie der Angriff genannt wurde, funktionierte technisch wie folgt: *The proof of concept malware of P. used the IVCA graphical user interface (GUI) as an attack-vector. It was written in AutoIt scripting language … which is a framework for scripting GUI-based Windows applications. Optical character recognition (OCR) technology was used on the IVCA screenshots to decode voter personal data and the intended candidate. Fake-IVCA was built from the screenshots and the message-loop of the original IVCA was poisoned with generated mouse events. The fake-IVCA was used to leave the voter with the impression that the ballot was cast as intended. Underneath the fake-IVCA, the original software accepted generated events and voted for a semi-randomly selected candidate.* [81]

Der Angriff wurde von ›Student P.‹ sogar noch variiert: *P. implemented a new type of attack – the malware now selectively held back ballots for certain candidates, whereas the voter was left with the impression that his vote was successfully sent to the VFS.* [81]

Wenn das REV-System, wie es in Estland seit 2013 [51] der Fall ist – als Reaktion auf *Student's attack* eingeführt [50] –, individuelle Verifizierung über einen unabhängigen Kanal erlaubt, fällt ein solcher Stimmendiebstahl dem Wähler, der von der Verifizierungsmöglichkeit Gebrauch macht, auf.

Nicht auffallen würde ihm jedoch folgender Angriff, die Von-Geistes-Hand-Attacke *(Ghost Click Attack)*, die Springall et al. konstruierten: *The malware silently sniffs the victim's PIN [für die digitale Signatur] during the original voting session. The real vote is cast, and everything appears normal, including the verification smartphone app if the voter uses it. Then, the malware waits until it is too late to verify again — either until the 30 minute time limit has passed or until after the user closes the client software and the QR code can no longer be scanned. At that point, the malware checks whether the voter's ID card is still present in the computer. If so, it opens a copy of the I-voting client in a hidden session and, through keystroke simulation, submits a replacement vote. If the ID card has already been removed, the malware remains dormant until the card is inserted again. Since Estonian ID cards are used for a variety of applications, many voters are likely to use their cards again within the week-long online voting period.* [49]

Was würde das Wahlkomitee machen, wenn aus den Log-Einträgen hervorginge, dass 20 % der Wähler ihre Stimme zweimal abgegeben haben? Wie wollte man dazwischen unterscheiden, ob Betrug vorliegt oder die Wähler ihre Entscheidung angesichts eines Skandälchen, das in der Wahlwoche bekannt wurde, überdacht haben?

Dem Wähler per SMS jede Stimmabgabe zu bestätigen, wäre keine Lösung für die Von-Geistes-Hand-Attacke, weil eine solche Benachrichtigung es ermöglichen würde, den ›Erfolg‹ von Zwang/Stimmen(ver)kauf zu dokumentieren.

[23] Trojanisches Pferd oder Hintertür? Schon im Trojanischen Krieg war die Wirkung dieselbe.

Die Glaubwürdigkeit der individuellen Verifizierbarkeit in Estland beruht auf der Annahme, dass das zweite Gerät wirklich unabhängig ist. Springall et al. geben zu bedenken: *Modern smartphones are not well isolated from users' PCs, as there is typically regular communication between the two devices. Users frequently plug their phones into their PCs to charge them or to transfer files. User content is regularly synchronized between devices through Google Drive, Dropbox, and other cloud services. Android even allows users to remotely install applications on their phones from their PCs through the Google Play Store web interface, and other platforms have similar mechanisms … As a result of this convergence, there are abundant means by which PC malware can attempt to infect the user's phone.* [49]

Vom Onlinebanking ist jedenfalls bekannt, dass Kriminelle auch Mobiltelefone infizieren, um die Zwei-Faktor-Authentifizierung auszuhebeln. [154]

Wenn beide Geräte mit passender Schadsoftware infiziert sind, wird eine Attacke möglich, bei der die Verifizierung gefälscht wird *(Bad Verify Attack).* Wie ein moderner Rechner einen historischen Rechner emulieren kann, z. B. um ein Computerspiel von damals auszuführen, **kann ein trojanisches Pferd ein anderes Programm emulieren.** Springall et al. entwerfen folgenden Angriff: *Malware on the PC detects which candidate the voter selects and modifies the QR code shown by the I-voting client so that it encodes the voter's chosen candidate. A malicious verification app on the voter's phone behaves just like the real verification app, except that it displays whatever candidate is embedded in the QR code, rather than the candidate for whom the vote was actually cast.* [49] Hier spielen zwei trojanische Pferde einander die Bälle zu.

Dieser Angriff funktioniert nicht, wenn der Wähler auf ein Smartphone zurückgreift, das nicht mit der korrespondierenden Schadsoftware infiziert ist, z. B. ein Smartphone, welches mit den infizierten Rechnern im Haushalt nie verbunden war. Aber ist es abwegig, anzunehmen, dass das fremde Smartphone mit derselben – vor der Wahl breit zu verteilenden – Schadsoftware infiziert ist? Und wie viele Wähler werden in den 30 min, die ihnen für die Verifizierung zur Verfügung stehen, auf das Smartphone eines Dritten zurückgreifen (können)? Und selbst wenn: Wie viele werden auf dem Smartphone eines Dritten im Klartext lesen wollen – im Cache-Speicher des Smartphones aufbewahrt? –, für wen sie gestimmt haben?

Stehen die Wahl-Apps einer nennenswerten Anzahl Wähler unter der Kontrolle eines Angreifers, so kann die Wahl-App dem Wähler, der den Kandidaten X wählen möchte, auch einen QR-Code anzeigen, der auf eine Stimme für X verweist, die jemand anderer, von einem anderen infizierten Rechner aus, für X abgegeben hat. Dass die Möglichkeit zur individuellen Verifizierung nur für 30 min und drei Versuche zur Verfügung steht [49], schränkt einen solchen Angriff ein; eine weitverbreitete Schadsoftware könnte hier aber mit Buchführung in der Cloud aufwarten. Wenn der Angreifer die Verifizierungsanfragen wählerübergreifend managt, kann er Anfragen, die von weit voneinander entfernten Orten ausgehen, so durch Internet leiten, dass nicht auffällt, dass unmöglich ein und derselbe Wähler hinter diesen drei Verifizierungsanfragen stehen kann.

Es hat also Gründe, weshalb auf Estlands Wahl-Website bis heute darauf hingewiesen wird: *Make sure that your computer is virus-free before i-voting.* [155]

Das Schweizer REV-System ist an dieser Stelle anders aufgebaut: Einem Angreifer ist es nicht möglich, die Bestätigungscodes zu erraten. Daher kann die Bundeskanzlei individuelle Verifizierbarkeit sogar in dem Fall garantieren, dass der Rechner des Wählers unter dem Einfluss von Schadsoftware steht. [14]

Gegen Viren und andere Schadsoftware wurde und wird Antivirussoftware (AV-Software) entwickelt. Wie bei biologischen Infektionen **muss man allerdings damit rechnen, dass zwischen Infektion und Entdeckung eine Latenzzeit liegt.** Es dauert – Sicherheit ist ein ständiger Wettlauf – eine gewisse Zeit, bis die AV-Software-Hersteller von dem neuen Schädling Kenntnis erlangen und reagieren.

In die FAQ zu Estlands REV-System wurde der Fall aufgenommen, dass AV-Software die Wahl-App als Schadsoftware einstuft: Die Antwort: *Although producers of virus protection programs have been notified, and they have been asked to categorise the voter application among allowed applications, some virus protection programs may hinder the opening of the voter application on a device. To solve the problem, please update your virus protection software. If this does not help, include the voter application among exceptions in your virus protection program. If this does not help either, please disable your virus protection program for the time when you are e-voting, or e-vote on another device.* [156] Die Frage ist, wie viele das betrifft und wie viele von ihnen sich mit den Einstellungen der AV-Software beschäftigen wollen. Was den letzten Tipp angeht: Ausgerechnet beim Wählen soll man seine AV-Software deaktivieren?

Das BSI hebt hervor, dass zu den Voraussetzungen für das korrekte Funktionieren von AV-Software gehört: *Antivirensoftware … verfügt über weitreichen-*

de Systemberechtigungen und muss systembedingt (zumindest für Aktualisierungen) eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten. [157] Die Implikationen sind, wie das BSI selbst feststellt, erheblich: ***Daher ist Vertrauen in die Zuverlässigkeit und den Eigenschutz eines Herstellers*** *sowie seiner authentischen Handlungsfähigkeit* ***entscheidend*** *für den sicheren Einsatz solcher Systeme.* [157] Im März 2022 hat das BSI in derselben Pressemitteilung, aus der die beiden vorigen Zitate stammen, eine Warnung vor AV-Software der Firma Kaspersky ausgesprochen [157], mit der Begründung: *Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen Willen gezwungen werden, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden.* [157] Ob Antivirussoftware, bei der vor dem Wort *IT-Hersteller* ein anderes Adjektiv steht, per se vertrauenswürdiger ist, sei an dieser Stelle dahingestellt. Sollte man also gerade beim Wählen seine AV-Software deaktivieren[24]? **Belegt ist jedenfalls, dass AV-Software Ziel von Angriffen geworden ist** [158], **und trotz der Verfügbarkeit von AV-Software sind die Cyberangriffe heutzutage Legion;** eine Auflistung von Vorfällen mit Links zu weiterführenden Informationen findet man z. B. bei [159]. Und was hilft die beste AV-Software, wenn Angreifer einen Weg gefunden haben – heise online berichtete [160] –, sie einfach abzuschalten?

Zu denken gibt, dass immer wieder auch Ziele, bei denen man Bewusstsein für die Sensibilität der Daten erwarten darf, Opfer von Angriffen werden; Beispiele aus Deutschland sind der Bundestags-*Hack* vom Mai 2015 oder der *Hack* auf den Mobilitätsdienstleister BwFuhrparkService GmbH im August 2020, dessen Gesellschafter das Bundesverteidigungsministerium und die Deutsche Bahn AG sind [161, 162]. Mit der Organisation und Durchführung von REV wären vergleichbare staatliche Stellen betraut. Das Versagen den Genannten mit Unfähigkeit zu erklären, greift zu kurz; denn es ist sicherlich nicht einfach, Informatiksysteme gegen mächtige Angreifer zu schützen, wenn die Systeme ein interessantes Angriffsziel darstellen.

Eine weitere Ursache von Schadsoftware kann in einem **Angriff** bestehen, **der weiter oben in der Lieferkette ansetzt *(supply chain attack)*;** hier kann auch Schadhardware ins Spiel kommen. Der CCC-CH gibt zu bedenken: *Die Schweiz und ihre kritische Infrastruktur hängt schon heute in entscheidendem Masse von US-amerikanischer und chinesischer Gnade ab … Dass praktisch die gesamten eingesetzten Hard- und Softwarekomponenten aus dem Ausland geliefert werden, erleichtert Angriffe auf die Lieferkette deutlich.* Die New York Times berichtet von einem solchen Angriff: *In one case, after the government learned that a foreign intelligence target had ordered new computer hardware, the American manufacturer agreed to insert a back door into the product before it was shipped …* [120]

Zu Angriffen auf die Lieferkette lässt sich auch ein Angriff über ein Update zählen. Ondrisek sieht im Update-Prozess ein hohes Sicherheitsrisiko, *da durch eine solche Schnittstelle … zusätzlicher Code eingebaut … werden kann. Durch eine derartig offene Schnittstelle zur Software können Angreifer bösartigen Code platzieren, Hintertüren einbauen und auf diese Art das Wahlergebnis manipulieren* [16], und zieht im Hinblick auf Schadsoftware das Fazit: *Dass die eingesetzten Systeme frei von … Schadsoftware sind, [ist] eine Annahme, die InformatikerInnen zu spontanen Heiterkeitsausbrüchen verleiten kann.* [79]

4.6.4 Angriff versus Angreifbarkeit

Heiberg von der Firma Cybernetica, die Estlands REV-System entwickelt hat, zufolge habe es bisher, berichtete die NZZ 2018, keinen erfolgreichen Angriff gegeben. [77]. Auf Seite 31 hatten wir allerdings zitiert, was Heiberg et al. über die – ihr eigener Wortlaut – *proof of concept malware* von ›Student P.‹ zu berichten hatten. Es mag sein, dass durch die Schadsoftware von ›Student P.‹ nur 1 Stimme verändert wurde, und man kann darüber streiten, ob ein Wähler seine eigene Stimme manipulieren kann. Wenn allerdings eine einzelne Person ohne nennenswerte materielle Ressourcen in einer überschaubaren Anzahl Stunden in der Lage ist, ein solches trojanisches Pferd zu schreiben, zu was ist dann organisierte Kriminalität, die über die Infrastruktur zum Ausliefern trojanischer Pferde in großem Stil verfügt, in der Lage – von Akteuren mit den Ressourcen eines Staates ganz zu schweigen!

Sobald eine Angreifbarkeit existiert, ist ein Angriff möglich; ob er stattfindet oder nicht stattfindet, hängt letztlich von nichtinformatischen Umständen ab. Dazu vier Beispiele:

Beispiel 1. In Illinois drangen Hacker in eine Wählerdatenbank ein und verschafften sich Zugriff auf Informationen von rund 200 000 Personen. Zwar

[24] Wie will der Wähler eigentlich überprüfen, ob die AV-Software, die er deaktiviert hat, sich wirklich deaktiviert hat?

gab es keine Hinweise darauf, dass bei dem Angriff Informationen gelöscht oder verfälscht wurden. Das Geheimdienstkomitee des Senats kam aber zu dem Schluss, dass es den Angreifern möglich gewesen wäre. [113] – Derjenige, der Schreibzugriff auf das Wählerverzeichnis erlangt, kann darüber bestimmen, wer an der Wahl *nicht* teilnehmen darf. Was würde es nützen, den Ausgesperrten im Nachhinein die Stimmabgabe zu ermöglichen? Auf wie viel Verständnis würde man bei denjenigen stoßen, zu deren Ungunsten das Wahlergebnis nun korrigiert werden soll?

Beispiel 2. Eine prinzipielle Bedrohung für REV-Systeme geht von **Überlastungsattacken (*Denial-of-Service*-Attacken)** aus. Angreifer, die eine Vielzahl von Rechnern gekapert haben – laut BSI sind allein in Deutschland rund eine Million Rechner Bestandteil von **Botnetzen** [163, 164] –, können diese zeitgleich einsetzen, um Server zu überlasten, die dann für die Wähler nicht verfügbar sind. In der NZZ wird das Störpotential illustriert: *Wenn das E-Voting in den letzten zwei Stunden vor dem Ende der Abstimmung nicht möglich ist, so wird diese wohl für ungültig erklärt werden müssen. Damit liesse sich jede unliebsame Abstimmung mit wenig Geld verhindern.* [117]

Beispiel 3. Die Überlastungsattacke tritt in vielen Varianten auf: Springall et al. fanden in Estlands System 2013 eine Lücke, die es einem Angreifer ermöglicht hätte, den Server durch Überlasten des Logspeichers dazu zu bringen, keine weiteren Stimmen mehr zu akzeptieren; für diese Überlastungsattacke hätte ein Angreifer circa 75 min benötigt. [49]

In Beispiel 4, wir kennen es von Seite 20, geht es um Wahlcomputer: *According to Harris, a manipulation technique she found in Diebold's AccuVote central vote tabulator is able to read totals from an untraceable bogus vote set within its software. ›By entering a two-digit code in a hidden location, a second set of votes is created; and this set of votes can be changed in a matter of seconds, so that it no longer matches the correct votes,‹ she has said. And she has demonstrated this live on television. Her conclusion is: ›You can easily edit the election.‹* [91, 111]

Die Beispiele verdeutlichen, dass es **nicht sinnvoll** ist, **zwischen Angreifbarkeit und versuchtem bzw. bis zu einem gewissen Grade verwirklichtem Angriff zu unterscheiden.** Wir überlassen es dem Leser, das folgende Korrigendum, das in der NZZ erschien, einzuordnen: *Im Bericht über die Entwicklung eines E-Voting-Systems … (NZZ 11.4.15) wurde ein Argument … erwähnt, wonach das elektronische Wahl- und Abstimmungssystem in Genf in einem Fall nachträglich manipuliert worden sei. Die Staatskanzlei Genf legt Wert auf die Feststellung, dass es nie einen erfolgreichen Hackerangriff auf das Genfer System gegeben habe. Ein Spezialist habe das System lediglich nachgebaut und unter Laborbedingungen die Wirkungsweise von Schadsoftware demonstriert.* [165]

5 Anmerkungen

Wir gehen in diesem Abschnitt auf Aspekte ein, die im Kern keine Frage der Informatik sind, aber im Hinblick auf das Fachgebiet ›Informatik und Gesellschaft‹ von Bedeutung sind.

5.1 Potentielle Angreifer

Motive für Angriffe sind a) der Gewinn indirekter Macht oder direkter Macht (Mandate, Regierungsstellen) sowie b) die Gewinnung von Informationen über das Abstimmungsverhalten der Wähler. (Daneben ist Selbstwirksamkeit von Hackern ein Motiv: zu beweisen, dass sie in der Lage sind, das System zu knacken.) Politische Macht ermöglicht die Entscheidung über große Geldbeträge – der Deutsche Bundestag z. B. entscheidet direkt oder indirekt, d. h., durch Setzen bzw. Verändern bzw. Nichtverändern der gesetzlichen Rahmenbedingungen, über viele einstellige, nicht wenige zweistellige und manche dreistellige Milliardenbeträge –; **an dieser potentiellen Beute ist der Aufwand zu messen, den ein Akteur zur Beeinflussung der Wahl zu investieren bereit wäre.** Auch Springall et al. sprechen von *enormous political and financial consequences at stake.* [49]

Diese Beträge muss man im Hinterkopf haben, wenn man die Prämien für das Finden von Sicherheitslücken im Rahmen von Intrusionstests, über welche die NZZ berichtet, einordnen möchte: *Der Bund und die Kantone leisten … einen Beitrag von 250.000 Franken an die Durchführung des öffentlichen Intrusionstests. Die Prämien können durchaus happig ausfallen. Wem es gelingt, individuelle Stimmen so zu manipulieren, dass es nicht entdeckt wird, erhält 20.000 bis 50.000 Franken. Wer entschlüsselt, wie jemand gestimmt hat, und damit die Privacy bricht, kann 5.000 Franken verdienen.* [166]

Die Kosten für den Einbruch in den REV-Prototypen von Washington D.C. fielen jedenfalls bescheiden aus: *Halderman said his team's attack would have cost less than $50,000 at generous consulting rates.* [108] Durch eine Manipulation der Wahl hätte ein Angreifer nichtintegre Personen in der Stadtverwaltung von Washington D.C. platzieren können. Wenn sich diese

an der Manipulation von Bauausschreibungen beteiligen, sind 50 000 Dollar Spesen, die sich in kürzester Zeit amortisieren.

Der Aufwand verengt den Kreis möglicher Angreifer auf **Staaten** (buchstäblich inter-nationale Angriffe) und **organisierte Kriminalität;** diese potentiellen Angreifer muss man vor Augen haben, wenn man die fachlichen Voraussetzungen für ein Ausnutzen folgender Angreifbarkeit einordnen möchte: *Konkret geht es um die theoretische Möglichkeit, dass ein Hacker gelöschte Daten wiederherstellen und somit herausfinden könnte, welcher Bürger welche Kandidaten gewählt hat. Laut Consortium würde ein solcher externer Zugriff aber ein sehr hohes technisches Fachwissen voraussetzen.* [55]

Man kann Betrachtungen anstellen [167], bei welcher Abstimmung wie viele Stimmen hätten manipuliert werden müssen, um das Ergebnis zu kippen. Es gibt aber mit Sicherheit Angreifer, die es sich leisten können, Ergebnisse über eine Reihe von Jahren Stück für Stück in die gewünschte Richtung zu lenken. Die klügeren Angreifer werden jedenfalls nicht so hochmütig sein, Wahlergebnisse wie 98,85 % (Kommunalwahl in der DDR 1989 [168]) zu fabrizieren.

5.2 Angriffsziele

5.2.1 Angriffsziel Wähler

Im Wahllokal stellen Wahlhelfer sicher, dass der Wähler in der Wahlkabine allein ist. Bei REV ist ein vergleichbarer Schutz der Vertraulichkeit der Stimme nicht möglich, **der Wähler kann bei der Stimmabgabe unter Druck stehen** (von den Eltern? vom matriarchal regierenden Familienoberhaupt? vom Arbeitgeber? von organisierten Kriminellen?), **oder er kann seine Stimme verkaufen,** z. B. auf eBay [134].[25,26]

Im Guardian wird darauf hingewiesen, dass per Post erhaltene Codes leicht weitergegeben werden können. [101] Nun kann man sich wie die Schweizerische Post auf den Standpunkt stellen: *In some countries, re-voting mitigates the risk of vote coercion, but in Switzerland — where mail-in voting is the predominant way of voting*[27] *— vote coercion is not a widespread problem.* [65] Transparency International zufolge sind aktuell weltweit aber gerade einmal sechs Länder vergleichbar wenig korrupt wie die Schweiz [172], und es liegt, von der Aussagekraft einer Liste mit dem Titel ›Korruptionswahrnehmungsindex‹ einmal ganz abgesehen, in der Natur der Sache, dass kein Land für seinen Rang auf dieser Liste ein Abonnement besitzt. Abgesehen davon ist belegt, dass selbst in als vergleichbar wenig korrupt geltenden Ländern Zwang bzw. Stimmen(ver)kauf vorkommen. [173]

Estlands Wähler werden davor zurückschrecken, ihre ID-Card einem Dritten ›auszuleihen‹ und diesem die PIN für digitale Signaturen mitzuteilen – er könnte großen Schaden anrichten, indem er rechtsverbindlich Verträge zulasten des Karteninhabers abschließt.

In der Schweiz kann der Wähler seine Stimme exakt ein Mal abgeben [65]; der ›Erfolg‹ von Zwang und Stimmen(ver)kauf wird dadurch dokumentierbar. Wenn ein REV-System Bestätigungen anbietet, dass eine Stimme für den Kandidaten X eingegangen ist, sollte man, wie in Estland, die Stimme mehrmals abgeben dürfen. Es bräuchte in der Schweiz eine niedrigschwellige Möglichkeit für die Wähler, sich eine neue Codeliste zu besorgen (wodurch eine mit alten Codes abgegebene Stimme ungültig würde).

5.2.2 Angriffsziel Wahlkommission

Befürworter von REV argumentieren, es ließen sich Kosten sparen – daran sind übrigens Zweifel angebracht –, vor allem Kosten für Wahlhelfer. Die zahlreichen Wahlhelfer in den Wahllokalen, die nach dem Vieraugenprinzip arbeiten, sind aber nicht nur eine Kostenposition, sie sind der Garant dafür, dass es äußerst schwer ist, eine Papierwahl in großem Stil zu fälschen: Die Anzahl der zu beteiligenden Personen würde so groß, dass unmöglich alle diese Positionen mit Verschwörern besetzt werden könnten. Daher würde es extrem unwahrscheinlich, dass die Manipulation von niemandem bemerkt wird.

[25] Zwang und Stimmen(ver)kauf sind der Grund, warum die Schöpfer einer Verfassung eine in großem Umfang praktizierte Briefwahl kritisch sehen müssen. Der Tagesspiegel (Berlin) hält fest, dass die massive Ausweitung der Briefwahl – seit Dezember 2008 müssen deutsche Bürger keine Gründe mehr angeben, nicht mehr glaubhaft machen, warum sie nicht im Wahllokal wählen können [169] – der Wahlmanipulation Tür und Tor öffnet. [170]

[26] Das Bundesverfassungsgericht hat diese Ausweitung der Briefwahl 2013 bestätigt, es schrieb in seinem Beschluss aber selbst: *Dass ein erheblicher Anstieg der Briefwahlbeteiligung durch den Wegfall der Glaubhaftmachung von Antragsgründen jedoch nicht zu befürchten ist, hat der Gesetzgeber für die Bundestagswahl insbesondere mit Erfahrungen bei Landtagswahlen begründet … Es gibt keine Anhaltspunkte dafür, dass diese Einschätzung in verfassungsrechtlich relevanter Weise verfehlt oder auf die Wahlen zum Europäischen Parlament nicht übertragbar sein könnte.* [171] – Es wird sich zeigen, ob die 47,3 % Briefwähler bei der Bundestagswahl 2021 [6] als Sondereffekt im Zusammenhang mit Covid-19 angesehen werden dürfen.

[27] *Im Jahr 2015 wird der briefliche Abstimmungskanal von den … wahlberechtigten Schweizern im Inland zu rund 90 % genutzt.* [31]

Wenn bei REV die Anzahl der Personen, die die Wahl durchführen, nur noch wenige Dutzend umfasst, entsteht, Simons und Jones weisen darauf hin, eine völlig andere Situation: *Since computerized voting is an opportunity for wholesale rigging through software used by large numbers of voters, the size of the conspiracy needed to win an election is greatly reduced, as is the risk of being caught.* [108] Ergo **skaliert das Manipulationsrisiko bei REV unabhängig vom verwendeten REV-System hoch.**

Wenn in die Durchführung einer Wahl nur wenige Dutzend Personen involviert sind, wird es für Angreifer attraktiv, unter diesen nach dem schwächsten Glied zu suchen. Diejenigen, die den Aufwand, eine Wahl zu manipulieren, schultern können, verfügen zweifellos über die Mittel finanzieller und personeller Art, um durch Kauf, Erpressung, Bedrohung auf einige an der Durchführung der Wahl beteiligte Personen, vielleicht auch über den Hebel Familie, Druck auszuüben. Verschärft wird dieses Problem dadurch, dass REV tagelang zur Verfügung steht.

Purgathofer weist darauf hin, dass für die Organisation der nächsten Wahl der Gewinner der letzten Wahl zuständig ist. [130] Wenn eine Regierung an die Macht käme, die nicht daran denkt, sie wieder abzugeben … Das mag unwahrscheinlich erscheinen, aber lässt sich dieser Fall ausschließen? Wer über die Einsetzung der Wahlkommission bestimmt, kann sie mit nichtintegren Personen besetzen, sodass die Suche nach einem schwächsten Glied unter diesen Personen obsolet wird. Droz stellt die rhetorische Frage: *Und nachdem das E-Voting mal eingeführt ist, wie soll man es wieder abschaffen können? Mit E-Voting?* [85]

5.2.3 Angriffsziel Vertraulichkeit der Stimme

Im Wahllokal erfolgen Autorisierung/Ausgabe des Stimmzettels und Stimmabgabe getrennt. Bei Briefwahl ist der ausgefüllte Stimmzettel in einem Umschlag beigelegt; hier muss der Wähler darauf vertrauen, dass die Mitarbeiter des Amtes das Stimmgeheimnis wahren. Bei REV verschärft sich dieses Problem.

Ein trojanisches Pferd auf dem Rechner des Wählers wäre in Estland wie in der Schweiz der in Lage, den Wahlkreis zu ermitteln (er ergibt sich aus der Liste der Kandidaten) und zu protokollieren, für wen die Stimme abgegeben wurde. Falls das trojanische Pferd verbreitet ist, kann sein Besitzer **das Wahlkreisergebnis hochrechnen** und abschätzen, in welchem Wahlkreis ein knappes Ergebnis zustande kommt. Wenn derjenige Kandidat das Mandat für den Wahlkreis gewinnt, der eine relative Mehrheit der Stimmen auf sich vereint (Mehrheitswahlrecht), kann ein winziger Vorsprung entscheidend sein. Angreifer könnten in solchen Wahlkreisen gezielt mobilisieren – wer einen Informationsvorsprung besitzt, wählt de facto mit einem höheren Stimmengewicht. In Estland könnte ein trojanisches Pferd mit seinen Geschwistern Attacken (Von-Geistes-Hand-Attacke, Verifizierungsattacke) koordinieren.

Wenn, Estland, auf dem Bildschirm der **Name des Wählers** [sic!] erscheint (in der Wahl-App, siehe Beispiel in [174], und in der Verifizierungs-App [46], übrigens auch in der digitalen Signatur der verschlüsselten Stimme), ist die Vertraulichkeit der Stimme aller Wähler mit einem eindeutigen Namen bedroht.

Ein Angreifer, der Informationen aus Telefonbüchern hinzuzieht oder Beziehungen zu Adresshändlern unterhält, kann die **Daten verknüpfen** und eine **Karte** erstellen, die das **Wahlverhalten in Abhängigkeit vom Wohnort** darstellt. In Deutschland dürfen Parteien bei den Meldebehörden Auskünfte über Wahlberechtigte anfragen, darunter Name und Anschrift.[28] Es würde genügen, wenn eine einzige nichtintegre Person, die Zugang zu solchen Daten hat, dem Angreifer zuarbeitet.

Der Besitzer des trojanischen Pferdes kann **auf dem gekaperten Rechner,** dies betrifft Estland wie die Schweiz, **nach Informationen suchen, die den Wähler identifizieren,** z. B. mehrere Rechnungen, die an ein und dieselbe Person adressiert sind; dann hätte er den Namen und die Adresse. Wir schätzen den zeitlichen Aufwand für einen solchen Angriff, wenn er teilautomatisiert wird (Skripte, reguläre Ausdrücke), auf eine Viertelstunde pro Wähler.[29]

Im Falle von REV per SMS, wie es in Großbritannien und in der Schweiz zeitweise möglich war [176, 83], flossen die Daten, von welchem Anschluss aus welche Partei gewählt wird, direkt bei den

[28] Der Wähler kann widersprechen, er muss den Widerspruch allerdings jährlich erneuern. [§ 50 Bundesmeldegesetz]

[29] Vor einem Angriff auf persönliche Daten könnte sich der Schweizer Wähler relativ einfach schützen, indem er für den Wahlakt ein Live-System hochfährt (Näheres dazu in [175]) – aber wie vielen Wählern leuchtet der Bedarf ein und wie viele werden sich das technisch zutrauen? – Alternativ wäre zu überlegen, ob man das System komplett auf Codes umstellt, die Namen der Kandidaten gar nicht mehr anzeigt, sondern bereits für die Auswahl einen Wahl-und-Wähler-individuellen Code eingeben lässt. Das hätte aber Auswirkungen auf die Architektur des Systems, vor allem das Berechnen der Auswahlbestätigungscodes. Davon ab stellt sich die Frage – Heiberg et al. wiesen darauf hin; wir zitierten sie in der ersten Fußnote auf Seite 17 –, wie das bei den Wählern ankäme.

Mobilfunkanbietern zusammen. Es wäre ein Leichtes gewesen, diese Daten mit dem Wohnort des Kunden zu verknüpfen.

Eine Partei könnte das Wahlverhalten, von dem sie weiß, zur Grundlage machen, **um potentielle Wähler gezielt zu umwerben.** Eine Regierungspartei erhielte mit Daten zum Wahlverhalten die ultimative Datengrundlage für ***Gerrymandering*** [177, 178, 179], das Neuziehen von Wahlkreisgrenzen mit dem Ziel, den eigenen Kandidaten den Gewinn des Wahlkreises zuzuschustern; Motiv b) von Seite 34, um bei der nächsten Wahl Motiv a) zu erreichen. In den USA ist *Gerrymandering* ein großes Thema: *Mit den heutigen … Datenerhebungen können die Parteien die Wahlkreise derart exakt entlang der Wohnorte ihrer Wähler ziehen, dass die Sieger meist bereits im Voraus feststehen. In solch ›sicheren Wahlkreisen‹ entscheidet die parteiinterne Vorwahl über den Einzug in den Kongress. Wer sie gewinnen will, muss einzig die eigene Basis überzeugen und kaum Rücksicht auf Wechselwähler nehmen. Bei den Wahlen zum Repräsentantenhaus … handelt es sich bei rund 90 % um solch ›sichere Sitze‹.* [179]

Spielt es wirklich eine Rolle, an welchen Kandidaten/welche Partei einzelne Mandate gehen? Ein Beispiel aus Deutschland: Hätte Die Linke bei der Bundestagswahl 2021 statt 3 nur 2 Direktmandate errungen, wäre sie, weil sie weniger als 5 % der Zweitstimmen erreicht hat, im 20. Deutschen Bundestag nicht mit 39, sondern nur mit 2 Abgeordneten vertreten.

Welche Folgen könnte ein Bruch der Vertraulichkeit der Stimme für den einzenen Wähler haben?

Beispiel 1. *Hacker schleichen sich in die elektronische Wahlurne des Kantons Zürich ein, stehlen die Daten der Wählenden und publizieren sie im Internet … sind nun Tausende Stimmbürger exponiert. Die Arbeitskollegin, die sich immer so wirtschaftsliberal gibt, hat die SP-Liste eingeworfen. Und der Bekannte, der für eine entwicklungspolitische NGO arbeitet, hat SVP gewählt.* [60] Man mag über die Beispiele schmunzeln – es ist dem Leser überlassen, sich analoge Konstellationen in seinem Heimatland vorzustellen –, sollte die **Gefahr des Rufschadens** aber ernst nehmen.[30]

Beispiel 2. Das Carter Centre hat festgestellt, dass Venezolaner Besorgnis geäußert haben, das REV-System ermögliche es den Behörden, herauszufinden, für wen sie gestimmt haben; befürchtet wurden Nachteile für diejenigen, die Chavez nicht gewählt haben. [180] Falls die Behörden herausfinden könnten, welcher Wähler für welche Partei gestimmt hat, wäre das **eine Datenbasis, mit der eine Regierung gezielt Oppositionelle identifizieren könnte** – das würde die Errichtung einer Diktatur erheblich vereinfachen. Da das Wahlverhalten einer Mehrheit der Menschen eine gewisse Trägheit besitzt, entsteht ein Problem, wenn die Vertraulichkeit der Stimme auch nur bei einer einzigen Wahl durchlässig wird.

Gibt es konkrete Gründe, bei REV einen Bruch der Vertraulichkeit der Stimme zu befürchten? Der Guardian berichtete 2003: *Swindon's e-votes are held in a data centre in Slough. The file … holds only the vote and a 10-digit personal identification number (Pin), randomly generated for this election – voters used it to log on to their chosen system. The file linking Pins to voters' names and addresses is held in Swindon. Sheffield's votes and voter lists are similarly separated … In both Swindon and Sheffield, the two databases will only be linked under a court order, in an electoral fraud case.* [34] Man war also technisch in der Lage, die Daten zusammenzuführen, und der Fall, Wahlbetrug (wie auch immer man einen solchen erkennen will), war sogar schon gesetzlich berücksichtigt. – Ein Projektleiter aus der Schweiz wurde in der NZZ 2005 wie folgt wiedergegeben: *Ein Zugriff auf die geöffnete elektronische Urne ist höchstens im Notfall und nur mit Bewilligung des Regierungsrats oder des Bundesrats möglich.* [181] Hier bleibt offen, ob die Stimmen zu diesem Zeitpunkt schon anonymisiert waren; in dem Fall bestünde allerdings gar kein Problem. – Heiberg et al. räumten 2011 ein: *It is theoretically possible for the NEC [National Electoral Committee] not to anonymize i-votes and use a modified VCS to break the secrecy of all ballots. To break the secrecy of one ballot, it is sufficient to decrypt it separately from others and later analyze audit log-files.* [81] In Estland war/ist man also technisch in der Lage, die Vertraulichkeit der Stimme zu brechen. – Die NZZ berichtete 2015, in einem Expertenbericht sei gezeigt worden, dass in dem REV-System des Consortiums Daten von Wählern nicht sauber gelöscht werden, es möglich gewesen wäre, herauszufinden, wer wie gewählt hat. [182] – Noch einmal Heiberg et al., 2016:

[30] Es wäre für viele Personen schädlich, wenn jemand ihre Wahlentscheidung öffentlich machen oder halbwegs glaubwürdig behaupten könnte, er wüsste, für wen sie gestimmt haben. Fußballer, Schauspieler, Autoren, Richter, Lehrer, Führungskräfte in der Wirtschaft oder im öffentlichen Dienst: Exponierte Personen können nur verlieren, wenn öffentlich wird, dass sie die Partei X gewählt haben – weil sie sich mit ihrer Entscheidung für die Partei X und gegen die Partei Y und gegen die Partei Z auf eine Seite gestellt haben. Die Vertraulichkeit der Stimme trägt ihren Teil dazu bei, eine politisch polarisierte Gesellschaft zu befrieden. Man würde auch bei anderen als weltanschaulichen Orientierungen kein *Outing* gegen den Willen der Betroffenen akzeptieren.

In principle, the EO [Election Organizer] is capable of breaking ballot secrecy completely. This means that the organizational integrity and private key management are crucial … [50]

Vor diesem Hintergrund verwundert es nicht, dass der Guardian 2015 warnte: *We are arriving at a point where the government has the ability to hold you accountable for how you vote. That is a 180-degree reversal of power.* [183] Wenn, obige Fälle, technisch die Möglichkeit besteht, die Vertraulichkeit der Stimme zu brechen – es wurde erläutert, welche gravierenden Folgen das haben könnte –, wird es mehr brauchen als Beteuerungen, das sei zwar möglich, aber man habe nicht vor, davon Gebrauch zu machen.

6 Zusammenfassung

Im Folgenden werden die wichtigsten Ergebnisse zu den REV-Systemen von Estland und der Schweiz zusammengefasst. Es wird auf Punkte hingewiesen, die in der künftigen Presseberichterstattung Berücksichtigung finden sollten.

Estland. 1. Trojanische Pferde können die Integrität der Stimme bedrohen. 2. Aufgrund der Architektur von Estlands REV-System ist es verhältnismäßig einfach, ein trojanisches Pferd so anzupassen, dass es neben dem Stimmverhalten die Identität des Abstimmenden (sein Name erscheint auf dem Bildschirm und in der digitalen Signatur) erfasst. Wenn man annehmen darf, dass in Estland ähnlich viele Rechner mit Schadsoftware infiziert sind wie in anderen Ländern, stellen trojanische Pferde für die Vertraulichkeit der Stimme eines nennenswerten Teils der Wähler in Estland eine ernstzunehmende Bedrohung dar. Die Möglichkeit, seine Stimme mehrmals abzugeben, schützt Estlands Wähler vor Zwang und Stimmen(ver)kauf.

Schweiz. Weil der Wähler mit dem REV-System Codes austauscht, können trojanische Pferde die Integrität der Stimme nicht bedrohen, sie können aber, auch wenn das Onlinesystem keine Kenntnis davon besitzt, welcher Bürger mit der jeweiligen Stimmkarte wählt, die Vertraulichkeit der Stimme einzelner Bürger bedrohen, und zwar dann, wenn sich ein Angreifer die (im Einzelfall geringe) Mühe macht, auf dem Rechner des Wählers nach persönlichen Daten zu suchen. Zwang und Stimmen(ver)kauf werden durch das Versenden von Codes und dadurch, dass die Schweizer Wähler ihre Stimme nur ein Mal abgeben dürfen, begünstigt, genau wie durch Briefwahl.

In der Presse wird selten thematisiert, welche **Auswirkungen** ein **Bruch der Vertraulichkeit der Stimme** für den einzelnen Bürger **haben kann,** nämlich Rufschädigung (und das längst nicht nur, wenn er ›die Falschen‹ wählt), und es wird selten thematisiert, welche Auswirkungen ein Bruch der Vertraulichkeit der Stimme eines nennenswerten Teils der Bürger haben kann, nämlich die Schaffung einer Datengrundlage, mit der sich nicht nur *Gerrymandering* betreiben lässt, sondern mit der eine weniger wohlmeinende Regierung Personen, die andere Parteien gewählt haben, das Leben schwer machen könnte.

Unabhängig von der Konstruktion des konkreten REV-Systems gilt: Das Manipulationsrisiko skaliert schon deswegen **hoch,** weil in die Durchführung von REV erheblich weniger Personen involviert sind als in die Durchführung einer klassischen Wahl im Wahllokal. Ob die Mitarbeiter, vgl. die Beobachtungen von Springall et al. [49], die vorgeschriebenen Abläufe (Vieraugenprinzip etc.) einhalten, lässt sich aus der Ferne schwer überwachen. Letztlich müssen die Wähler ihnen an dieser Stelle vertrauen. Das Vertrauen ließe sich stärken, wenn, sowohl was das Verfahren für die Auswahl der Mitarbeiter angeht als auch was die Einhaltung der Abläufe betrifft, nicht auf Sicherheit durch Geheimhaltung, sondern auf maximale Transparenz gesetzt wird. Auf jeden Fall sind an die Integrität der Mitarbeiter bedeutend höhere Anforderungen zu stellen, als sie an Mitarbeiter in Wahllokalen üblicherweise gestellt werden.

Zu kurz gekommen ist in der Presse, **welche Akteure ein Interesse an einer Manipulation der Wahl haben und über welche Ressourcen sie verfügen, ferner, über welche Beträge illegitim ins Amt gekommene Politiker disponieren können.** Solche Überlegungen sind aber die Voraussetzung dafür, das Thema Wahl ernst zu nehmen und die Eignung von Schutzmaßnahmen zu beurteilen.

In der öffentlichen Diskussion über REV bleibt immer wieder Aussage gegen Aussage stehen, z. B. in folgendem Zitat aus der NZZ: *Eine 100-prozentige Sicherheit vor bösartigen Angreifern gebe es nicht … Aber beim System [egal welches] könne zu 100 Prozent eruiert werden, ob und wann es bei der Stimmabgabe zu Manipulationen gekommen sei. Kritiker wenden ein, Verfälschungen würden teilweise gar nicht bemerkt.* [146] **Wie kann der eine ein System als hundertprozentig sicher bewerben und der andere immer noch Vorbehalte geltend machen?** Es muss nicht so sein, dass hier eine Seite irrt oder wider besseren Wissens Behauptungen aufstellt, und es muss auch nicht so sein, dass nur

eine Seite recht haben kann. Jedes System basiert auf Annahmen. Wenn die Annahmen gelten, dann sind die Schlussfolgerungen valide; falls aber auch nur eine Annahme nicht erfüllt ist, lassen sich die Garantien im Allgemeinen nicht mehr halten. Die Kritik betrifft also die Annahmen. **Durch entsprechende Annahmen lassen sich Probleme für erledigt erklären, die zu lösen alles andere als trivial ist.**

Von Bedeutung für die Debatte über REV ist schließlich die Erkenntnis: **Man kann nicht beweisen, dass ein System *nicht* gehackt worden ist – man kann lediglich beweisen, *dass* ein System gehackt worden ist.**

7 Ausblick

Wir gehen auf die aktuelle Planung für REV in der Schweiz ein und sprechen eine mögliche Richtung zukünftiger Forschung an.

Die Schweizerische Bundeskanzlei gab am 20. April 2022 folgenden Zwischenstand: *Das E-Voting-System, das die Schweizerische Post derzeit entwickelt, wurde massgeblich verbessert … Die Berichte [von Expertinnen und Experten aus Wissenschaft und Industrie] zeigen aber auch, dass weitere, zum Teil wesentliche Verbesserungen am System nötig sind. Die festgestellten Mängel betreffen u. a. das kryptografische Protokoll, das die Verifizierbarkeit unter Wahrung des Stimmgeheimnisses gewährleisten soll. Insbesondere sind für die Sicherheit mitentscheidende Aspekte teilweise noch nicht genügend klar dokumentiert, so dass offenbleibt, wie das System in den entsprechenden Punkten funktionieren soll.* [184]

Nehmen wir an, es gelingt den Schweizern in naher Zukunft, die festgestellten Mängel zur Zufriedenheit der Kryptografen zu lösen. Darf man das Problem, ein sicheres REV-System zu entwickeln, angesichts der Systeme, die in Estland bzw. in der Schweiz zum Einsatz kommen, dann als gelöst ansehen? Es ist sicherlich nicht falsch, festzuhalten, **dass es noch nicht gelungen ist, ein System zu entwickeln, bei dem sowohl die Integrität der Stimme als auch die Vertraulichkeit der Stimme vergleichbar sicher sind wie bei Wahl im Wahllokal.** Teague hält fest: *Nearly thirty years after the first voting-specific cryptography papers were written, some parts of the problem are solved while others seem as unachievable as ever. The more we learn about voting as a practical problem in security, the harder it seems.* [112] Fortschritte verspricht sie sich ausgerechnet von Forschung in Richtung Verifizierbarkeit von auf Papier abgegebenen Stimmen. [112]

Literatur

[1] *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*. State Electoral Office of Estonia. URL: https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia (besucht am 11. 06. 2022).

[2] *BESCHLUSS (EU, Euratom) 2018/994 DES RATES vom 13. Juli 2018 zur Änderung des dem Beschluss 76/787/ EGKS, EWG, Euratom des Rates vom 20. September 1976 beigefügten Akts zur Einführung allgemeiner unmittelbarer Wahlen der Mitglieder des Europäischen Parlaments*. Artikel 4a. 16. Juli 2018. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018D0994.

[3] Ülle Madise und Priit Vinkel. „Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience over Six Elections". In: *Regulating eTechnologies in the European Union*. Springer International Publishing, 2014, S. 53–72. ISBN: 9783319081168.

[4] *Microsoft-Electronic voting: What Europe can learn from Estonia*. 13. Mai 2019. URL: link.gale.com/apps/doc/A585269351/STND?u=fub&sid=bookmark-STND&xid=12e309ae (besucht am 23. 03. 2022).

[5] Norbert Kersting. „Online-Wahlen im internationalen Vergleich". In: *Aus Politik und Zeitgeschichte* (22. Apr. 2004). URL: https://www.bpb.de/shop/zeitschriften/apuz/28366/online-wahlen-im-internationalen-vergleich.

[6] Der Bundeswahlleiter. *Bundestagswahl 2021: Anteil der Briefwählerinnen und Briefwähler bei 47,3 %*. 15. Okt. 2021. URL: https://www.bundeswahlleiter.de/info/presse/mitteilungen/bundestagswahl-2021/53_21_briefwahlbeteiligung.html (besucht am 20. 04. 2022).

[7] Kim Zetter. *US voters living abroad sue for access to electronic voting*. 2. Okt. 2020. URL: https://www.theguardian.com/us-news/2020/oct/02/us-voting-electronic-lawsuit-voters-living-abroad (besucht am 15. 06. 2022).

[8] *Urnengang mit einem Mausklick*. NZZ. 17. Mai 2011. URL: https://www.wiso-net.de/document/NZZ__e3ae1c4b2bbf49c12fd53e692a131a24cf94dda2.

[9] *Election special: Polling experiments win popular vote*. The Guardian. 6. Mai 2000. URL: https://link.gale.com/apps/doc/A75766171/AONE?u=fub&sid=bookmark-AONE&xid=9b62ddf6.

[10] *Die e-ssoufflierte Demokratie*. NZZ. 13. Jan. 2001. URL: https://www.wiso-net.de/document/NZZ__643c08ee597adff43547c935d677217c771ca33d.

[11] *Five things that got broken at the oldest hacking event in the world; Information security took a hammering at Chaos Communications Congress, with intercoms, smart meters and even numbers themselves in the spotlight*. The Guardian. 5. Jan. 2017. URL: https://link.gale.com/apps/doc/A476613601/AONE?u=fub&sid=bookmark-AONE&xid=9adaba41.

[12] *Politische Rechte im digitalen Zeitalter*. NZZ. 22. Aug. 2013. URL: https://www.wiso-net.de/document/NZZ__5b2a0e9d95161fd6e4b5851d81d26dbc8639b96b.

[13] *Es braucht einen Neustart für das E-Voting*. NZZ. 27. März 2019. URL: https://www.wiso-net.de/document/NZZ__79438cc3285bd74ca6ef6deaca50f571e923c49c.

[14] Swiss Post. *Swiss Post Voting System. System specification, Version 1.0.0*. Based on original work by Scytl Secure Electronic Voting S.A. (succeeded by Scytl Election Technologies S.L.U.), modified by Swiss Post. 24. Juni 2022. URL: https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/raw/master/System/System_Specification.pdf (besucht am 06. 08. 2022).

[15] *Electronic Voting*. URL: https://history.house.gov/Exhibitions-and-Publications/Electronic-Technology/Electronic-Voting/ (besucht am 11. 03. 2022).

[16] Barbara Ondrisek. *Sicherheit elektronischer Wahlen. Eine Methode zur Bewertung und Optimierung der Sicherheit von E-Voting-Systemen*. Dissertation, Technische Universität Wien. Mai 2008. URL: https://resolver.obvsg.at/urn:nbn:at:at-ubtuw:1-27919 (besucht am 03. 09. 2022).

[17] J Paul Gibson, Robert Krimmer, Vanessa Teague und Julia Pomares. „A review of E-voting: the past, present and future“. In: *Annales des télécommunications* 71.7-8 (2016), S. 279–286. ISSN: 0003-4347.

[18] Philipp Mayring. *Qualitative Inhaltsanalyse. Grundlagen und Techniken*. Beltz, 2010, S. 3–58.

[19] Ulrike Schott-Maire, Manuel Riel und Ralf Romeike. „Expertenmeinungen über Bildung zur IT-Sicherheit: Was jeder Mensch wissen sollte!“ In: *INFOS 2021 – 19. GI-Fachtagung Informatik und Schule*. Hrsg. von Ludger Humbert. Gesellschaft für Informatik, Bonn, 2021, S. 83–92. DOI: 10.18420/infos2021_f258.

[20] *Will the US elections be hacked? It's doubtful, but machines could be 'rigged'; The fact that most election machines are not connected to the internet makes hacking unlikely, but the software itself could be vulnerable*. The Guardian. 6. Aug. 2016. URL: https://link.gale.com/apps/doc/A460098266/AONE?u=fub&sid=bookmark-AONE&xid=e560aab7.

[21] *International: Race for the White House: Ballot debacle predicted for November 4: High turnout and passions may defeat voting system: Pew group warning comes as early polling begins*. The Guardian. 22. Okt. 2008. URL: https://link.gale.com/apps/doc/A187560494/AONE?u=fub&sid=bookmark-AONE&xid=b288876c.

[22] Jessica Cunti. *Das Gefängnis macht sie zu Bürgern ohne Stimmrecht. In den USA dürfen Millionen Häftlinge und ehemalige Insassen nicht wählen. In einigen Swing States würden ihre Stimmen den Ausgang wesentlich beeinflussen.* 1. Nov. 2012. URL: https://www.zeit.de/politik/ausland/2012-11/usa-wahl-haeftlinge-wahlverbot.

[23] *Verfahren gegen „Zeit“-Chef di Lorenzo eingestellt*. 18. Nov. 2014. URL: https://www.welt.de/politik/deutschland/article134483671/Verfahren-gegen-Zeit-Chef-di-Lorenzo-eingestellt.html.

[24] *Verordnung der BK über die elektronische Stimmabgabe (VEleS)*. 25. Mai 2022. URL: https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/2022/336/20220701/de/pdf-a/fedlex-data-admin-ch-eli-cc-2022-336-20220701-de-pdf-a-1.pdf (besucht am 07. 08. 2022).

[25] *Hintergrund: Wahlen in der DDR. Die Volkskammerwahl 1986*. URL: https://www.planet-schule.de/wissenspool/alltag-in-der-ddr/inhalt/hintergrund/wahlen-in-der-ddr.html (besucht am 15. 06. 2022).

[26] *Wählen und Auswählen*. NZZ. 12. Dez. 2015. URL: https://www.wiso-net.de/document/NZZ__9d08900d55886ac9734ce579f7a4376e552eb335.

[27] *Schwierigkeiten bei der Stimmabgabe in Berlin*. Zeit online. 26. Sep. 2021. URL: https://www.zeit.de/politik/deutschland/2021-09/wahllokale-berlin-bundestagswahl-berliner-wahl-wartezeiten-stimmzettel.

[28] Julius Betschka. *Prüfungsausschuss des Bundestags will Neuwahl in 400 Berliner Wahllokalen*. 8. Juli 2022. URL: https://www.tagesspiegel.de/berlin/landeswahlleitung-haelt-wiederholung-fuer-unnoetig-pruefungsausschuss-des-bundestags-will-neuwahl-in-400-berliner-wahllokalen/28490140.html.

[29] *Ungültige Stimmabgabe*. URL: https://www.bundeswahlleiter.de/service/glossar/u/ungueltige-stimmabgabe.html (besucht am 11. 06. 2022).

[30] *Ungültiger Stimmzettel*. URL: https://www.bundeswahlleiter.de/service/glossar/u/ungueltiger-stimmzettel.html (besucht am 11. 06. 2022).

[31] *Digitale Demokratie verlangt Pioniergeist*. NZZ. 25. Sep. 2015. URL: https://www.wiso-net.de/document/NZZ__a8c8370a0e6ca9aa141f77791985108 59f5343e5.

[32] *Bekommen Auslandschweizer ihre Stimmcouverts bald per Diplomatenpost?* NZZ. 3. Apr. 2021. URL: https://www.wiso-net.de/document/NZZ__39bff8fd994790cc645425d36925a12f0d2c048d.

[33] *E-Voting: Faktenblatt*. Dez. 2020. URL: https://www.bk.admin.ch/dam/bk/de/dokumente/pore/E-Voting_%20Faktenblatt.pdf.download.pdf/E-Voting_%20Faktenblatt.pdf (besucht am 18. 03. 2022).

[34] *Inside IT: X marks the spot: Today's local elections mark the biggest experiment so far in e-voting*. The Guardian. 1. Mai 2003. URL: https://link.gale.com/apps/doc/A100975555/AONE?u=fub&sid=bookmark-AONE&xid=9f4e3c43.

[35] *Off cuts*. The Guardian. 5. Apr. 2000. URL: https://link.gale.com/apps/doc/A75779759/AONE?u=fub&sid=bookmark-AONE&xid=364835ca.

[36] *Turbos, Bremser und Trittbrettfahrer*. NZZ. 11. Nov. 2016. URL: https://www.wiso-net.de/document/NZZ__49b3b99f26db4537371f539045b7c083b8d4aee5.

[37] *Should Britain introduce electronic voting? Using technology instead of paper ballots reduces costs and could boost voter turnout – but questions remain over security and possible electoral fraud; Using technology instead of paper ballots reduces costs and could boost voter turnout – but questions remain over security and possible electoral fraud*. The Guardian. 26. Feb. 2015. URL: https://link.gale.com/apps/doc/A403272231/AONE?u=fub&sid=bookmark-AONE&xid=69b345db.

[38] *Hohe Beteiligung an der ersten Internet-Abstimmung*. NZZ. 20. Jan. 2003. URL: https://www.wiso-net.de/document/NZZ__3c78035b58be60f887afc07c5b978ef05e06ea02.

[39] *Maus statt Stimmzettel / Erfolgreicher E-Voting-Versuch in Genf*. NZZ. 27. Sep. 2004. URL: https://www.wiso-net.de/document/NZZ__d77c72991f350a32f2fde2dc450336bfedecbd95.

[40] *Society: epublic: Poll position: Does e-voting mean the end of the ballot box? Michael Cross investigates*. The Guardian. 8. Okt. 2003. URL: https://link.gale.com/apps/doc/A108689075/AONE?u=fub&sid=bookmark-AONE&xid=fc1e514d.

[41] *Bald ein Schwarzmarkt für Wahlergebnisse?* NZZ. 19. Nov. 2013. URL: https://www.wiso-net.de/document/NZZ__19b08c926f4b7f063dd999d1ce7b8aff83d4ca04.

[42] Nelson Hastings, Rene Peralta, Stefan Popoveniuc und Andrew Regenscheid. *Security Considerations for Remote Electronic UOCAVA Voting. NISTIR 7770*. URL: https://www.nist.gov/system/files/documents/itl/vote/NISTIR-7700-feb2011.pdf (besucht am 06. 08. 2022).

[43] Chaos Computer Club Schweiz (CCC-CH). *Vernehmlassungsantwort E-BPR: E-Voting ist ein Hochrisikoprojekt*. 30. Apr. 2019. URL: https://chaosticino.ch/docs/20190430-vernehmlassung--e-voting-ordentlicher-betrieb.pdf (besucht am 12. 04. 2022).

[44] *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*. State Electoral Office of Estonia, 20. Juni 2017. URL: https://www.valimised.ee/en/internet-voting/more-about-i-voting/general-framework-electronic-voting (besucht am 17. 03. 2022).

[45] *Activities of i-voting and voting on paper compared*. Valimised (= Estländisches Wahlportal). URL: https://www.valimised.ee/en/internet-voting/more-about-i-voting/activities-i-voting-and-voting-paper-compared (besucht am 10. 07. 2022).

[46] *IVXV Protocols. Specification, Versioon 1.6.0, 53 lk, Dok IVXV-PR-EN-1.6.0*. 31. Mai 2020. URL: https://www.valimised.ee/sites/default/files/2021-05/IVXV%20protocols%20%E2%80%93%20data%20structures%20and%20data%20exchange%20protocols.pdf (besucht am 07. 08. 2022).

[47] *Voter applications and checking authenticity*. Valimised (= Estländisches Wahlportal). URL: https://www.valimised.ee/index.php/en/internet-voting/guidelines/voter-applications-and-checking-authenticity (besucht am 17. 03. 2022).

[48] *Activities of i-voting and voting on paper compared*. URL: https://www.valimised.ee/en/internet-voting/more-about-i-voting/activities-i-voting-and-voting-paper-compared (besucht am 13. 08. 2022).

[49] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine und J. Alex Halderman. „Security Analysis of the Estonian Internet Voting System". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. CCS '14. Scottsdale, Arizona, USA: Association for Computing Machinery, 2014, S. 703–715. ISBN: 9781450329576. URL: https://doi.org/10.1145/2660267.2660315.

[50] Sven Heiberg, Tarvi Martens, Priit Vinkel und Jan Willemson. „Improving the Verifiability of the Estonian Internet Voting Scheme“. In: *Electronic Voting. First International Joint Conference, E-Vote-ID 2016*. Hrsg. von Robert Krimmer u. a. Okt. 2016, S. 92–107. ISBN: 3319522396. DOI: 10.1007/978-3-319-52240-1_6.

[51] Sven Heiberg und Jan Willemson. „Verifiable internet voting in Estonia“. In: *6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*. 2014, S. 1–8. DOI: 10.1109/EVOTE.2014.7001135.

[52] Schweizerische Bundeskanzlei. *Chronik*. URL: https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/chronik.html (besucht am 31. 08. 2022).

[53] Schweizerische Bundeskanzlei. *Vote électronique*. URL: https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting.html (besucht am 31. 08. 2022).

[54] *Neuenburger setzen fürs E-Voting auf die Post*. 1. Sep. 2015. URL: https://www.handelszeitung.ch/unternehmen/neuenburger-setzen-fuers-e-voting-auf-die-post-849341 (besucht am 31. 08. 2022).

[55] *Schwerer Rückschlag für das Wählen per Mausklick*. NZZ. 13. Aug. 2015. URL: https://www.wiso-net.de/document/NZZ__dab80a0b9fa8be5d2e51da85f440dc044d2727cd.

[56] *Der grösste E-Voting-Verbund steht vor dem Aus*. NZZ. 17. Sep. 2015. URL: https://www.wiso-net.de/document/NZZ__3b4c260a06fc1a9605df23a8fea393cd657f63e1.

[57] Jan Gerlach und Urs Gasser. *Three Case Studies from Switzerland: E-Voting*. März 2009. URL: https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf.

[58] *E-Voting-Union löst sich auf*. NZZ. 22. Sep. 2015. URL: https://www.wiso-net.de/document/NZZ__3a5b91d09ee84e05cee7f4dad38aa0863b5a2269.

[59] *Plan für E-Voting war zu ambitiös - Bundesrat legt eine Pause ein*. NZZ. 28. Juni 2019. URL: https://www.wiso-net.de/document/NZZ__c18f215de663c0056948fac47db2421c38f4644c.

[60] *Mehr E-Demokratie wagen*. NZZ. 5. Nov. 2015. URL: https://www.wiso-net.de/document/NZZ__9470032c0e94a6f16d54a5f1785430479f1fefd6.

[61] *Fehler im E-Voting-System entdeckt*. NZZ. 13. März 2019. URL: https://www.wiso-net.de/document/NZZ__b869822791ba17f6cf4cbd4e15d2085a3addab13.

[62] *Schritt für Schritt zum E-Voting*. NZZ. 18. Dez. 2014. URL: https://www.wiso-net.de/document/NZZ__81ed3b000f99ed1e72da7441e2a30fc975bbcfd6.

[63] *Post gibt ihr E-Voting-System per sofort auf*. NZZ. 6. Juli 2019. URL: https://www.wiso-net.de/document/NZZ__211a5c96b59f6ed79f58edf2d298f41621aea897.

[64] *E-Voting der Post geht in nächste Entwicklungsphase*. Medienmitteilung. 20. Apr. 2022. URL: https://www.post.ch/de/ueber-uns/medien/medienmitteilungen/2022/e-voting-der-post-geht-in-naechste-entwicklungsphase (besucht am 11. 08. 2022).

[65] Swiss Post. *Swiss Post Voting System. E-Voting Architecture Document, v1.0.0*. 24. Juni 2022. URL: https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/raw/master/System/SwissPost_Voting_System_architecture_document.pdf (besucht am 06. 08. 2022).

[66] Swiss Post. *Cryptographic Primitives of the Swiss Post Voting System. Pseudo-code Specification, Version 1.0.0*. 24. Juni 2022. URL: https://gitlab.com/swisspost-evoting/crypto-primitives/crypto-primitives/-/raw/master/Crypto-Primitives-Specification.pdf?inline=false (besucht am 07. 08. 2022).

[67] Swiss Post. *Protocol of the Swiss Post Voting System. Computational Proof of Complete Verifiability and Privacy, Version 1.0.0*. 24. Juni 2022. URL: https://gitlab.com/swisspost-evoting/crypto-primitives/crypto-primitives/-/raw/master/Crypto-Primitives-Specification.pdf?inline=false (besucht am 07. 08. 2022).

[68] Sarah Jamie Lewis, Olivier Pereira und Vanessa Teague. *Ceci n'est pas une preuve. The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiabilty of the Scytl-SwissPost Internet voting system*. 12. März 2019. URL: https://cva.unifr.ch/content/ceci-n%E2%80%99est-pas-une-preuve-use-trapdoor-commitments-bayer-groth-proofs-and-implications (besucht am 12. 04. 2022).

[69] *Schlußbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft*. Deutscher Bundestag, 22. Juni 1998. URL: https://dserver.bundestag.de/btd/13/110/1311004.pdf (besucht am 16. 03. 2022).

[70] Richard Sietmann. *Dreimal drücken – fertig? E-Voting-Großeinsatz bei der Bundestagswahl*. 5. Sep. 2005. URL: https://www.heise.de/ct/artikel/Dreimal-druecken-fertig-290088.html (besucht am 30. 08. 2022).

[71] Deutscher Bundestag. *Dritte Beschlussempfehlung des Wahlprüfungsausschusses zu 44 gegen die Gültigkeit der Wahl zum 16. Deutschen Bundestag eingegangenen Wahleinsprüchen. Drucksache 16/3600*. 30. Nov. 2006. URL: https://dserver.bundestag.de/btd/16/036/1603600.pdf.

[72] Zweiter Senat des Bundesverfassungsgerichts. *Urteil 2 BvC 3/07, 2 BvC 4/07*. Bundesverfassungsgericht, 3. März 2009. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/03/cs20090303_2bvc000307.html (besucht am 16. 03. 2022).

[73] Constanze Kurz und Frank Rieger. „NEDAP-Wahlcomputer – Manipulationsmethoden an Hard- und Software." In: *Informatik Spektrum* 30 (28. Aug. 2007), S. 313–321. URL: https://doi.org/10.1007/s00287-007-0182-4 (besucht am 21. 03. 2022).

[74] Melanie Volkamer, Guido Schryen, Lucie Langer, Axel Schmidt und Johannes Buchmann. „Elektronische Wahlen: Verifizierung vs. Zertifizierung". In: *Informatik 2009 – Im Focus das Leben*. Hrsg. von Stefan Fischer, Erik Maehle und Rüdiger Reischuk. Bonn: Gesellschaft für Informatik e. V., 2009, S. 207–207.

[75] *Eidgenössische Volksinitiative ›Für eine sichere und vertrauenswürdige Demokratie (E-Voting-Moratorium)‹*. URL: https://www.bk.admin.ch/ch/d/pore/vi/vis493t.html (besucht am 02. 09. 2022).

[76] *Eidgenössische Volksinitiative ›Für eine sichere und vertrauenswürdige Demokratie (E-Voting-Moratorium)‹*. URL: https://www.bk.admin.ch/ch/d/pore/vi/vis493.html (besucht am 02. 09. 2022).

[77] *Estland ist auf der E-Voting-Überholspur*. NZZ. 26. Juli 2018. URL: https://www.wiso-net.de/document/NZZ__442e21399e0ac37424e870085b1eb6812ce0ba42.

[78] Andreas Eschbach. *Ein König für Deutschland*. 1. Auflage. Bastei Lübbe, Juli 2011.

[79] Barbara Ondrisek und Peter Purgathofer. *Nicht schon wieder E-Voting!* 18. Nov. 2020. URL: https://papierwahl.at/ (besucht am 12. 07. 2022).

[80] Bianca Schroeder, Eduardo Pinheiro und Wolf-Dietrich Weber. „DRAM Errors in the Wild: A Large-Scale Field Study". In: *Proceedings of the Eleventh International Joint Conference on Measurement and Modeling of Computer Systems*. SIGMETRICS '09. Seattle, WA, USA: Association for Computing Machinery, 2009, S. 193–204. ISBN: 9781605585116. DOI: 10.1145/1555349.1555372. URL: https://doi.org/10.1145/1555349.1555372.

[81] Sven Heiberg, Peeter Laud und Jan Willemson. „The Application of I-Voting for Estonian Parliamentary Elections of 2011". In: *3rd International Conference on E-Voting and Identity*. Sep. 2011, S. 208–223. ISBN: 978-3-642-32746-9. DOI: 10.1007/978-3-642-32747-6_13.

[82] *Open Source als Vertrauensgarantie*. NZZ. 22. Dez. 2015. URL: https://www.wiso-net.de/document/NZZ__2859399a5faac27abb9703ed4fcbc0de1a6399f3.

[83] *Kumulieren und panaschieren per SMS und Internet / Mit den Bülacher Stadt- und Gemeinderatswahlen nimmt E-Voting im Kanton Zürich die nächste Hürde*. NZZ. 30. März 2006. URL: https://www.wiso-net.de/document/NZZ__8b2dfa95250bbd4822e79f38ea85afac841552ea.

[84] *Technology: Inside IT: Why machines are bad at counting votes: Democracy is made difficult by the fact that electronic voting systems are inherently flawed - and susceptible to fraud*. The Guardian. 30. Apr. 2009. URL: https://link.gale.com/apps/doc/A198789705/AONE?u=fub&sid=bookmark-AONE&xid=65b30150.

[85] René Droz. *E-Voting – Das Ende der Demokratie. Jetzt legen wir uns ein Kuckucksei ins Netz*. URL: https://www.noevoting.ch/public/downloadable/Das_Ende_der_Demokratie_18-01.pdf (besucht am 09. 05. 2022).

[86] Kristian Gjøsteen. *The Norwegian Internet Voting Protocol*. Cryptology ePrint Archive, Report 2013/473. 2013-08-09. URL: https://ia.cr/2013/473 (besucht am 03. 05. 2022).

[87] *Why eletronic voting isn't secure – but may be safe enough; We bank online, so why can't we vote online? There's good reason, argue security experts*. The Guardian. 30. März 2015. URL: https://link.gale.com/apps/doc/A407635042/AONE?u=fub&sid=bookmark-AONE&xid=0c376b36.

[88] *Sicherheit im E-Voting / Facettenreiche Probleme bei Wahlen und Abstimmungen*. NZZ. 4. Feb. 2003. URL: https://www.wiso-net.de/document/NZZ__39f447fc99d5d21e02f5e4855b2575edf63dd901.

[89] Post CH Netz AG. *So können Bürgerinnen und Bürger überprüfen, dass ihre Stimmen beim E-Voting unverändert eingeworfen wurden*. Video 2. URL: https://www.post.ch/de/geschaeftsloesungen/e-voting/sicherheit-an-erster-stelle (besucht am 22. 08. 2022).

[90] *Post setzt weiterhin auf das E-Voting-System der insolventen Scytl*. NZZ. 23. Mai 2020. URL: https://www.wiso-net.de/document/NZZ__0127be6b1f30aaa3067267b037c87b35b89c6edc.

[91] *Comment &; Analysis: Political machinations: The government is keen to deploy e-voting despite evidence of ballot rigging*. The Guardian. 2. Feb. 2005. URL: https://link.gale.com/apps/doc/A128023981/AONE?u=fub&sid=bookmark-AONE&xid=9e165ebb.

[92] *E-Voting: Glossar*. Dez. 2020. URL: https://www.bk.admin.ch/dam/bk/de/dokumente/pore/E-Voting_%20Glossar.pdf.download.pdf/E-Voting_%20Glossar.pdf (besucht am 12. 04. 2022).

[93] *Automatisierung der Übersetzung*. URL: https://www.inf-schule.de/rechner/compiler/automatisierung (besucht am 06. 08. 2022).

[94] *Unter dem Titel «Mehr E-Demokratie wagen» plädiert …* NZZ. 16. Nov. 2015. URL: https://www.wiso-net.de/document/NZZ__adf4e1b7fecbf77b56f99afea348a1cfe2485452.

[95] *Das E-Voting erleidet einen weiteren schweren Rückschlag*. NZZ. 30. März 2019. URL: https://www.wiso-net.de/document/NZZ__c3e8bab34d1ab552b2d90773a758aa466450715d.

[96] Schweizerische Post. *E-Voting und Sicherheit. Höchste Sicherheitsstandards garantiert*. URL: https://www.post.ch/de/geschaeftsloesungen/e-voting/sicherheit-an-erster-stelle (besucht am 14. 08. 2022).

[97] *Das E-Voting braucht Nachbesserungen*. NZZ. 27. Apr. 2019. URL: https://www.wiso-net.de/document/NZZ__ef4f0f9330bc673503a45c844bf06dfbbd88e9fb.

[98] *Gefahren des E-Voting*. NZZ. 2. Mai 2011. URL: https://www.wiso-net.de/document/NZZ__9b905cafd3df13b0749f7166e24685e990b276bf.

[99] *E-Voting-System wird demokratisiert*. NZZ. 23. Jan. 2014. URL: https://www.wiso-net.de/document/NZZ__a56e086ead372094f2921e751f990351e2e85470.

[100] *Genfer Offensive beim E-Voting*. NZZ. 20. Aug. 2015. URL: https://www.wiso-net.de/document/NZZ__3f6fc79aa0da987cfce3641dfe506392a0ce9fb5.

[101] *Technology: Hacking the online ballot box: Today, some councils will offer voting via the internet. But exactly how accountable, secure, and desirable are the online polling systems? Danny Bradbury investigates*. The Guardian. 3. Mai 2007. URL: https://link.gale.com/apps/doc/A162936940/AONE?u=fub&sid=bookmark-AONE&xid=e31b53a3.

[102] *Der Bund kann Digitalisierung nicht. Er muss sie lernen*. NZZ. 10. Feb. 2021. URL: https://www.wiso-net.de/document/NZZ__4fe72f4b260334bb48fa7a704e0f9712c7409aaa.

[103] Steven Vaughan-Nichols. *Out-of-date, insecure open-source software is everywhere*. 12. Mai 2020. URL: https://www.zdnet.com/article/out-of-date-insecure-open-source-software-is-everywhere/ (besucht am 12. 07. 2022).

[104] *IVXV Architecture. Specification Versioon 1.4.0, 39 lk, Dok IVXV-AR-EN-1.4.0*. 18. Jan. 2019. URL: https://www.valimised.ee/sites/default/files/2021-05/IVXV%20architecture%20%E2%80%93%20overview%20of%20technical%20realisation.pdf (besucht am 07. 08. 2022).

[105] Tor E. Bjørstad. *The rise and fall of Internet Voting in Norway (and the spiders from Mars). Vortrag auf dem 31. Chaos Communication Congress*. 30. Dez. 2014. URL: https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2551/original/31c3-final.pdf (besucht am 03. 05. 2022).

[106] *Die Post lässt Hacker auf das E-Voting-System los*. NZZ. 26. Feb. 2019. URL: https://www.wiso-net.de/document/NZZ__3d6dcec830e31e1ef75ff2fd45142314c68170f6.

[107] *Die digitale Stimmabgabe wird sicher*. NZZ. 19. Mai 2018. URL: https://www.wiso-net.de/document/NZZ__7e4bd56261b56317aab911dca7d5b650334d55cc.

[108] Barbara Simons und Douglas W. Jones. „Internet Voting in the U.S.“ In: *Communications of the ACM* 55.10 (Okt. 2012), S. 68–77. ISSN: 0001-0782. DOI: 10.1145/2347736.2347754. URL: https://doi.org/10.1145/2347736.2347754.

[109] Karl R. Popper. „Logik der Forschung“. In: Bd. 4. Die Einheit der Gesellschaftswissenschaften. 10., verb. u. vermehrte Aufl. Mohr, 1994. ISBN: 3-16-146234-3.

[110] Ariel J. Feldman, J. Alex Halderman und Edward W. Felten. *Security Analysis of the Diebold AccuVote-TS Voting Machine*. 13. Sep. 2006. URL: https://citpsite.s3.amazonaws.com/wp-content/uploads/2019/01/23191614/ts06full.pdf (besucht am 14. 08. 2022).

[111] Bev Harris. *Backdoor Found In Diebold Vote Counting Program*. 2. Sep. 2004. URL: https://www.scoop.co.nz/stories/HL0409/S00027.htm (besucht am 27. 08. 2022).

[112] Vanessa Teague. „Which E-Voting Problems Do We Need to Solve?“ In: *Advances in Cryptology – CRYPTO 2021*. Lecture Notes in Computer Science. Springer International Publishing, 2021, S. 3–7. ISBN: 303084241X.

[113] *Haben die USA aus den Hackerangriffen gelernt?* NZZ. 17. Okt. 2020. URL: https://www.wiso-net.de/document/NZZ__c955a0e676c24ba3f0342f484bcd5a657e2bf72d.

[114] U.S. Election Assistance Commission. *Election Audits Across the United States*. 6. Okt. 2021. URL: https://www.eac.gov/sites/default/files/bestpractices/Election_Audits_Across_the_United_States.pdf (besucht am 14. 08. 2022).

[115] *What's at stake as India's 900m voters head for the polls? The world's biggest democracy will this week begin the 40-day process of choosing a new government in which an eighth of the world's population will have the vote; The world's biggest democracy will this week begin the 40-day process of choosing a new government in which an eighth of the world's population will have the vote*. The Guardian. 8. Apr. 2019. URL: https://link.gale.com/apps/doc/A581654404/AONE?u=fub&sid=bookmark-AONE&xid=3c2b7e94.

[116] *Online: Public Domain: Voting against internet elections: More delays for e-democracy as a new report raises major security concerns. By Michael Cross*. The Guardian. 12. Feb. 2004. URL: https://link.gale.com/apps/doc/A113214724/AONE?u=fub&sid=bookmark-AONE&xid=89f00b49.

[117] *Alle E-Voting-Systeme wurden gehackt*. NZZ. 2. März 2018. URL: https://www.wiso-net.de/document/NZZ__fb487cc43e02e8bcfc3678ec7a584225e6c5e8d7.

[118] *Abstimmen übers Internet spaltet die Fachwelt*. NZZ. 11. Mai 2018. URL: https://www.wiso-net.de/document/NZZ__8adb95614c17d69f8afbc787ba968ce81d06d44e.

[119] *Die E-Voting-Lösung der Post. Online wählen und abstimmen – einfach und sicher*. URL: https://www.post.ch/de/geschaeftsloesungen/e-voting/die-e-voting-loesung-fuer-kantone (besucht am 14. 08. 2022).

[120] Nicole Perlroth, Jeff Larson und Scott Shane. *N.S.A. Able To Foil Basic Safeguards Of Privacy On Web*. 6. Sep. 2013. URL: https://link.gale.com/apps/doc/A341964396/AONE?u=fub&sid=bookmark-AONE&xid=2ae7efb2 (besucht am 07. 08. 2022).

[121] *Politische Rechte im Digitalzeitalter*. NZZ. 20. Aug. 2013. URL: https://www.wiso-net.de/document/NZZ__c18356bbb19f2813935cbece1adb4b0da490cd5c.

[122] *Unsicheres E-Voting*. NZZ. 15. Aug. 2013. URL: https://www.wiso-net.de/document/NZZ__dd3a201387c7a2c754edf9ebb60798a907e53846.

[123] Akila Welihinda. *How To Build an Evil Compiler*. URL: https://www.awelm.com/posts/evil-compiler/ (besucht am 13. 08. 2022).

[124] Dimitris A Gritzalis. „Principles and requirements for a secure e-voting system". In: *Computers & security* 21.6 (2002), S. 539–556. ISSN: 0167-4048.

[125] *Langer Weg zum Wählen per Mausklick*. NZZ. 15. Aug. 2014. URL: https://www.wiso-net.de/document/NZZ__aa9fbeaa380f6b442775a7a841a68bd0739691c0.

[126] *Demokratie verträgt nicht das leiseste Misstrauen*. NZZ. 6. Apr. 2018. URL: https://www.wiso-net.de/document/NZZ__528de1690889704cccd820298707007db8079295.

[127] Andrew Appel. *How the Swiss Post E-voting system addresses client-side vulnerabilities*. 29. Juni 2022. URL: https://freedom-to-tinker.com/2022/06/29/how-the-swiss-post-e-voting-system-addresses-client-side-vulnerabilities/ (besucht am 06. 08. 2022).

[128] Dietmar Wätjen. *Kryptographie. Grundlagen, Algorithmen, Protokolle*. Köln: Bastei Lübbe Taschenbuch, 2018. URL: https://doi.org/10.1007/978-3-658-22474-5.

[129] *Society: Cross culture: The government is putting its faith in the potential of electronic voting to the test in tomorrow's local elections. But are indifference and disillusionment the real enemies of democracy?* The Guardian. 30. Apr. 2003. URL: https://link.gale.com/apps/doc/A100889055/AONE?u=fub&sid=bookmark-AONE&xid=3955ab66.

[130] Peter Purgathofer. *E-Voting sollten wir nicht machen*. 3. März 2009. URL: https://www.bizeps.or.at/e-voting-sollten-wir-nicht-machen/ (besucht am 21. 03. 2022).

[131] R. L. Rivest, A. Shamir und L. Adleman. „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Communications of the ACM* 21.2 (Feb. 1978), S. 120–126. DOI: 10.1145/359340.359342.

[132] Taher ElGamal. „A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". In: *Advances in Cryptology*. Hrsg. von George Robert Blakley und David Chaum. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, S. 10–18. ISBN: 978-3-540-39568-3.

[133] Michael Brenner. *Rechnen mit sieben Siegeln. Verschlüsselt rechnen mit homomorpher Verschlüsselung*. 2016. URL: https://www.heise.de/select/ct/2016/6/1457858670546232 (besucht am 24. 08. 2022).

[134] *Online letter: Second sight: Text for the next PM*. The Guardian. 28. Nov. 2002. URL: https://link.gale.com/apps/doc/A94710119/AONE?u=fub&sid=bookmark-AONE&xid=a8e764f3.

[135] Bundesamt für Sicherheit in der Informationstechnik. „BSI – Technische Richtlinie TR-02102-1. Kryptographische Verfahren: Empfehlungen und Schlüssellängen". In: (28. Jan. 2022). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=5.

[136] Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter. *Moderne Verfahren der Kryptographie. Von RSA zu Zero-Knowledge*. Wiesbaden: Friedr. Vieweg & Sohn Verlag/GWV Fachverlage GmbH, 2006.

[137] *Kryptologische Hash-Funktion*. URL: https://www.inf-schule.de/kryptologie/digitalesignatur/konzept_hashfunktion (besucht am 06. 08. 2022).

[138] *Staat und Internet / Standortbestimmung zum E-Government*. NZZ. 26. März 2001. URL: https://www.wiso-net.de/document/NZZ__22118c88b899be81c051992b894b7d310e6dcc30.

[139] *Zertifikate*. URL: http://ddi.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page10.html (besucht am 06. 08. 2022).

[140] *Was ist ein digitales Zertifikat?* URL: https://www.inf-schule.de/kryptologie/sicherheitsinfrastruktur/konzept_zertifikat (besucht am 06. 08. 2022).

[141] Stephanie Bayer und Jens Groth. „Efficient Zero-Knowledge Argument for Correctness of a Shuffle". In: *Advances in Cryptology – EUROCRYPT 2012*. Hrsg. von David Pointcheval und Thomas Johansson. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, S. 263–280. ISBN: 978-3-642-29011-4.

[142] *Open Verificatum*. URL: https://www.verificatum.org/ (besucht am 14. 08. 2022).

[143] Udo Hebisch. *Anagramm*. URL: http://www.mathe.tu-freiberg.de/~hebisch/cafe/kryptographie/anagramm.html (besucht am 14. 08. 2022).

[144] *Gegner des E-Votings spüren Aufwind*. NZZ. 15. Aug. 2015. URL: https://www.wiso-net.de/document/NZZ__516886f2e064093f69e9276c8e1dcd34446cddee.

[145] Thomas Haines, Sarah Jamie Lewis, Olivier Pereira und Vanessa Teague. „How not to prove your election outcome". eng. In: *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, S. 644–660. ISBN: 9781728134970.

[146] *Schritt für Schritt zu mehr E-Voting*. NZZ. 3. Dez. 2016. URL: https://www.wiso-net.de/document/NZZ__5a7981c9b1362fcf64b193daa7afb57886d581d9.

[147] *US elections 2004: Dirty tricks return to the sunshine state: US election begins with voting in Florida dogged by controversy over faulty machines and disenfranchised voters*. The Guardian. 19. Okt. 2004. URL: https://link.gale.com/apps/doc/A123372124/AONE?u=fub&sid=bookmark-AONE&xid=fc68d8f5.

[148] *(Wo)Man in the middle Angriff*. URL: https://www.inf-schule.de/kryptologie/sicherheitsinfrastruktur/einstieg_maninthemiddleangriff (besucht am 14. 07. 2022).

[149] *NSW election result could be challenged over iVote security flaw; 'Major vulnerability' revealed in the online voting system could have compromised 66,000 electronic votes*. The Guardian. 23. März 2015. URL: https://link.gale.com/apps/doc/A406549590/AONE?u=fub&sid=bookmark-AONE&xid=89f1f52f.

[150] Dennis Schirrmacher. *Freak Attack: SSL-Verschlüsselung von Millionen Webseiten angreifbar*. 4. März 2015. URL: https://www.heise.de/security/meldung/Freak-Attack-SSL-Verschluesselung-von-Millionen-Webseiten-angreifbar-2566444.html.

[151] *Drive-by attack*. URL: https://encyclopedia.kaspersky.com/glossary/drive-by-attack/ (besucht am 07. 08. 2022).

[152] Andy Greenberg. *Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits*. 23. März 2012. URL: https://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/?sh=3a87fb92660b (besucht am 07. 08. 2022).

[153] *S-Protect: c't entdeckt Sicherheitsmängel in Banking-Software der Sparkasse. Sicheres Online-Banking, sogar auf infizierten Rechnern: Das klingt unmöglich? Nicht weniger versprechen Sparkassen mit ihrem Banking-Browser S-Protect.* 3. Juni 2022. URL: https://www.heise.de/news/c-t-entdeckt-Sicherheitsmaengel-in-Banking-Software-der-Sparkasse-7126688.html.

[154] *MiVote aims to shake up democratic process with a click and a tap; It's about more choices, says start-up, which wants to harness the internet and mobile devices to let voters set Australia's direction*. The Guardian. 14. Apr. 2017. URL: https://link.gale.com/apps/doc/A489633177/AONE?u=fub&sid=bookmark-AONE&xid=8ae05642.

[155] *Requirements to the voter and their computer*. Valimised (= Estländisches Wahlportal). URL: https://www.valimised.ee/en/internet-voting/guidelines/requirements-voter-and-their-computer (besucht am 17. 03. 2022).

[156] *Questions about i-voting*. URL: https://www.valimised.ee/en/internet-voting/frequently-asked-questions/questions-about-i-voting (besucht am 13. 08. 2022).

[157] Bundesamt für Sicherheit in der Informationstechnik. *BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten*. 15. März 2022. URL: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html (besucht am 15. 03. 2022).

[158] *Zwei Millionen Rechner durch Update von Optimierungs-Software infiziert. Hacker haben einen Computer-Virus in einem Update des CCleaner versteckt. Gut zwei Millionen Rechner wurden mit der Schadsoftware infiziert. Offenbar wollten die Hacker die Kontrolle über die infizierten PCs übernehmen.* 18. Sep. 2017. URL: https://www.handelsblatt.com/unternehmen/it-medien/ccleaner-von-avast-zwei-millionen-rechner-durch-update-von-optimierungs-software-infiziert/20342988.html.

[159] *Ransomware & Cyberangriffe aktuell heute 2022. Hackerangriffe auf Unternehmen, Firmen, Organisationen und Behörden - Deutschland, Österreich, Schweiz & weltweit*. URL: https://konbriefing.com/de-topics/cyber-angriffe.html (besucht am 05. 08. 2022).

[160] Dirk Knop. *Ransomware: Einbrecher deaktivieren Virenschutz mit Anti-Cheat-Treiber. Cyberkriminelle deaktivieren den Virenschutz mit einem verwundbaren und signierten Anti-Cheat-Treiber eines Spiels. Das ist jedoch gar nicht installiert.* 26. Aug. 2022. URL: https://www.heise.de/news/Ransomware-Einbrecher-deaktivieren-Virenschutz-mit-Anti-Cheat-Treiber-7244566.html (besucht am 27. 08. 2022).

[161] Markus Feilner und Jan Kleinert. *Bundestag-Hack: Die Ursachen, der Ablauf und die Folgen*. Apr. 2016. URL: https://www.linux-magazin.de/ausgaben/2016/04/bundestags-it/ (besucht am 06. 08. 2022).

[162] *Rechenzentrum der BwFuhrparkService GmbH gehackt*. 15. Aug. 2020. URL: https://www.bundeswehr-journal.de/2020/rechenzentrum-der-bwfuhrparkservice-gmbh-gehackt/ (besucht am 06. 08. 2022).

[163] Bundesamt für Sicherheit in der Informationstechnik. *BSI will Zwangstrennung infizierter Rechner vom Internet*. 14. Jan. 2015. URL: https://www.golem.de/news/bsi-rechner-mit-malware-zwangsweise-vom-internet-trennen-1501-111700.html (besucht am 15. 03. 2022).

[164] Bundesamt für Sicherheit in der Informationstechnik. *Botnetze – Auswirkungen und Schutzmaßnahmen*. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/botnetze_node.html (besucht am 17. 08. 2022).

[165] *Korrigendum - zz. Im Bericht über die Entwicklung ...* NZZ. 17. Apr. 2015. URL: https://www.wiso-net.de/document/NZZ__a7eb3ab15b433c256b1e309cc0514e9f40de2ca3.

[166] *Wer die Urne knackt, kassiert eine Belohnung*. NZZ. 8. Feb. 2019. URL: https://www.wiso-net.de/document/NZZ__088d26131f4e0ba9b4a35b09ef22e770fef1e632.

[167] *Mehr Sicherheit beim E-Voting verlangt*. NZZ. 12. Juni 2018. URL: https://www.wiso-net.de/document/NZZ__e613562e0f4e81b996ad023cef1e1ad52e914476.

[168] *Kommunalwahl'89: Krenz verkündet 98,85 Prozent Ja-Stimmen*. URL: https://www.mdr.de/geschichte/stoebern/damals/video139280.html (besucht am 05. 07. 2022).

[169] *Briefwahlteilnahme ohne Begründung ist rechtens*. URL: https://www.bundestag.de/webarchiv/textarchiv/2013/46178429_kw31_briefwahl_urteil-213280 (besucht am 08. 07. 2022).

[170] Christoph Seils. *Wie viele Briefwähler verträgt die Demokratie?* 13. Sep. 2013. URL: https://www.tagesspiegel.de/themen/wahlkampfbeobachter/die-wahlkampfbeobachter-29-wie-viele-briefwaehler-vertraegt-die-demokratie/8787238.html.

[171] Zweiter Senat des Bundesverfassungsgerichts. *Beschluss 2 BvC 7/10*. Bundesverfassungsgericht, 9. Juli 2013. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2013/07/cs20130709_2bvc000710.pdf (besucht am 10. 07. 2022).

[172] Transparency International Deutschland e. V. *Korruptionswahrnehmungsindex 2021*. URL: https://www.transparency.de/cpi/ (besucht am 06. 08. 2022).

[173] Paul Kreiner und Susanne Janssen. *Gefälschte Wahlzettel. Clanangehörige aus Kalabrien sollen ihren Landsleuten Stimmzettel für die Briefwahl zum Parlament abgekauft und gefälscht haben*. 26. Feb. 2010. URL: https://www.stuttgarter-zeitung.de/inhalt.organisierte-kriminalitaet-gefaelschte-wahlzettel.37bcc084-b778-40b1-80c5-12636558012f.html.

[174] *Stages of i-voting in voter application*. Valimised (= Estländisches Wahlportal). URL: https://www.valimised.ee/en/internet-voting/guidelines/stages-i-voting-voter-application (besucht am 14. 08. 2022).

[175] Mirko Dölle. *Live-System am Start. Selbstgemachtes Live-Ubuntu für DVD und USB-Stick*. Nov. 2016. URL: https://www.heise.de/select/ct/2016/11/1463987158011508 (besucht am 01. 09. 2022).

[176] *May 1 elections: E-voting on trial in attempt to combat apathy*. The Guardian. 25. Apr. 2003. URL: https://link.gale.com/apps/doc/A105837157/AONE?u=fub&sid=bookmark-AONE&xid=77d1d4a3.

[177] Roman Kaiser und Fabian Michl. *Bei uns doch nicht! Oder doch?: Gerrymandering in Deutschland,* 1. Juli 2019. DOI: 10.17176/20190701-232650-0. URL: https://verfassungsblog.de/bei-uns-doch-nicht-oder-doch/.

[178] Fabian Michl und Roman Kaiser. „Wer hat Angst vorm Gerrymander? Manipulative Wahlkreiszuschnitte in Deutschland". In: *Jahrbuch des öffentlichen Rechts* 67 (2019), S. 51–105.

[179] Christian Weisflog. *Mit oder ohne Trump: Über den USA schwebt das Gespenst eines Bürgerkriegs*. 5. Juli 2022. URL: https://www.nzz.ch/international/ueber-den-usa-schwebt-das-gespenst-eines-buergerkriegs-ld.1691374.

[180] *Front: Unease and AK47s on the streets as Venezuelans flock to the polls*. The Guardian. 8. Okt. 2012. URL: https://link.gale.com/apps/doc/A304679046/AONE?u=fub&sid=bookmark-AONE&xid=5599c075.

[181] *«Wir revolutionieren die Stimmabgabe» / Bülach befindet per SMS über Tempo 30*. NZZ. 12. Okt. 2005. URL: https://www.wiso-net.de/document/NZZ__d3154ff0222b0eaf9dcc8545e7b66c3cc03d4305.

[182] *Sicherheit schafft Vertrauen*. NZZ. 1. Okt. 2015. URL: https://www.wiso-net.de/document/NZZ__a11580988eb3ebd2a61124512a636a03f055c882.

[183] *Pirate party founder: 'Online voting? Would you want 4chan to decide your government?'; Rick Falkvinge backs electronic voting but warns of potential for abuse if the process goes entirely online*. The Guardian. 21. Jan. 2015. URL: https://link.gale.com/apps/doc/A398294658/AONE?u=fub&sid=bookmark-AONE&xid=2d64b382.

[184] Schweizerische Bundeskanzlei. *E-Voting: Ergebnisse der ersten unabhängigen Überprüfung liegen vor*. 20. Apr. 2022. URL: https://www.bk.admin.ch/bk/de/home/dokumentation/medienmitteilungen.msg-id-88085.html (besucht am 31. 08. 2022).

[185] *Georgia ist Trumps Ground Zero*. NZZ. 7. Mai 2022. URL: https://www.wiso-net.de/document/NZZ__dbfaeb0e72072b381e2436a5b4ec3893aebf1ebe.

[186] *Die tiefe Wahlbeteiligung in der Waadt wirkt ernüchternd*. NZZ. 22. März 2022. URL: https://www.wiso-net.de/document/NZZ__2725ef9e27ae8943b5760daf7fbe0bdb54f06af9.

[187] *Die öffentliche Meinung zerfällt in Bubbles*. NZZ. 5. Feb. 2022. URL: https://www.wiso-net.de/document/NZZ__68138191767e6efe9fcc1e2ec66a07fcf25d1470.

[188] *Anspruchshaltung gegenüber dem digitalen Staat*. NZZ. 13. Jan. 2022. URL: https://www.wiso-net.de/document/NZZ__5310efe358709b8a3c6d3606d1b5fd8a42c4f7b2.

[189] *Mittagessen mit einem Getriebenen*. NZZ. 6. Nov. 2021. URL: https://www.wiso-net.de/document/NZZ__5ba754f0100175efe621f80bb2ebc465e61f4711.

[190] *Kantone wollen mehr Geld für E-Voting*. NZZ. 5. Nov. 2021. URL: https://www.wiso-net.de/document/NZZ__aeed6bd456cb3aa3bf4461b27f204968c1c6c916.

[191] *Der Kreml tut alles für den Sieg*. NZZ. 17. Sep. 2021. URL: https://www.wiso-net.de/document/NZZ__9721f78a31706294f4f1ab4d08b5db8ee8aeb01c.

[192] *Es hapert bei der Digitalisierung der Verwaltung*. NZZ. 8. Sep. 2021. URL: https://www.wiso-net.de/document/NZZ__06a02908d5c3b79f9622632e734dddfd81c6913a.

[193] *Der Bundesrat küsst das E-Voting wach*. NZZ. 29. Apr. 2021. URL: https://www.wiso-net.de/document/NZZ__b02694d9dfb5fbbd4343d5ae22305f42d792e45b.

[194] *«Man kann es nicht beschönigen: Wir haben ein Problem»*. NZZ. 25. März 2021. URL: https://www.wiso-net.de/document/NZZ__30fa796cab9f33378b3c484cb251aec27838cf56.

[195] *Wie inkonsequent sind wir eigentlich?* NZZ. 23. Feb. 2021. URL: https://www.wiso-net.de/document/NZZ__679ee6599543062366352930b0f8416e4ab6a1272.

[196] *«Datenschutz steht nicht im Vordergrund»*. NZZ. 19. Feb. 2021. URL: https://www.wiso-net.de/document/NZZ__ed2874f131d0c3f4e6a2565a505110981449d3ec.

[197] *Schweizer Firmen laden Hacker ein*. NZZ. 8. Feb. 2021. URL: https://www.wiso-net.de/document/NZZ__9ef40592c1b28152a143d3844637bdeaeb421d5e.

[198] *Die E-ID muss Vertrauen gewinnen*. NZZ. 27. Jan. 2021. URL: https://www.wiso-net.de/document/NZZ__59ad02e1c54d2a7f5312ea63a9e38e1a8ff9ac07.

[199] *Das Corona-Fiasko ist nur ein Symptom*. NZZ. 26. Jan. 2021. URL: https://www.wiso-net.de/document/NZZ__757ee2c82502cdbd0dbecd78b8ae9ad9848dbf77.

[200] *E-ID-Gegner werfen der Post unzulässige Einmischung in den Abstimmungskampf vor*. NZZ. 14. Jan. 2021. URL: https://www.wiso-net.de/document/NZZ__1592fca2b07d46c322e914e8189fe2d1fa5ae0d8.

[201] *Neuer Anlauf im E-Voting*. NZZ. 22. Dez. 2020. URL: https://www.wiso-net.de/document/NZZ__17c3cacc9070cbd6282cb43dbdd689349f123f75.

[202] *Der Corona-Notfallplan ist blockiert*. NZZ. 11. Nov. 2020. URL: https://www.wiso-net.de/document/NZZ__3af19a0647c63193347fd2e28150a1fd52507def.

[203] *CDU-Parteitag wird verschoben*. NZZ. 27. Okt. 2020. URL: https://www.wiso-net.de/document/NZZ__0397a0635e3bdd7a5f94f28e2fb52a17ac529aa9.

[204] *Gute Gründe gegen das Stimmrechtsalter 16*. NZZ. 6. Okt. 2020. URL: https://www.wiso-net.de/document/NZZ__3c351faaec824f3ebbf5469c7c4c165910f95375.

[205] *Initianten befürchten, dass ihre Volksbegehren scheitern*. NZZ. 25. Mai 2020. URL: https://www.wiso-net.de/document/NZZ__e5916bd11493dfe6706e08256d5c0831561f901b.

[206] *Franz Grüter soll es für die SVP richten*. NZZ. 16. Mai 2020. URL: https://www.wiso-net.de/document/NZZ__ed76778c13477f5a231a6799839c17324e67bd3f.

[207] *Der Druck beim E-Voting steigt*. NZZ. 4. Jan. 2020. URL: https://www.wiso-net.de/document/NZZ__64e8ecb51ffa5a15581a24dca7f6ba9403bcf2e1.

[208] *Weniger «4.0», dafür exakt*. NZZ. 11. Nov. 2019. URL: https://www.wiso-net.de/document/NZZ__0d7db88a6e6194f12f84da6430364c9d90811e54.

[209] *Die Jagd nach den Wählern im Ausland*. NZZ. 14. Okt. 2019. URL: https://www.wiso-net.de/document/NZZ__99ba0d45ec501ba8da62badecf558257c711cdc8.

[210] *Machiavelli lesen heisst siegen lernen*. NZZ. 9. Sep. 2019. URL: https://www.wiso-net.de/document/NZZ__fdaae330185303b7b75d58a75b50db4eb551fcc5.

[211] *«Wir wollen die Fühler ins Ausland ausstrecken»*. NZZ. 2. Sep. 2019. URL: https://www.wiso-net.de/document/NZZ__c4e37fffe6041450d93f30919383f6fac6a45305.

[212] *«Es ist auch Politik, sich um den Spielplatz im Hof zu kümmern»*. NZZ. 27. Aug. 2019. URL: https://www.wiso-net.de/document/NZZ__8c767364c049743a69b928f979834b8a46be4d29.

[213] *Ein Vorzeigeprojekt wird für die Post zum Fiasko*. NZZ. 29. Juni 2019. URL: https://www.wiso-net.de/document/NZZ__9c125fb03960db77bcdfff3521d50c9969a42f28.

[214] *Genf beendet E-Voting früher als geplant*. NZZ. 20. Juni 2019. URL: https://www.wiso-net.de/document/NZZ__91881de89cd538e0f6a9641a5ddb9d95183350a0.

[215] *Das hatte der Kanton nicht auch noch nötig*. NZZ. 11. Mai 2019. URL: https://www.wiso-net.de/document/NZZ__88a6a67bcd7bcc4a30b3f472d7c072a67f658bae.

[216] *Online-Plattformen werden zum Brutkasten der Demokratie*. NZZ. 29. Apr. 2019. URL: https://www.wiso-net.de/document/NZZ__3dc29cb9682da9cb769eb3152e885772c2f329d9.

[217] *Bürgerliche erzielen zu Hausbesetzungen nur einen Pyrrhussieg*. NZZ. 9. Apr. 2019. URL: https://www.wiso-net.de/document/NZZ__940e61f299c4db0012c8f8f21ee9ea76385f0322.

[218] *Online-Tools für politische Mitbestimmung sind Mauerblümchen*. NZZ. 29. März 2019. URL: https://www.wiso-net.de/document/NZZ__a40225d80e3158f28a6c56ef370f6020cc699c16.

[219] *Der Staat steht in der Verantwortung*. NZZ. 21. März 2019. URL: https://www.wiso-net.de/document/NZZ__eac7c5896c1b8f54da04db71f7ebf5dbc923c9f1.

[220] *Die E-Wähler verändern die Politik*. NZZ. 6. März 2019. URL: https://www.wiso-net.de/document/NZZ__af612ae026d3a93651fede1a36ec7e2511111d09.

[221] *Beim E-Voting tritt der «Techie» auf die Bremse*. NZZ. 5. März 2019. URL: https://www.wiso-net.de/document/NZZ__b82f03358caad3545ab52b338f3c2f453466f242.

[222] *Estland schwingt nach rechts*. NZZ. 4. März 2019. URL: https://www.wiso-net.de/document/NZZ__87e4f05d007e54bf27d17feb82d68e0a0e93cd15.

[223] *Die CVP entdeckt das E-Collecting*. NZZ. 7. Feb. 2019. URL: https://www.wiso-net.de/document/NZZ__2b32236c0ab2342526f2fd6fc0b92d06936e1e36.

[224] *Die Jagd auf Unterschriften verlagert sich ins Internet*. NZZ. 28. Jan. 2019. URL: https://www.wiso-net.de/document/NZZ__80e06e195c6ecde159785b584e327401ce234e07.

[225] *Ein Moratorium, das ewig dauern könnte*. NZZ. 26. Jan. 2019. URL: https://www.wiso-net.de/document/NZZ__85e3b82ed10a55fbe6df0933a7f4fba5139429d7.

[226] *Digitalisierung der Urne ist unnötig*. NZZ. 26. Jan. 2019. URL: https://www.wiso-net.de/document/NZZ__83f47331c70f4f310cfaf477a37bead91a8bb37b.

[227] *Hartes Ringen um den digitalen Pass*. NZZ. 24. Jan. 2019. URL: https://www.wiso-net.de/document/NZZ__3f15c0aba6ac4f5951db3a901a5fccbcbeb9b17d.

[228] *Das Wallis ist bei der Digitalisierung das Schlusslicht*. NZZ. 22. Dez. 2018. URL: https://www.wiso-net.de/document/NZZ__89d0fa00cef679cf627ff22d9316971847b20ee7.

[229] *400 Hacker kämpfen gegen das E-Voting*. NZZ. 20. Dez. 2018. URL: https://www.wiso-net.de/document/NZZ__1b69b1b3d9ca6cc44782f63cdee2618d6242ee98.

[230] *Das E-Voting ist noch nicht erledigt*. NZZ. 8. Dez. 2018. URL: https://www.wiso-net.de/document/NZZ__270944665c7e10036992adf7a1dfc6443eed67df.

[231] *Auslandschweizer fordern E-Voting bis 2021*. NZZ. 1. Dez. 2018. URL: https://www.wiso-net.de/document/NZZ__3129fc32e3c8c5dd5d94de0dde71b5b9c1e2e86a.

[232] *Marschhalt für E-Voting notwendig*. NZZ. 29. Nov. 2018. URL: https://www.wiso-net.de/document/NZZ__077985de8c7ebfcd2595bac65eb3dec09a50877d.

[233] *Rückschlag für das E-Voting*. NZZ. 29. Nov. 2018. URL: https://www.wiso-net.de/document/NZZ__7c515c862c73a6f4600654d7202ecbcfdc14d79a.

[234] *Schwachstelle in Genfer E-Voting-System*. NZZ. 3. Nov. 2018. URL: https://www.wiso-net.de/document/NZZ__8410c83407ea3f4e01679c134e3aff9aceda3cf6.

[235] *Kommission tritt bei E-Voting auf die Bremse*. NZZ. 13. Okt. 2018. URL: https://www.wiso-net.de/document/NZZ__6db9c4abb98ad6ccf8a02658d9003331db620d8a.

[236] *Lobbying bis zum Letzten Uno rügt Schweiz wegen Ausweisung nach Italien*. NZZ. 15. Sep. 2018. URL: https://www.wiso-net.de/document/NZZ__5471ebe6c3c72e5e37df52e1169800969f83187e.

[237] *Ju-52-Absturz: Alle zwanzig Opfer sind identifiziert*. NZZ. 11. Aug. 2018. URL: https://www.wiso-net.de/document/NZZ__c1691284762204b1ed68631055cb57a2ddb927ad.

[238] *Zürich vor der digitalen Rundumreform*. NZZ. 25. Juli 2018. URL: https://www.wiso-net.de/document/NZZ__3ee7d40bcfc7c2920b9f3bc72d4a33df67121e13.

[239] *Umverteilung im Rentensystem*. NZZ. 9. Juli 2018. URL: https://www.wiso-net.de/document/NZZ__d243d1da54e06a0ada35956380b5c723cec46503.

[240] *Bundesrat treibt E-Voting voran*. NZZ. 28. Juni 2018. URL: https://www.wiso-net.de/document/NZZ__2f4874274471104 41d7ab901d8210e5355da3ffc.

[241] *Totalverbot für E-Voting*. NZZ. 16. Juni 2018. URL: https://www.wiso-net.de/document/NZZ__fdf280206e90fe3c62f84cd93d6dc47f0641f414.

[242] *Impulse für die digitale Demokratie*. NZZ. 6. Juni 2018. URL: https://www.wiso-net.de/document/NZZ__76c7c24f9b5597dc8680b03160fe190421d05e52.

[243] *Türkische Propaganda in Schulen*. NZZ. 15. Mai 2018. URL: https://www.wiso-net.de/document/NZZ__48f30334657ad35f943deb2bed9a63b037d9a36f.

[244] *Intellektuelle und Kapitalismus*. NZZ. 3. Mai 2018. URL: https://www.wiso-net.de/document/NZZ__6b84818c38ced6510c00d283cae9379b22c900c3.

[245] *«Ich meine, das Risiko sei vertretbar»*. NZZ. 28. Apr. 2018. URL: https://www.wiso-net.de/document/NZZ__a356b2ce95260ee9b779ee816ed3d0a2f818f210.

[246] *E-Voting erhöht die Wahlbeteiligung nicht*. NZZ. 18. Apr. 2018. URL: https://www.wiso-net.de/document/NZZ__f498f1377081c57f7261b1b95abcddc2be4d0930.

[247] *Politische Pop-up-Stores geben das Tempo vor*. NZZ. 11. Apr. 2018. URL: https://www.wiso-net.de/document/NZZ__04f23b427dbf352954e29ee7984ccae804f32762.

[248] *Trotz Kritik hält Zürich am E-Voting fest*. NZZ. 6. Apr. 2018. URL: https://www.wiso-net.de/document/NZZ__78752ffcbaf46d9d9363eaca7722b8aebd6bc375.

[249] *Mit dem Smartphone auf Unterschriftenfang*. NZZ. 3. März 2018. URL: https://www.wiso-net.de/document/NZZ__fcb183e374e7cc0cdbe5c694f4d90f3b7de2253a.

[250] *E-Voting soll an der Urne versenkt werden*. NZZ. 27. Feb. 2018. URL: https://www.wiso-net.de/document/NZZ__d53f41ea9f3f04dd05c7e7d229ca0fdee08f1adf.

[251] *E-Voting muss absolut sicher sein*. NZZ. 17. Feb. 2018. URL: https://www.wiso-net.de/document/NZZ__22fd8ceece2b4911d75aa51479bbeb4d5e2dc725.

[252] *Wer das E-Voting knackt, kriegt eine Million*. NZZ. 17. Feb. 2018. URL: https://www.wiso-net.de/document/NZZ__45fdd51dc5d5b3191d3448e4b323a7e2aeed7a48.

[253] *Gericht stützt Basler E-Voting-Entscheid*. NZZ. 13. Dez. 2017. URL: https://www.wiso-net.de/document/NZZ__7d13a948d2de196ba1ad5ba66272394 88394f40a.

[254] *Steuern senken - aber wie?* NZZ. 12. Dez. 2017. URL: https://www.wiso-net.de/document/NZZ__1d5f3d4740b0e8a1ce261faa97103da261d58cc0.

[255] *Politiker fordern einen Mister Digital*. NZZ. 22. Nov. 2017. URL: https://www.wiso-net.de/document/NZZ__033b5842158e18430a18455a84083c4b8ad7235e.

[256] *Basler E-Voting-Entscheid wirft Fragen auf*. NZZ. 4. Nov. 2017. URL: https://www.wiso-net.de/document/NZZ__d1d2ffdc7a196072ab25dcc874e57690bf825165.

[257] *New Kids on the Blockchain*. NZZ. 2. Okt. 2017. URL: https://www.wiso-net.de/document/NZZ__a1e560244e4ab873699d50ae8c18bd565f0aa4fe.

[258] *Die Gilde der modernen Unternehmer sucht ihr Glück*. NZZ. 19. Sep. 2017. URL: https://www.wiso-net.de/document/NZZ__eaf1d37fd6ef58e80143a197bbb599a929b30380.

[259] *Thurgau entscheidet sich für E-Voting der Post*. NZZ. 22. Aug. 2017. URL: https://www.wiso-net.de/document/NZZ__2aa889d7bd37cc4556276b12b584b1e0f15dd222.

[260] *Der Staat braucht einen digitalen Kick*. NZZ. 4. Aug. 2017. URL: https://www.wiso-net.de/document/NZZ__57a6dae00e10ae61fe0863b336b5d1a31c9f382a.

[261] *E-Voting in den Kantonen St. Gallen und Aargau*. NZZ. 29. Juni 2017. URL: https://www.wiso-net.de/document/NZZ__6ed0873b3d4762c8824fb09316d96d47f03d71bd.

[262] *Letzte Chance für den digitalen Pass*. NZZ. 7. Juni 2017. URL: https://www.wiso-net.de/document/NZZ__4b4949b398e3f54461644a382f65c1a7c412fd55.

[263] *BVK-Wahl sorgt für Unmut*. NZZ. 31. Mai 2017. URL: https://www.wiso-net.de/document/NZZ__11e7e26aacfa276bc6c088296040d5a78b1969aa.

[264] *Wer soll den digitalen Pass verwalten?* NZZ. 24. Apr. 2017. URL: https://www.wiso-net.de/document/NZZ__e70645942225ddcc4e188d94f6bdec264f8b351b.

[265] *Moderater Druck aufs Gaspedal*. NZZ. 6. Apr. 2017. URL: https://www.wiso-net.de/document/NZZ__851f14ff3183dc128c5fb185439994518aebfec5.

[266] *Elektronisch abstimmen soll Standard werden*. NZZ. 6. Apr. 2017. URL: https://www.wiso-net.de/document/NZZ__41029d4fe4ea09d708f4ab138cd9d8c9921ae287.

[267] *Nationalrat will Mindesttarife tilgen*. NZZ. 17. März 2017. URL: https://www.wiso-net.de/document/NZZ__188d37c9710c3de6e330ab747bd1e83dab065fee.

[268] *Rekurs gegen Basler Beschluss zum E-Voting*. NZZ. 10. März 2017. URL: https://www.wiso-net.de/document/NZZ__5a61928b0aca6f4c982829e15211d34ebe5a9706.

[269] *E-Voting schlägt briefliches Abstimmen*. NZZ. 7. Feb. 2017. URL: https://www.wiso-net.de/document/NZZ__9ae70ce3ea8b8e47a885d76317c2fff67574a9e9.

[270] *Viele Fragezeichen zum E-Voting*. NZZ. 7. Dez. 2016. URL: https://www.wiso-net.de/document/NZZ__a9b232d2719e545b35fe165af9e84905ea2daaf4.

[271] *Amerika, hast du's nun besser?* NZZ. 14. Nov. 2016. URL: https://www.wiso-net.de/document/NZZ__7b271a04cfff41791fce8e67e3306edb09d31f96.

[272] *Der lange Weg zum E-Voting*. NZZ. 11. Nov. 2016. URL: https://www.wiso-net.de/document/NZZ__273106965b8822fa6f916876b5a6579aff643059.

[273] *Zweikampf zwischen Genf und der Post*. NZZ. 11. Nov. 2016. URL: https://www.wiso-net.de/document/NZZ__0789cffb31094f10713b5833e0dedc09ded94eba.

[274] *Der elektronische Konsularbeamte*. NZZ. 6. Okt. 2016. URL: https://www.wiso-net.de/document/NZZ__eaf288f9f2b41f45c4f2d44d98c708f153bab1be.

[275] *Angst vor verfälschten Resultaten*. NZZ. 28. Sep. 2016. URL: https://www.wiso-net.de/document/NZZ__6084e030ab378bee0741b6f5999d3c5d057b01c9.

[276] *Erneut E-Voting im Kanton Freiburg*. NZZ. 17. Sep. 2016. URL: https://www.wiso-net.de/document/NZZ__3175ac75e396b246732a1a6269ec65d5f93c9893.

[277] *Russische Hacker in Amerikas Wahlregistern*. NZZ. 31. Aug. 2016. URL: https://www.wiso-net.de/document/NZZ__16d51ae53ec2c802261ee26b3418fa505992a171.

[278] *E-Voting in allen Kantonen*. NZZ. 6. Aug. 2016. URL: https://www.wiso-net.de/document/NZZ__d041490707b9f6b78841dee629209f8dc6f45f5c.

[279] *Politischer Weckruf aus der Late-Night-Show*. NZZ. 7. Juli 2016. URL: https://www.wiso-net.de/document/NZZ__c0f7b03e0986e0dbbcc27f9707c826e9636f730a.

[280] *Ständeratswahl soll gestrafft werden*. NZZ. 5. Juli 2016. URL: https://www.wiso-net.de/document/NZZ__26078fd598a766d08a0acb0e134608f86a215b56.

[281] *E-Voting braucht Zeit*. NZZ. 17. Juni 2016. URL: https://www.wiso-net.de/document/NZZ__46dd7f8f81d57dc260db5fa518cbc2278be9e8d0.

[282] *Kreative Kasachen*. NZZ. 14. Jan. 2016. URL: https://www.wiso-net.de/document/NZZ__c7e1586b94e10b6b04e124474c8410d39a6f1008.

[283] *E-Demokratie - Nachdem der Bundesrat in Sachen E-Voting ...* NZZ. 12. Dez. 2015. URL: https://www.wiso-net.de/document/NZZ__7cf3b0f65f2d88c4b397f63ad3c16e6fdafb49e2.

[284] *Risiken und Nebenwirkungen*. NZZ. 12. Dez. 2015. URL: https://www.wiso-net.de/document/NZZ__143ebd00f36ed17c0cfd54f21fc3ed2ba8032677.

[285] *Und ab geht die Post*. NZZ. 8. Dez. 2015. URL: https://www.wiso-net.de/document/NZZ__edd90a4a543a0e0ba6f3625dd2a0566e17c49e64.

[286] *Referendum über E-Voting in Bulgarien gescheitert*. NZZ. 27. Okt. 2015. URL: https://www.wiso-net.de/document/NZZ__0de7e9acc22db86c562506f8a9558f1b5071af70.

[287] *Nur ein Bruchteil wählte elektronisch*. NZZ. 22. Okt. 2015. URL: https://www.wiso-net.de/document/NZZ__a35ce27125e6cc981eb608eced977b9e1656adb.

[288] *Exodus aus der Börse*. NZZ. 15. Okt. 2015. URL: https://www.wiso-net.de/document/NZZ__0b3a2da5218614a29161c069a6e3222503509bb7.

[289] *Avenir Suisse setzt auf einen Modernisierer*. NZZ. 3. Okt. 2015. URL: https://www.wiso-net.de/document/NZZ__2092190f18522db633eb68e3fe546ff8e1e9b5fc.

[290] *Neue Allianzen beim E-Voting?* NZZ. 7. Sep. 2015. URL: https://www.wiso-net.de/document/NZZ__19475b98cd29c9f2511cec61486fc2e1a9004fa7.

[291] *Freiwild für Hacker?* NZZ. 3. Sep. 2015. URL: https://www.wiso-net.de/document/NZZ__e5cd75d77843938aa20a30b9337b5e7b1deb4047.

[292] *Leuthard verteidigt E-Voting-Entscheid*. NZZ. 17. Aug. 2015. URL: https://www.wiso-net.de/document/NZZ__33935e2d576acc200f834565aa4fa04f6e0cda78.

[293] *Übungsabbruch beim E-Voting verlangt*. NZZ. 15. Aug. 2015. URL: https://www.wiso-net.de/document/NZZ__058e03a4fcb4c1d01c1f394998bbdbe9760a1587.

[294] *John Kerry in Havanna/Anti-Folter-Bericht/Die Fünfte Schweiz zu Hause*. NZZ. 14. Aug. 2015. URL: https://www.wiso-net.de/document/NZZ__2e409c9ca7a78ddf6211313234cfe566815a3dbe.

[295] *OSZE will E-Voting begutachten*. NZZ. 12. Aug. 2015. URL: https://www.wiso-net.de/document/NZZ__e691b51e8b1a091b37756b0c0a6552da1fd58f0e.

[296] *E-Voting auch für Einheimische*. NZZ. 25. Juli 2015. URL: https://www.wiso-net.de/document/NZZ__fdcc5fb280446389a53887c5140af6808dd10f57.

[297] *Das Fünftel hinter den Räten*. NZZ. 21. Juli 2015. URL: https://www.wiso-net.de/document/NZZ__bc9df0d47995edcd64399efd440d6c44f006c9cf.

[298] *Unklare Ausgangslage nach Corina Casanovas angekündigtem Rücktritt*. NZZ. 30. Juni 2015. URL: https://www.wiso-net.de/document/NZZ__5617a68ec94ed055a43d9eb8974d2d446a6b69a3.

[299] *Abstimmungen in den Kantonen*. NZZ. 15. Juni 2015. URL: https://www.wiso-net.de/document/NZZ__7f889e1431928e81663b799f79af563d0f68115b.

[300] *Zürich verfolgt E-Voting weiter*. NZZ. 2. Juni 2015. URL: https://www.wiso-net.de/document/NZZ__8b248d7bd0470275c1d2d14efbe0fe89786cbf67.

[301] *Klick-Demokratie am Horizont*. NZZ. 27. Mai 2015. URL: https://www.wiso-net.de/document/NZZ__aa7132f59c4caab75d78548976d3c319be4435a9.

[302] *E-Voting kostet deutlich mehr*. NZZ. 11. Apr. 2015. URL: https://www.wiso-net.de/document/NZZ__8c864014f2b45c08150db952ae329fc63ef0d1d9.

[303] *Estland als digitaler Musterschüler*. NZZ. 27. Feb. 2015. URL: https://www.wiso-net.de/document/NZZ__ab977c6fc63f0415265dcadddadcb6010beb6d6c.

[304] *E-Voting für Auslandschweizer*. NZZ. 24. Jan. 2015. URL: https://www.wiso-net.de/document/NZZ__9c3b94794e2ad9a6ec9e429741db1c5a79d24a9b.

[305] *Visionäre aus «Crypto Valley»*. NZZ. 11. Sep. 2014. URL: https://www.wiso-net.de/document/NZZ__f57375f19f69ee92eda5e6c9a12a45c86a438cb4.

[306] *Die Berner Börse blutet*. NZZ. 29. Aug. 2014. URL: https://www.wiso-net.de/document/NZZ__4ae700172c3419a747461e7d6a9ea83e16f17da8.

[307] *E-Voting hat mehr als «nur» technische Risiken*. NZZ. 29. Juli 2014. URL: https://www.wiso-net.de/document/NZZ__62493c4c6595d403af3317917bede0b7454e9eaa.

[308] *«Wir müssen IT-Berufe für Frauen attraktiver machen»*. NZZ. 28. Juni 2014. URL: https://www.wiso-net.de/document/NZZ__c2867fc8f83d033f64a72743fbb68e79eed79d2f.

[309] *Was würden Sie stimmen, wenn schon am nächsten Sonntag . . .* NZZ. 8. Mai 2014. URL: https://www.wiso-net.de/document/NZZ__074a6e200f9c027102ba00fc8d21b7c09c4b9603.

[310] *Stop-and-go-Politik beim E-Voting*. NZZ. 17. März 2014. URL: https://www.wiso-net.de/document/NZZ__0e713e4c59225311ed1ebf3827fadf326912cda4.

[311] *Bund treibt E-Voting voran*. NZZ. 27. Feb. 2014. URL: https://www.wiso-net.de/document/NZZ__a49b164626789c0165f99e8ff626366056ed956e.

[312] *Vorerst kein E-Voting in der Waadt*. NZZ. 14. Dez. 2013. URL: https://www.wiso-net.de/document/NZZ__5ca0764db6f1ff38f5c8a74d44770dd2804456cb.

[313] *Daumen hoch, Daumen runter*. NZZ. 14. Dez. 2013. URL: https://www.wiso-net.de/document/NZZ__2359a1049e4ecbef61e2ab20e77e9d991d79bb4e.

[314] *Mehr Staat als Markt?* NZZ. 11. Dez. 2013. URL: https://www.wiso-net.de/document/NZZ__58898f059aff1dcd1831260991cc88572d50e223.

[315] *Ausgereizte Volksrechte*. NZZ. 30. Nov. 2013. URL: https://www.wiso-net.de/document/NZZ__85032f50c36f94beb33e88c921bab5deb0ea1d00.

[316] *Traktanden als Diskussionsstoff*. NZZ. 24. Okt. 2013. URL: https://www.wiso-net.de/document/NZZ__e97d7712c88f62bd6f27100548 0e20d1f1498887.

[317] *E-Voting ab 2015 für Auslandschweizer*. NZZ. 14. Okt. 2013. URL: https://www.wiso-net.de/document/NZZ__faa71762481a88678ec9ea021d2a195ca48e3c05.

[318] *Stimmzettel statt PC-Taste*. NZZ. 2. Okt. 2013. URL: https://www.wiso-net.de/document/NZZ__33cabbb8bb61077fb56d086cef83ebf17984d80f.

[319] *Bund hält am E-Voting fest*. NZZ. 17. Sep. 2013. URL: https://www.wiso-net.de/document/NZZ__0189c5eec4b5041f8b4a34b728e47293dada5e81.

[320] *E-Voting in der Zange*. NZZ. 30. Aug. 2013. URL: https://www.wiso-net.de/document/NZZ__61f7a6fd1d7557d7429d518318ecdbd1dd35f394.

[321] *Wahl per Internet aus dem Ausland*. NZZ. 3. Mai 2013. URL: https://www.wiso-net.de/document/NZZ__cc2cf40901b3b93a372c6e2c277539d6afdbb677.

[322] *Architektonische Abstimmungsspiele*. NZZ. 6. Apr. 2013. URL: https://www.wiso-net.de/document/NZZ__1aaf8876f6297201f5c7fb17a482e44270c8b1da.

[323] *CVP setzt auf Solidarität in der Familie*. NZZ. 8. Jan. 2013. URL: https://www.wiso-net.de/document/NZZ__4400aa36beaa4ecff716765a64e556052dbac0ce.

[324] *Führungsgremium für Russlands Opposition gewählt*. NZZ. 24. Okt. 2012. URL: https://www.wiso-net.de/document/NZZ__13b6a342b28f0ed19197ca6c6b04892cfd6103f1.

[325] *«Ich würde nur ein einziges Wort streichen»*. NZZ. 9. Okt. 2012. URL: https://www.wiso-net.de/document/NZZ__966fcebbb6e0aeb17d2b7e35c6f108bdcf361222.

[326] *Oberster Statistiker geht*. NZZ. 31. Aug. 2012. URL: https://www.wiso-net.de/document/NZZ__4db616f102419273b301fd1930b2b422d62e3fea.

[327] *Ausweitung des E-Voting*. NZZ. 28. Juni 2012. URL: https://www.wiso-net.de/document/NZZ__c3d038112a3ab432a2be0127f50c91d87a82dda8.

[328] *Wie die Fünfte Schweiz politisch tickt*. NZZ. 22. Mai 2012. URL: https://www.wiso-net.de/document/NZZ__6f0551719d1576d833d28dfff6c1a7127175578a.

[329] *Die ÖVP für mehr direkte Demokratie*. NZZ. 6. Jan. 2012. URL: https://www.wiso-net.de/document/NZZ__49fe6345e5a825d8ceae931ea93d27b4819cc37c.

[330] *E-Voting im ganzen Kanton*. NZZ. 28. Dez. 2011. URL: https://www.wiso-net.de/document/NZZ__4ea8182f4328d1283aba85ee7bb171c061e0b9fd.

[331] *E-Voting frühestens wieder ab 2015*. NZZ. 21. Dez. 2011. URL: https://www.wiso-net.de/document/NZZ__bebbcbbc1e61c617b8a1951014781da7db381962.

[332] *Pause für E-Voting*. NZZ. 26. Nov. 2011. URL: https://www.wiso-net.de/document/NZZ__b9736ac444af19b1eda5c6ac548e232263f7f31e.

[333] *Der künftige «Mister Post» wird Weichen stellen müssen*. NZZ. 2. Nov. 2011. URL: https://www.wiso-net.de/document/NZZ__3866707468706d484e425baa38726c8850b640f8.

[334] *Auslandschweizer ohne Erfolg*. NZZ. 29. Okt. 2011. URL: https://www.wiso-net.de/document/NZZ__bfddd5f201e2d761e252cb8e5d63492d796ee17d.

[335] *Was die «fünfte Schweiz» will*. NZZ. 29. Aug. 2011. URL: https://www.wiso-net.de/document/NZZ__9fb823265dbbeaad866a8e96307f3a39f6ad8f00.

[336] *E-Voting für 22 000 Auslandschweizer*. NZZ. 23. Juni 2011. URL: https://www.wiso-net.de/document/NZZ__91953527a5c0078432f83a5c1c80a4775ae728fe.

[337] *Optionen für die E-Demokratie*. NZZ. 11. Juni 2011. URL: https://www.wiso-net.de/document/NZZ__ca49234c52fa40ee5be6f01d6c1577c154d8b514.

[338] *Genf setzt sich aufs Fahrrad*. NZZ. 16. Mai 2011. URL: https://www.wiso-net.de/document/NZZ__487d998eeecd712c6d0c2312bfff41de0ab22c6a.

[339] *Novum bei den Nationalratswahlen*. NZZ. 29. März 2011. URL: https://www.wiso-net.de/document/NZZ__f467cc84a63d7e552a044c56ec5c862c5820ca2c.

[340] *Beim E-Voting nicht zurückbuchstabieren*. NZZ. 28. März 2011. URL: https://www.wiso-net.de/document/NZZ__996e1d3cdecd27172331bce38441703f602421f3.

[341] *Gruppe der E-Voting-Gemeinden schrumpft vorzeitig*. NZZ. 8. März 2011. URL: https://www.wiso-net.de/document/NZZ__9af2461a8769506d418d7b4a31e4a372d9b95166.

[342] *Überlegener Wahlsieg der estnischen Koalition*. NZZ. 8. März 2011. URL: https://www.wiso-net.de/document/NZZ__0d2e502d733476bc802fb3c48d715224914cbe9f.

[343] *Pause beim E-Voting / Software-Probleme befürchtet*. NZZ. 6. Dez. 2010. URL: https://www.wiso-net.de/document/NZZ__5713e7f7b709444bb26ec1243613474ee7b07390.

[344] *Abstimmung per Internet*. NZZ. 3. Nov. 2010. URL: https://www.wiso-net.de/document/NZZ__0c5db988a64638670d3d6f0313247571632e864d.

[345] *E-Voting für Auslandschweizer*. NZZ. 9. Sep. 2010. URL: https://www.wiso-net.de/document/NZZ__a4e935c0e7b0bf3ae5a7c3096323870d685561dc.

[346] *Man hüte sich vor dem Drucker-Experten*. NZZ. 7. Sep. 2010. URL: https://www.wiso-net.de/document/NZZ__3eb7dc6726206e420b5462e4e6c0276bf02c0cb2.

[347] *Weisse Flecken in Fünfter Schweiz*. NZZ. 20. Aug. 2010. URL: https://www.wiso-net.de/document/NZZ__532a453097884158a8f0e587cb3c4c4925c53d2f.

[348] *E-Voting für Berner im Ausland*. NZZ. 26. Apr. 2010. URL: https://www.wiso-net.de/document/NZZ__122ac9a97df8da676284a5b66117e00baf6b0a98.

[349] *E-Voting mit begrenzter Auswahl*. NZZ. 26. Feb. 2010. URL: https://www.wiso-net.de/document/NZZ__ac74517bacb4b106408e98d0ccaa8645be437291.

[350] *Probleme mit E-Voting*. NZZ. 24. Nov. 2009. URL: https://www.wiso-net.de/document/NZZ__ea9c6df660cc6908f578078efa169faeb605ed77.

[351] *Hunderttausende von Alternativen*. NZZ. 27. Okt. 2009. URL: https://www.wiso-net.de/document/NZZ__983a4e4b5bba94a0a58b1de003a128238b2b497c.

[352] *Mehr E-Voting für Auslandschweizer*. NZZ. 5. Sep. 2009. URL: https://www.wiso-net.de/document/NZZ__f4465e48d5893a5788ac766aea95fb0a9fd247e5.

[353] *Ein Potenzial der Schweiz in der Welt*. NZZ. 10. Aug. 2009. URL: https://www.wiso-net.de/document/NZZ__6902a37ca6e67e55be2af5610cb2240ecb222aff.

[354] *Genfer E-Voting für Auslandbasler*. NZZ. 16. Juni 2009. URL: https://www.wiso-net.de/document/NZZ__3ea7d701c090e84ac663441a78ecf8b4c3b1a50d.

[355] *E-Voting erhöht Stimmbeteiligung nicht*. NZZ. 27. März 2009. URL: https://www.wiso-net.de/document/NZZ__3516b53b9f1d8dbba698bb73615a1f36f28cb689.

[356] *Schwung für E-Voting aus Genf*. NZZ. 10. Feb. 2009. URL: https://www.wiso-net.de/document/NZZ__e03411cd46292502aea870d4749e6c1356c4ac3d.

[357] *Schweizer E-Voting-Premiere*. NZZ. 9. Feb. 2009. URL: https://www.wiso-net.de/document/NZZ__eb5d6049698eb3502739b9e8312ea6b0ca2571fc.

[358] *Harte Verteilkämpfe in unsicherer Zeit*. NZZ. 5. Feb. 2009. URL: https://www.wiso-net.de/document/NZZ__4be8752f5f2f2f63c1cbd64f7bc13337897b6cb9.

[359] *Wegen Vorlagen-Flut hohe Stimmbeteiligung erwartet*. NZZ. 28. Nov. 2008. URL: https://www.wiso-net.de/document/NZZ__00fff199ffcb7ce4bd08866e323dbd083ccff4ca.

[360] *E-Voting wird ausgebaut*. NZZ. 28. Aug. 2008. URL: https://www.wiso-net.de/document/NZZ__4f1c50825577a37b2141ffecb554ba2b77f0ae94.

[361] *E-Voting-Ausbau im Zeitplan*. NZZ. 28. Mai 2008. URL: https://www.wiso-net.de/document/NZZ__9f75f42845f6edb10bb32935b018c6495c4c8625.

[362] *Digitaler Graben zwischen den Generationen*. NZZ. 17. Dez. 2007. URL: https://www.wiso-net.de/document/NZZ__b6d66bd68fcf68087b6c6f30de9447a2c97f6b30.

[363] *100 000 sollen elektronisch abstimmen können*. NZZ. 1. Dez. 2007. URL: https://www.wiso-net.de/document/NZZ__e2368eb38c29532c83877bb3a22b3cd0d41b9836.

[364] *Heftige Schelte für drei Zürcher Kreiswahlbüros*. NZZ. 8. Nov. 2007. URL: https://www.wiso-net.de/document/NZZ__57b38194b8fd179df11412eb9b6faa4b8153e07b.

[365] *Chantal Galladé als Phantom-Kandidatin*. NZZ. 7. Nov. 2007. URL: https://www.wiso-net.de/document/NZZ__df870db4cb2ed69efb51d07e2dbe71d6743ef1b2.

[366] *«Ein Super-GAU wäre denkbar»*. NZZ. 15. Okt. 2007. URL: https://www.wiso-net.de/document/NZZ__87fc83867a5aa15f9f55e918f66c59283ae9e336.

[367] *Fünfte Schweiz lässt SVP zappeln*. NZZ. 18. Aug. 2007. URL: https://www.wiso-net.de/document/NZZ__bfd185a9d5c54faddf25e442a8b27e44fa4c2698.

[368] *Bemühen um Vertretung der Fünften Schweiz*. NZZ. 6. Aug. 2007. URL: https://www.wiso-net.de/document/NZZ__50f04d5a97b80a843f15e29c71860f3a6930a99f.

[369] *Die briefliche Stimmabgabe wirkt mobilisierend*. NZZ. 4. Aug. 2007. URL: https://www.wiso-net.de/document/NZZ__8caca328c4ce8f7e4a4e82d299bed7a84880308f.

[370] *Uno zeichnet Zürcher Versuch für E-Voting aus*. NZZ. 18. Juni 2007. URL: https://www.wiso-net.de/document/NZZ__334a91beb665d142a069a0351a072adf7e518b72.

[371] *Falsch gedruckte Stimmrechtsausweise*. NZZ. 24. Mai 2007. URL: https://www.wiso-net.de/document/NZZ__9af60a86f680eb9c9bf0eb136c4f2f9532ad2e15.

[372] *Schweiz und USA diskutieren über E-Voting*. NZZ. 25. Apr. 2007. URL: https://www.wiso-net.de/document/NZZ__1204528d1ca5d08d3c91233e2f36baa87689715a.

[373] *Auslandschweizer drängen auf E-Voting*. NZZ. 2. Apr. 2007. URL: https://www.wiso-net.de/document/NZZ__953616004a93bcffc50d55a255cb93653af5b3e1.

[374] *30 000 Stimmen per Mausklick*. NZZ. 3. März 2007. URL: https://www.wiso-net.de/document/NZZ__66c0b91b18bfd6e5f1e00bbc587382107a35f68b.

[375] *Wahl des Studierendenrats muss wiederholt werden / Fehlerhafte Wahlausweise*. NZZ. 15. Dez. 2006. URL: https://www.wiso-net.de/document/NZZ__dc199ced8597db8ef8bb4d990b6c32f0ee48e7bb.

[376] *In kleinen Schritten zum E-Voting*. NZZ. 5. Dez. 2006. URL: https://www.wiso-net.de/document/NZZ__94ce95a8592b45107a0a29e569f1596f7daea658.

[377] *Debattieren auf der Baustelle*. NZZ. 5. Dez. 2006. URL: https://www.wiso-net.de/document/NZZ__645333154b5ff635199492011b45d5574c777b3b.

[378] *«E-Democracy» als Chance / Breitere Partizipationsmöglichkeiten*. NZZ. 1. Nov. 2006. URL: https://www.wiso-net.de/document/NZZ__91821a256281e5778a66e3ac8cfc8fa46f0a906e.

[379] *Bund genehmigt weitere elektronische Abstimmungen*. NZZ. 14. Sep. 2006. URL: https://www.wiso-net.de/document/NZZ__c770e7ac9d393e510c60c4ab6005f15a28c10ed1.

[380] *Erfolgreiches E-Voting-Pilotprojekt in Bülach / Versuch auch auf Bundesebene*. NZZ. 31. Aug. 2006. URL: https://www.wiso-net.de/document/NZZ__0979827190eae0e81ab1444e517d919ec6014908.

[381] *Die Demokratie und das Internet*. NZZ. 24. Juli 2006. URL: https://www.wiso-net.de/document/NZZ__338a938cf0d4ec6875f5c159ac7aa4b8004bb0d2.

[382] *Massvoller Ausbau elektronischer Stimmabgabe.* NZZ. 1. Juni 2006. URL: https://www.wiso-net.de/document/NZZ__73fa402aa250d767c5197e8c51195ffa00c4ccf3.

[383] *Wieso man geheim abstimmt*. NZZ. 29. Apr. 2006. URL: https://www.wiso-net.de/document/NZZ__ae352f9b14e9c47619ca5a007c46f7ffd24c3de8.

[384] *Kaderschmieden* / Einen Master in E-Governance*. NZZ. 11. Apr. 2006. URL: https://www.wiso-net.de/document/NZZ__dc4cead4523ddd2e5ee4ab2cdf17bf7e244ace92.

[385] *Schwarzer Wahltag für FDP in Bülach / Zwei Stadträte abgewählt*. NZZ. 3. Apr. 2006. URL: https://www.wiso-net.de/document/NZZ__dbb115bf0facc513e5c62d7e0881c9da9da87d0a.

[386] *Eine nicht zu vernachlässigende Stimmkraft*. NZZ. 3. Apr. 2006. URL: https://www.wiso-net.de/document/NZZ__e62c1c905970f94d3bae93afba99b9d06bd6d45b.

[387] *Stippvisite internationaler Wahlbeobachter / Am Wahltag unterwegs mit dem Mathematiker Friedrich Pukelsheim und seiner Gefolgschaft*. NZZ. 13. Feb. 2006. URL: https://www.wiso-net.de/document/NZZ__b26e9732a14cd90997d997c00fa0c845c9240d92.

[388] *Elektronisch wählen in Bülach / Gemeindewahlen 2006 mit E-Voting*. NZZ. 19. Dez. 2005. URL: https://www.wiso-net.de/document/NZZ__7d6adc13590459f38f11eca4ba4d31595a17dc46.

[389] *Kanton will elektronisches Abstimmen forcieren*. NZZ. 28. Nov. 2005. URL: https://www.wiso-net.de/document/NZZ__5a372945a43e1e80b7ab93f496b5f4abea65c7f5.

[390] *Bülach: weniger Stadtratsmitglieder*. NZZ. 28. Nov. 2005. URL: https://www.wiso-net.de/document/NZZ__c51cf5b7a071342d31c6907cdd8c8c5302dea971.

[391] *Über ein Drittel stimmte per SMS oder Internet*. NZZ. 31. Okt. 2005. URL: https://www.wiso-net.de/document/NZZ__2a945ea59fbb8f1341edfd7f09215f71bbcaaded.

[392] *Nicht ganz ohne Tücken / Abstimmen per SMS in Bülach*. NZZ. 15. Okt. 2005. URL: https://www.wiso-net.de/document/NZZ__b00a21f8175b3740068af93c839168a997fa90d9.

[393] *Umstrittene Bülacher / Abstimmungszeitung / Tempo-30-Zonen als Streitobjekt*. NZZ. 11. Okt. 2005. URL: https://www.wiso-net.de/document/NZZ__63814ee7ea678c3a6740e0b04b1b61b7cef04437.

[394] *Verfahren für elektronisches Abstimmen festgelegt*. NZZ. 16. Sep. 2005. URL: https://www.wiso-net.de/document/NZZ__a430c090af1523f014ecc11102e5fd440be7cbd6.

[395] *Die Termine der nächsten Abstimmungen*. NZZ. 9. Sep. 2005. URL: https://www.wiso-net.de/document/NZZ__1c26b8ea4091ac0f1bc796ccc01439ab691da606.

[396] *Kantonale E-Voting-Premiere nur in drei Gemeinden*. NZZ. 11. Aug. 2005. URL: https://www.wiso-net.de/document/NZZ__24d2a782559c894657e8bbc19bf7f4721d59c706.

[397] *Nebenbei notiert / Es stand in der Zeitung*. NZZ. 12. Juli 2005. URL: https://www.wiso-net.de/document/NZZ__b7d2c30a9dc4d92c02a2ef11bea1851a8df6c4ad.

[398] *Kantonsspitäler vor Verselbständigung / Linke unterliegen mit allen Minderheitsanträgen / Selbständigeres Unispital Unterlassungssünde der Kommission Schicksalsparagraph 13? Diener: «Volksabstimmung sicher» Bürgerliche setzen sich durch Spitäler bekommen Startgeld Geplänkel um Taxen Knapp gegen Fremdmittel / Kantonsspital Winterthur Stichentscheid gegen die eigene Fraktion*. NZZ. 12. Juli 2005. URL: https://www.wiso-net.de/document/NZZ__0e3e8f6fdd077b52cb0f99038552fc436fae5904.

[399] *Abstimmung über Integrationskurse erst später / E-Voting-Projekt als Begründung*. NZZ. 9. Juli 2005. URL: https://www.wiso-net.de/document/NZZ__0df560c3be271301a9a826ed2472b2af03f4dddc.

[400] *Jeder Fünfte nutzte E-Voting*. NZZ. 26. Apr. 2005. URL: https://www.wiso-net.de/document/NZZ__daab9d1cf8b395f2a6206fd92acded288045eb48.

[401] *E-Voting feiert in Bülach Premiere*. NZZ. 22. Apr. 2005. URL: https://www.wiso-net.de/document/NZZ__06c38a848f2ec6e190a4deccdeea51d2381f64d2.

[402] *Bund verzichtet auf virtuellen Amtsschalter / / Der Föderalismus als Hindernis*. NZZ. 22. März 2005. URL: https://www.wiso-net.de/document/NZZ__1b4a065cf4497a772a3792e30f0e6b2c0a115a9d.

[403] *Kein Berner Alleingang beim elektronischen Abstimmen*. NZZ. 15. Feb. 2005. URL: https://www.wiso-net.de/document/NZZ__6ce835e79153f9ca26b8746ea0d39af81df2f039.

[404] *E-Voting - ein Rückschritt*. NZZ. 6. Jan. 2005. URL: https://www.wiso-net.de/document/NZZ__ad5b5b7e36d7ed67944ca9b1524d440f754b925f.

[405] *Neue Rechte im Kanton Zürich*. NZZ. 3. Jan. 2005. URL: https://www.wiso-net.de/document/NZZ__bdcf889edc14e40b6df1d49ab8d9a15047739o2d.

[406] *Erfolgreicher Test für E-Voting-System*. NZZ. 15. Dez. 2004. URL: https://www.wiso-net.de/document/NZZ__e85417391562ob26600a4134f6024891ad0619b1.

[407] *Testlauf für die elektronische Wahl / E-Voting-Pilotprojekt an der Universität Zürich*. NZZ. 20. Nov. 2004. URL: https://www.wiso-net.de/document/NZZ__98000036ad0470bfd25a1fa8e0052a475c736e9e.

[408] *Genf erhält Preis für Pionierarbeit im E-Voting*. NZZ. 16. Nov. 2004. URL: https://www.wiso-net.de/document/NZZ__8311cddab88386c5bb2a38c5c48dff41c11cde05.

[409] *Schritt für Schritt zum «Vote électronique» / Testphase für die Schweizer Pilotprojekte*. NZZ. 12. Nov. 2004. URL: https://www.wiso-net.de/document/NZZ__fc95a1fb129c4e2024cd225aa1a93b104db414fd.

[410] *Eine moderne, neue Stadt am Zürichsee*. NZZ. 11. Nov. 2004. URL: https://www.wiso-net.de/document/NZZ__ec71ab3d204b08afcc655ce3cf1a941a0ae40c91.

[411] *Versuch mit E-Voting wird ausgeweitet*. NZZ. 2. Okt. 2004. URL: https://www.wiso-net.de/document/NZZ__2796944f3e34770beffa6ee7b6ce9a113fc87195.

[412] *Sparpotenzial bei der Stadtverwaltung*. NZZ. 23. Sep. 2004. URL: https://www.wiso-net.de/document/NZZ__9cf3b8dd121c9b738cb161023238e1284f622880.

[413] *E-Voting hat einen schweren Stand*. NZZ. 15. Sep. 2004. URL: https://www.wiso-net.de/document/NZZ__7ca5ec56d2faa84d0d683ddf14f5eec9371b2c9f.

[414] *Genf testet E-Voting / Test bei eidgenössischer Abstimmung*. NZZ. 11. Sep. 2004. URL: https://www.wiso-net.de/document/NZZ__e524d6a13169cfd26cceddo3124c183ded17b0f0.

[415] *Elektronisches Abstimmen ab 2005 möglich / Die Technik für erste Projekte wäre bereit*. NZZ. 27. Aug. 2004. URL: https://www.wiso-net.de/document/NZZ__931c0e3453c0f414d2859d5183b7232f8e6b34ce.

[416] *Der lange Weg zur virtuellen Amtsstube / E-Government in der Schweiz*. NZZ. 12. März 2004. URL: https://www.wiso-net.de/document/NZZ__be26cbf590b0dafe60b98608af0766427df90f6a.

[417] *Kantonales Datennetzwerk / Kanton zahlt weiterhin Anschlusskosten*. NZZ. 16. Jan. 2004. URL: https://www.wiso-net.de/document/NZZ__c6982b153ebbe00a2928c8c95f2739196eba4d03.

[418] *Die Nachträge verschlechtern das kantonale Budget 2004 nur wenig*. NZZ. 7. Nov. 2003. URL: https://www.wiso-net.de/document/NZZ__fd995b04b5b341ff772ebfddf73740ce8ae997b9.

[419] *www.ch.ch / Der nationale Guichet virtuel wird ausgebaut*. NZZ. 31. Okt. 2003. URL: https://www.wiso-net.de/document/NZZ__431143fc457c1269e9787b278aa3b80d4914dc6e.

[420] *Über die Wahlbeteiligung der jüngeren Wahlberechtigten*. NZZ. 11. Okt. 2003. URL: https://www.wiso-net.de/document/NZZ__20a1f46d2da222dcfacff4a557fe8b2f26cfb3de.

[421] *Kanton Zürich vergibt Projekt für E-Voting*. NZZ. 6. Okt. 2003. URL: https://www.wiso-net.de/document/NZZ__b4be5af93c9a29e3a5478f624d10dc2f66b7496b.

[422] *Die Sitzung im Überblick*. NZZ. 23. Sep. 2003. URL: https://www.wiso-net.de/document/NZZ__bb3e1b5ca6cdc611e8be6563011740643obc3235.

[423] *Zu grosse Ausfälle für den Kanton Abstimmung In Unkenntnis entschieden / Abstimmung*. NZZ. 23. Sep. 2003. URL: https://www.wiso-net.de/document/NZZ__25ce3a7492e4d65eedf37f8889f5a3d16cc33ee2.

[424] *«Wir sind in vielen Punkten visionär»*. NZZ. 10. Juni 2003. URL: https://www.wiso-net.de/document/NZZ__f429954fdef215eaf4d6d4cb91890b448cd07426.

[425] *Wo Urnengang noch Gang zur Urne bedeutet*. NZZ. 19. Mai 2003. URL: https://www.wiso-net.de/document/NZZ__8bc576b151e70cfdb170c8a3bb0e8a2440b13ace.

[426] *Neuregelung der politischen Rechte / Kein passives Wahlrecht für Ausländer / Politische Rechte Zuerst Schweizer werden Plutokratie / Wahlrecht für Ausländer Wahllisten*. NZZ. 8. Apr. 2003. URL: https://www.wiso-net.de/document/NZZ__c62b469db2b87f0559fec9b02ccc248bb882a5ed.

[427] *Entwurf eines Gesetzes über politische Rechte*. NZZ. 2. Okt. 2002. URL: https://www.wiso-net.de/document/NZZ__e75cb9057f58edb8ee158498d12f9a6dd5a12f22.

[428] *Verelendung nicht zwingend / Droht der Gesellschaft eine «digitale Spaltung»?* NZZ. 16. Aug. 2002. URL: https://www.wiso-net.de/document/NZZ__9db57239b955e5d17902bcb13c41838736a08956.

[429] *Ein Schlüssel für viele Schlösser*. NZZ. 2. Juli 2002. URL: https://www.wiso-net.de/document/NZZ__594228064eef82501e3689c9e0107ba774ed384b.

[430] *Arbeitsbewilligungen über das Internet / Der Stand des Zürcher E-Government*. NZZ. 27. Mai 2002. URL: https://www.wiso-net.de/document/NZZ__b804fb020f7e793dc4e95bf79c3add2ef5bed2ff.

[431] *Probeläufe mit E-Voting*. NZZ. 15. Mai 2002. URL: https://www.wiso-net.de/document/NZZ__bcaa682743e47baeccceb5b07bd68218fdc9f14c.

[432] *Das E-Voting fordert die Demokratie heraus*. NZZ. 15. Mai 2002. URL: https://www.wiso-net.de/document/NZZ__2cd475c1fe5620f0252a65a6c49eac94d7f01bb7.

[433] *Pilotprojekte zur elektronischen Stimmabgabe*. NZZ. 15. Mai 2002. URL: https://www.wiso-net.de/document/NZZ__4501f8a27ac395eccfcd5c9360b806537f329211.

[434] *Zwischen 97 und 2 Prozent*. NZZ. 15. Mai 2002. URL: https://www.wiso-net.de/document/NZZ__6b41b349e88da65c01a0a0295159aced42f20fea.

[435] *Wo steht die Informationsgesellschaft in der Schweiz?* NZZ. 4. Mai 2002. URL: https://www.wiso-net.de/document/NZZ__c938b25a2169b5a2b19687a6547e80af19976689.

[436] *Gesetzliche Grundlage für E-Voting schafft erste Hürde*. NZZ. 20. März 2002. URL: https://www.wiso-net.de/document/NZZ__609a81b556b5963a3548decb96432d0e55576fe2.

[437] *Politische Rechte / Elektronische Demokratie*. NZZ. 20. März 2002. URL: https://www.wiso-net.de/document/NZZ__dc5ef29cf8bda5fd91e8b02f87a76943691bc62b.

[438] *Briten testen E-Voting*. NZZ. 15. Feb. 2002. URL: https://www.wiso-net.de/document/NZZ__8c49fbf9a491f56c83076b27d90519479606f362.

[439] *E-Voting in der Schweiz frühestens 2010*. NZZ. 10. Jan. 2002. URL: https://www.wiso-net.de/document/NZZ__06e8d08beb0d6fa323f9f7b74f5275b27b2d908c.

[440] *E-Voting/ und Frauenförderung / Bundesrat beantragt Änderungen*. NZZ. 1. Dez. 2001. URL: https://www.wiso-net.de/document/NZZ__844b2f1070811dc88390791ae6b6ae0515536477.

[441] *Digitale Signaturen und unfallträchtige Fahrer*. NZZ. 22. Juni 2001. URL: https://www.wiso-net.de/document/NZZ__b1422e515084927fe486a3008713d2a72ca7619b.

[442] *Bund will Versuche mit E-Voting starten /Änderungen der politischen Rechte*. NZZ. 19. Juni 2001. URL: https://www.wiso-net.de/document/NZZ__724ed232395f77c6966cecb0ca95b2ff28196c35.

[443] *Internetprojekte des Kantons / Bald elektronische Abstimmungen?* NZZ. 8. Juni 2001. URL: https://www.wiso-net.de/document/NZZ__62396593b4053afd408a9bd2dc1ca942913b42b9.

[444] *Kampf gegen die digitale Spaltung*. NZZ. 16. Mai 2001. URL: https://www.wiso-net.de/document/NZZ__bb3a232ce29d90e62aa0a3443ec7c0506b5d3a1c.

[445] *Pilotversuche für elektronisches Abstimmen*. NZZ. 6. Apr. 2001. URL: https://www.wiso-net.de/document/NZZ__d781d9ac9ec3a53671fa31b21bdfe95eb5f825fb.

[446] *Genfer Versuch mit Stimmabgabe per Internet*. NZZ. 23. März 2001. URL: https://www.wiso-net.de/document/NZZ__92a6988248ec7ee100802e589426f5ce801c9a93.

[447] *Ein Drittel der Gemeinden mit Webseite*. NZZ. 21. Feb. 2001. URL: https://www.wiso-net.de/document/NZZ__96aa9b7cba9a5c26ba60d63104a7ecd37ddb7b37.

[448] *Die e-ssoufflierte Demokratie*. NZZ. 19. Jan. 2001. URL: https://www.wiso-net.de/document/NZZ__c179db52abb18965ad1803ec64bdf82216b157bf.

[449] *Wie sieht «E-Switzerland» aus?* NZZ. 13. Jan. 2001. URL: https://www.wiso-net.de/document/NZZ__9d81e2f4962a2d9737d832b2b1aeeda7d5576e17.

[450] *Regierungen im Banne der «Informationsgesellschaft» / Der Staat muss Bedingungen für Chancengleichheit beim Netzzugang schaffen*. NZZ. 13. Jan. 2001. URL: https://www.wiso-net.de/document/NZZ__59aafdf3ee2c0253ec6a8e7177fd20a7e41ec30f.

[451] *Virtueller Amtsschalter / Eröffnung auf Ende 2001 vorgesehen*. NZZ. 15. Dez. 2000. URL: https://www.wiso-net.de/document/NZZ__8013ff27feefaf88011522d0a77da70ece78759e.

[452] *«e-census» - Volkszählung auch per Internet /Europapremiere in der Schweiz*. NZZ. 28. Sep. 2000. URL: https://www.wiso-net.de/document/NZZ__b3edc5c3e8f10d37706ad8d24ad4a3e17805c161.

[453] *Erste Fanfarenstösse für den virtuellen Staat*. NZZ. 26. Sep. 2000. URL: https://www.wiso-net.de/document/NZZ__1da290f4b73150fa17875b25ac9401d5ee9a7253.

[454] *Wer hört mit? / Digitale Zertifikate als sichere Punkte im Web-Dschungel*. NZZ. 26. Sep. 2000. URL: https://www.wiso-net.de/document/NZZ__77ce5914d5d0fbe08b2ade0fe1468256fc7846b9.

[455] *Bundesrat will Heimatbindung durch E-Voting fördern*. NZZ. 21. Aug. 2000. URL: https://www.wiso-net.de/document/NZZ__e0b098acadc151996e2a550ab6271b8df3f96db7.

[456] *Gegen das digitale Analphabetentum*. NZZ. 11. Juli 2000. URL: https://www.wiso-net.de/document/NZZ__647a23532b4398eb38b130514a2ea2adeb81cd00.

[457] *CIA director urged Bolsonaro to stop doubting Brazil's voting system – report; Fears Brazilian president might refuse to accept defeat in this year's election as leftist rival Lula is set to announce candidacy.* The Guardian. 5. Mai 2022. URL: https://link.gale.com/apps/doc/A702634250/AONE?u=fub&sid=bookmark-AONE&xid=46df9e6f.

[458] *Trump loyalists form alliance in bid to take over election process in key states; 'Coalition of America First secretary of state candidates' disclosed by Jim Marchant, who is running for secretary of state in Nevada.* The Guardian. 13. Jan. 2022. URL: https://link.gale.com/apps/doc/A689464925/AONE?u=fub&sid=bookmark-AONE&xid=8c41d301.

[459] *Capitol attack panel subpoenas author of PowerPoint plan for coup; Trump operative who outlined 'Options for 6 Jan' met with the president's chief of staff repeatedly before the Capitol riot.* The Guardian. 16. Dez. 2021. URL: https://link.gale.com/apps/doc/A687129191/AONE?u=fub&sid=bookmark-AONE&xid=cf78eb45.

[460] *Capitol attack panel obtains PowerPoint that set out plan for Trump to stage coup; Presentation turned over by Mark Meadows made several recommendations for Trump to pursue to retain presidency.* The Guardian. 11. Dez. 2021. URL: https://link.gale.com/apps/doc/A686450181/AONE?u=fub&sid=bookmark-AONE&xid=52fc22ed.

[461] *Russian MP denies illegal hunting after shot elk found in car; Police say Communist party's Valery Rashkin claimed to have found animal after it had been killed.* The Guardian. 29. Okt. 2021. URL: https://link.gale.com/apps/doc/A680643026/AONE?u=fub&sid=bookmark-AONE&xid=b58672c1.

[462] *The Guardian view on Brazil's Bolsonaro: democracy is under attack; The far-right president has never hidden his admiration for dictatorship. There are growing fears he will not accept defeat in next year's election.* The Guardian. 8. Sep. 2021. URL: https://link.gale.com/apps/doc/A676397748/AONE?u=fub&sid=bookmark-AONE&xid=5873009a.

[463] *Election victory, death or prison: Bolsonaro names his three alternatives for 2022; Brazilian president's remark to evangelical leaders came as he questioned country's voting system.* The Guardian. 29. Aug. 2021. URL: https://link.gale.com/apps/doc/A673648026/AONE?u=fub&sid=bookmark-AONE&xid=d9f367d2.

[464] *World can't tolerate 'premature death' of Brazil's democracy, says Bolsonaro rival; The centre-left politician Ciro Gomes tells the Guardian that Brazil is 'living through the worst government in its history'.* The Guardian. 16. Juli 2021. URL: https://link.gale.com/apps/doc/A668696615/AONE?u=fub&sid=bookmark-AONE&xid=b4ce4419.

[465] *First Thing: Record-shattering heatwave bakes western US amid mega-drought; Soaring temperatures raise fears over drought and fire, and Juneteenth is now a federal holiday. Plus, the man who swallowed an AirPod.* The Guardian. 18. Juni 2021. URL: https://link.gale.com/apps/doc/A665486823/AONE?u=fub&sid=bookmark-AONE&xid=3e2b75c7.

[466] *Trump social media ban sparks calls for action against other populist leaders; After US president's ban, some wonder if action will be taken against populists accused of using social media to stir chaos.* The Guardian. 17. Jan. 2021. URL: https://link.gale.com/apps/doc/A648777584/AONE?u=fub&sid=bookmark-AONE&xid=a3f93487.

[467] *The Guardian view on delayed elections: make democracy a priority; By loosening restrictions on shopping while saying nothing about voting in England, ministers are sending the wrong signal.* The Guardian. 21. Juni 2020. URL: https://link.gale.com/apps/doc/A627246509/AONE?u=fub&sid=bookmark-AONE&xid=133ca2f1.

[468] *The Guardian view on Covid-19 and politics: institutionally vulnerable; British government and parliamentary democracy are trapped in outdated buildings and habits. The coronavirus has exposed the need to rethink how they workCoronavirus – latest updatesSee all our coronavirus coverage.* The Guardian. 29. März 2020. URL: https://link.gale.com/apps/doc/A618912095/AONE?u=fub&sid=bookmark-AONE&xid=2f3ce194.

[469] *The coronavirus crisis will pass, but life may never be 'normal' again; From exams to the five-day week, the pandemic is making us question our everyday practices. Some changes will stick.* The Guardian. 13. März 2020. URL: https://link.gale.com/apps/doc/A617323488/AONE?u=fub&sid=bookmark-AONE&xid=d997ca1d.

[470] *Cyber attacks and electronic voting errors threaten 2020 outcome, experts warn; Key Democrats and election analysts say more needs to be done to ensure safe elections free from 'foreign malicious actors'.* The Guardian. 2. Jan. 2020. URL: https://link.gale.com/apps/doc/A610273885/AONE?u=fub&sid=bookmark-AONE&xid=396abe1f.

[471] *Russian hackers likely to target Florida again in 2020 election, experts warn; Florida was targeted in the 2016 election as a critical swing state and 'should assume they will be targeted again'.* The Guardian. 27. Aug. 2019. URL: https://link.gale.com/apps/doc/A597533354/AONE?u=fub&sid=bookmark-AONE&xid=fe9aeba4.

[472] *DRC opposition blames election day problems on government; Polling station difficulties said to be aimed at ensuring victory for protege of President Kabila.* The Guardian. 30. Dez. 2018. URL: https://link.gale.com/apps/doc/A567807180/AONE?u=fub&sid=bookmark-AONE&xid=5d55f7ca.

[473] *Coalition pushes for voter identification laws and launches attack on GetUp; Labor warns demanding proof of identity at polling booths is a 'pathway to voter suppression'.* The Guardian. 5. Dez. 2018. URL: https://link.gale.com/apps/doc/A564373047/AONE?u=fub&sid=bookmark-AONE&xid=84ee552e.

[474] *In Brazil, only the grandest of coalitions can now defeat Bolsonaro; Experts believe rival Fernando Haddad must position himself as a centrist champion of democracy.* The Guardian. 8. Okt. 2018. URL: https://link.gale.com/apps/doc/A557339309/AONE?u=fub&sid=bookmark-AONE&xid=c6f37583.

[475] *Congo's splintered opposition vows to defy repression and return to streets; Opposition figures in the DRC risk imprisonment, injury or even death. But still they speak out against President Joseph Kabila.* The Guardian. 26. Apr. 2018. URL: https://link.gale.com/apps/doc/A536278309/AONE?u=fub&sid=bookmark-AONE&xid=1b6ce8e2.

[476] *Over-16s to get voting rights in some Welsh elections; Welsh government also plans to give local election votes to foreign nationals living in Wales.* The Guardian. 28. Jan. 2018. URL: https://link.gale.com/apps/doc/A525422586/AONE?u=fub&sid=bookmark-AONE&xid=9216328a.

[477] *Parliament's palace of booze and sex seems bad, but it has been a lot worse; Modern Westminster might seem on the verge of moral and physical disaster. But to MPs of previous generations it would probably seem quite a sober place*. The Guardian. 9. Dez. 2017. URL: https://link.gale.com/apps/doc/A518154495/AONE?u=fub&sid=bookmark-AONE&xid=8dde9a87.

[478] *Tony Abbott-backed motion for NSW Liberal preselections wins party support; Votes on other reform models yet to be held but Waringah proposal wins 61% majority of party's members in NSW*. The Guardian. 23. Juli 2017. URL: https://link.gale.com/apps/doc/A499072980/AONE?u=fub&sid=bookmark-AONE&xid=6e5a1794.

[479] *How do you solve Britain's youth voting crisis? With the voter registration deadline looming, young people are being targeted with the usual patronising hashtags and bad Snapchats. Is there a better way?* The Guardian. 18. Mai 2017. URL: https://link.gale.com/apps/doc/A491932930/AONE?u=fub&sid=bookmark-AONE&xid=bf534167.

[480] *Russian involvement in US vote raises fears for European elections; CIA investigation may have implications for upcoming French and German polls, even raising doubts over integrity of Brexit vote*. The Guardian. 10. Dez. 2016. URL: https://link.gale.com/apps/doc/A473541476/AONE?u=fub&sid=bookmark-AONE&xid=f6792e8b.

[481] *Jill Stein raises over $2m to request US election recounts in battleground states; Green party presidential candidate seeks donations to fund efforts in Michigan, Pennsylvania and Wisconsin over 'compelling evidence of voting anomalies'*. The Guardian. 24. Nov. 2016. URL: https://link.gale.com/apps/doc/A471310441/AONE?u=fub&sid=bookmark-AONE&xid=1187b5c0.

[482] *Hillary Clinton urged to call for election vote recount in key states; Alleged irregularities in battleground states of Michigan, Pennsylvania and Wisconsin prompt demands for audit amid concerns over 'foreign hackers'*. The Guardian. 23. Nov. 2016. URL: https://link.gale.com/apps/doc/A471194428/AONE?u=fub&sid=bookmark-AONE&xid=d9a5a114.

[483] *Why the rush? In defence of Australia's slow election count; Bill Shorten and Malcolm Turnbull want to move to electronic voting but in this election it wouldn't have saved time and is fraught with risk*. The Guardian. 11. Juli 2016. URL: https://link.gale.com/apps/doc/A457605476/AONE?u=fub&sid=bookmark-AONE&xid=be01f69b.

[484] *Malcolm Turnbull and Bill Shorten back move to electronic voting; Bipartisan push comes as both leaders concede the voting system needs to be sped up, and PM calls for regulations to cover political texts and robocalls*. The Guardian. 10. Juli 2016. URL: https://link.gale.com/apps/doc/A457510984/AONE?u=fub&sid=bookmark-AONE&xid=c47139f1.

[485] *Utah's e-caucus mess: why online voting in the state Cruz swept was so flawed; Utah's new online voting system was supposed to boost participation in the Republican caucus, but instead it was plagued by glitches. What went wrong?* The Guardian. 23. Apr. 2016. URL: https://link.gale.com/apps/doc/A450376558/AONE?u=fub&sid=bookmark-AONE&xid=8d20d318.

[486] *I've had bruising encounters with trade unions, but I condemn efforts to silence them; For all my frustrations as former head of the civil service, I fear that the trade union bill shows a worryingly authoritarian streak in this government*. The Guardian. 11. Jan. 2016. URL: https://link.gale.com/apps/doc/A439561438/AONE?u=fub&sid=bookmark-AONE&xid=215419ea.

[487] *Brazil's supreme court suspends impeachment moves against president; High drama as judge steps in after committee that will decide whether or not to undertake proceedings against Dilma Rousseff is packed with her opponents*. The Guardian. 9. Dez. 2015. URL: https://link.gale.com/apps/doc/A436988111/AONE?u=fub&sid=bookmark-AONE&xid=58621f1f.

[488] *Tommy Sheppard's top 10 most ridiculous things about Westminster; SNP MP for Edinburgh East devotes party conference speech to poking fun at customs and practices of Palace of Westminster*. The Guardian. 16. Okt. 2015. URL: https://link.gale.com/apps/doc/A431821653/AONE?u=fub&sid=bookmark-AONE&xid=2de46387.

[489] *Cameron challenged by TUC on claim that he met leadership over trade bill; Prime Minister accused of dodging negotiations after refusing to consider Len McCluskey offer to drop opposition to trade union reform*. The Guardian. 4. Okt. 2015. URL: https://link.gale.com/apps/doc/A430698946/AONE?u=fub&sid=bookmark-AONE&xid=4b04a35f.

[490] *Tory conference: Cameron uses Marr to dismiss reports low-paid will lose out from tax credit cuts - Politics live; Rolling coverage of all the developments at the Conservative conference in Manchester, including David Cameron's interview on the Andrew Marr ShowDavid Cameron's Andrew Marr interview - Snap summary and analysis*. The Guardian. 4. Okt. 2015. URL: https://link.gale.com/apps/doc/A430698976/AONE?u=fub&sid=bookmark-AONE&xid=e7badf7e.

[491] *Sebastian Coe thought to be ahead of Sergey Bubka on eve of IAAF poll; * London 2012 chair lobbying until last minute in contest against Sergey Bubka * Lord Coe claims to have met representatives of every member association*. The Guardian. 18. Aug. 2015. URL: https://link.gale.com/apps/doc/A425895837/AONE?u=fub&sid=bookmark-AONE&xid=0a309b12.

[492] *Support the National Gallery strikes while they're still legal; Cameron's trade union bill will obstruct the kind of justified protests seen at the art museum this week*. The Guardian. 11. Aug. 2015. URL: https://link.gale.com/apps/doc/A425024061/AONE?u=fub&sid=bookmark-AONE&xid=8c09502b.

[493] *Is London's stranglehold on power a big turn-off for young voters? Many in the north feel like Westminster is too distant and doesn't serve them. Regional devolution may help to re-engage them; Many in the north feel like Westminster is too distant and doesn't serve them. Regional devolution may help to re-engage them*. The Guardian. 20. Apr. 2015. URL: https://link.gale.com/apps/doc/A410480933/AONE?u=fub&sid=bookmark-AONE&xid=48ff4aef.

[494] *Federal election review: voters should have to prove identity, says committee; Joint standing committee also calls for training and tighter rules for scrutineers in response to the loss of 1,370 Senate ballot papers in Western Australia in 2013*. The Guardian. 15. Apr. 2015. URL: https://link.gale.com/apps/doc/A409743373/AONE?u=fub&sid=bookmark-AONE&xid=619c4740.

[495] *The UK's political system is dying, but digital technology offers an alternative; Politicians can reverse the public's disenchantment with politics, but only once they fully embrace the digital age*. The Guardian. 1. Apr. 2015. URL: https://link.gale.com/apps/doc/A408441542/AONE?u=fub&sid=bookmark-AONE&xid=cb7eaee6.

[496] *NSW poll result could be challenged after parties are left off electronic ballot paper; About 19,000 people voted while Animal Justice party and Outdoor Recreation party were omitted from above-the-line voting squares on upper house ballot*. The Guardian. 18. März 2015. URL: https://link.gale.com/apps/doc/A405853207/AONE?u=fub&sid=bookmark-AONE&xid=8c764f0d.

[497] *MPC should consider jobless - O'Grady*. The Guardian. 5. Sep. 2014. URL: https://link.gale.com/apps/doc/A381568905/AONE?u=fub&sid=bookmark-AONE&xid=9c8baac6.

[498] *India's 551m voters usher in a new era: Exit polls show opposition win after massive turnout: Political outsider expected to oust centre-left party*. The Guardian. 13. Mai 2014. URL: https://link.gale.com/apps/doc/A367886087/AONE?u=fub&sid=bookmark-AONE&xid=fb8e29f9.

[499] *Electoral Commission examines online voting to attract under-25s*. The Guardian. 27. März 2014. URL: https://link.gale.com/apps/doc/A362952082/AONE?u=fub&sid=bookmark-AONE&xid=232e10a3.

[500] *Front: Fury with MPs is main reason for not voting: Poll reveals anger, not boredom, lies behind drop in political engagement*. The Guardian. 27. Dez. 2013. URL: https://link.gale.com/apps/doc/A354126107/AONE?u=fub&sid=bookmark-AONE&xid=fd577267.

[501] *Politics: Speaker sets up digital democracy commission*. The Guardian. 28. Nov. 2013. URL: https://link.gale.com/apps/doc/A350710465/AONE?u=fub&sid=bookmark-AONE&xid=12bf0be9.

[502] *Bloody nose for Putin after mayoral candidates give Kremlin a close run: Strong showing for critic Navalny in Moscow race: Anti-drugs activist within sight of win in key city*. The Guardian. 9. Sep. 2013. URL: https://link.gale.com/apps/doc/A342293977/AONE?u=fub&sid=bookmark-AONE&xid=0d943335.

[503] *Leading article: Kenya: President as defendant*. The Guardian. 11. März 2013. URL: https://link.gale.com/apps/doc/A321863226/AONE?u=fub&sid=bookmark-AONE&xid=93cf1bf4.

[504] *Saturday: I've just given a talk to some of Europe's leading money men. How timely*. The Guardian. 26. Nov. 2011. URL: https://link.gale.com/apps/doc/A273431094/AONE?u=fub&sid=bookmark-AONE&xid=10701670a.

[505] *National: Electoral reform: Coalition divisions: Gloves off as Clegg derides 'desperate' no campaign*. The Guardian. 16. Apr. 2011. URL: https://link.gale.com/apps/doc/A254127316/AONE?u=fub&sid=bookmark-AONE&xid=bf1fad77.

[506] *Comment: The anti-state right takes the Welsh for idiots who mustn't be left alone: Backing big government against the people is not so strange when what you really hate is state spending on the poor*. The Guardian. 1. März 2011. URL: https://link.gale.com/apps/doc/A250251280/AONE?u=fub&sid=bookmark-AONE&xid=18291805.

[507] *Reply: Letter: Brazil goes green and heads for the future*. The Guardian. 8. Okt. 2010. URL: https://link.gale.com/apps/doc/A238877354/AONE?u=fub&sid=bookmark-AONE&xid=1235a461.

[508] *Society: Interview: Chris Quigley: Curriculum vitae*. The Guardian. 28. Juli 2010. URL: https://link.gale.com/apps/doc/A232892048/AONE?u=fub&sid=bookmark-AONE&xid=66d848b5.

[509] *Review: Theatre: Counted? County Hall, London 3/5*. The Guardian. 22. Apr. 2010. URL: https://link.gale.com/apps/doc/A224486259/AONE?u=fub&sid=bookmark-AONE&xid=eb6a7d8d.

[510] *National: New voting rules for top Oxford poetry post*. The Guardian. 9. Dez. 2009. URL: https://link.gale.com/apps/doc/A213871963/AONE?u=fub&sid=bookmark-AONE&xid=f4586244.

[511] *Letter: Other lives: Keith Mothersson*. The Guardian. 23. Okt. 2009. URL: https://link.gale.com/apps/doc/A210371980/AONE?u=fub&sid=bookmark-AONE&xid=0cb8d915.

[512] *Technology: Counting the cost - electronically: Its meant to be faster and cheaper, but e-counting has been heavily criticised - though as Charles Arthur discovers, that hasn't stopped the London Assembly choosing it*. The Guardian. 1. Okt. 2009. URL: https://link.gale.com/apps/doc/A208756996/AONE?u=fub&sid=bookmark-AONE&xid=aea5e1ad.

[513] *International: Rebels attack polling stations as India votes: Killings and kidnappings by Maoists hit five states: High turnout elsewhere in month-long election*. The Guardian. 17. Apr. 2009. URL: https://link.gale.com/apps/doc/A197922821/AONE?u=fub&sid=bookmark-AONE&xid=cd59ac46.

[514] *International: Indian election: 700m voters, 28 days, 250,000 police: world's biggest democratic poll begins: Gandhi's ruling Congress party remains favourite: Big players expected to seek coalition partners*. The Guardian. 16. Apr. 2009. URL: https://link.gale.com/apps/doc/A197848497/AONE?u=fub&sid=bookmark-AONE&xid=042dec5e.

[515] *Technology: Opinion: Letters and blogs: Progress of a sort*. The Guardian. 20. Nov. 2008. URL: https://link.gale.com/apps/doc/A189481396/AONE?u=fub&sid=bookmark-AONE&xid=3810412d.

[516] *Technology: Inside IT: I vote for the old-fashioned way of balloting in elections*. The Guardian. 13. Nov. 2008. URL: https://link.gale.com/apps/doc/A188906495/AONE?u=fub&sid=bookmark-AONE&xid=9a9c1952.

[517] *Film &; Music: Film: Reviews: Swing Vote: 2 stars: Director: Joshua Michael Stern With: Kevin Costner, Madeline Carroll: 120 mins, cert 12A*. The Guardian. 26. Sep. 2008. URL: https://link.gale.com/apps/doc/A185614524/AONE?u=fub&sid=bookmark-AONE&xid=7be50c55.

[518] *Technology: Inside IT: Dear PM, please be more daring with e-democracy*. The Guardian. 29. Nov. 2007. URL: https://link.gale.com/apps/doc/A171890471/AONE?u=fub&sid=bookmark-AONE&xid=65ac89df.

[519] *Politics: Voters treated as afterthought in ballot fiasco, says inquiry: Commission, parties and officials criticised Scottish politicians accused of self-interest: Backstory*. The Guardian. 24. Okt. 2007. URL: https://link.gale.com/apps/doc/A170196970/AONE?u=fub&sid=bookmark-AONE&xid=7377ae74.

[520] *Electronic voting not safe, warns election watchdog*. The Guardian. 2. Aug. 2007. URL: https://link.gale.com/apps/doc/A167902982/AONE?u=fub&sid=bookmark-AONE&xid=6c816a77.

[521] *Browns reforms: PM offers to hand power to the people in constitution debate: Proposals may change relationship between citizen and state*. The Guardian. 4. Juli 2007. URL: https://link.gale.com/apps/doc/A165999632/AONE?u=fub&sid=bookmark-AONE&xid=41f1d0d2.

[522] *Comment &; Debate: The internet will revolutionise the very meaning of politics: The web could yet bypass government and existing political communities, and either expand democracy in the process - or stifle it*. The Guardian. 30. Mai 2007. URL: https://link.gale.com/apps/doc/A164215002/AONE?u=fub&sid=bookmark-AONE&xid=1ee14496.

[523] *Amid the chaos, Scotland takes historic step: SNP wins narrow victory: Salmond seeks Lib Dem deal: 100,000 ballots spoiled: Tories gain ground in England*. The Guardian. 5. Mai 2007. URL: https://link.gale.com/apps/doc/A163015040/AONE?u=fub&sid=bookmark-AONE&xid=225a637c.

[524] *National: Council poll monitors fear e-vote fraud*. The Guardian. 30. Apr. 2007. URL: https://link.gale.com/apps/doc/A162796574/AONE?u=fub&sid=bookmark-AONE&xid=1f8565e1.

[525] *The Guide: Film: In cinemas*. The Guardian. 21. Apr. 2007. URL: https://link.gale.com/apps/doc/A162842012/AONE?u=fub&sid=bookmark-AONE&xid=91516e12.

[526] *The Guide: film: in cinemas*. The Guardian. 14. Apr. 2007. URL: https://link.gale.com/apps/doc/A162109005/AONE?u=fub&sid=bookmark-AONE&xid=51e7d195.

[527] *Simon Hoggart's week: Just a bellow - or a roar of public rage?* The Guardian. 10. Feb. 2007. URL: https://link.gale.com/apps/doc/A159195703/AONE?u=fub&sid=bookmark-AONE&xid=1962b8f6.

[528] *International: US Midterms: Control of Senate hangs by thread as Virginia counts on: Media claim that Democrat has won crucial senate seat: The election goes on, says Republican incumbent*. The Guardian. 9. Nov. 2006. URL: https://link.gale.com/apps/doc/A154151745/AONE?u=fub&sid=bookmark-AONE&xid=6d7e1c2c.

[529] *Reply Letters and emails: Georges dragons*. The Guardian. 9. Nov. 2006. URL: https://link.gale.com/apps/doc/A154151776/AONE?u=fub&sid=bookmark-AONE&xid=d97a6da6.

[530] *International: Midterms 2006: Senate: Parties locked in mortal combat in southern testing ground*. The Guardian. 8. Nov. 2006. URL: https://link.gale.com/apps/doc/A154060880/AONE?u=fub&sid=bookmark-AONE&xid=59b18054.

[531] *International: Midterms 2006: The count: Electronic glitches put results under cloud*. The Guardian. 8. Nov. 2006. URL: https://link.gale.com/apps/doc/A154060883/AONE?u=fub&sid=bookmark-AONE&xid=5b0ed233.

[532] *Democrats pile pressure on Bush as glitches hit US poll: Republicans lose key Senate seats - reports Questions raised over electronic voting system*. The Guardian. 8. Nov. 2006. URL: https://link.gale.com/apps/doc/A154060923/AONE?u=fub&sid=bookmark-AONE&xid=47930e47.

[533] *Guardian Weekly: US News: Warning of chaos over electronic ballot*. The Guardian. 3. Nov. 2006. URL: https://link.gale.com/apps/doc/A154236738/AONE?u=fub&sid=bookmark-AONE&xid=bba8b2e2.

[534] *The Guide: Film: Doc/Fest Sheffield*. The Guardian. 28. Okt. 2006. URL: https://link.gale.com/apps/doc/A153565724/AONE?u=fub&sid=bookmark-AONE&xid=b4e83f5c.

[535] *US warned of ballot box chaos as elections near: Report says 10 states not ready for electronic vote: Scientist hacks into new polling machine on TV*. The Guardian. 27. Okt. 2006. URL: https://link.gale.com/apps/doc/A153384876/AONE?u=fub&sid=bookmark-AONE&xid=2d29b2b3.

[536] *Technology: Inside IT: By 2010, you just might be able to vote in your pyjamas*. The Guardian. 17. Aug. 2006. URL: https://link.gale.com/apps/doc/A149596876/AONE?u=fub&sid=bookmark-AONE&xid=41c0a542.

[537] *Epublic: Events: Events: What's on February-June*. The Guardian. 22. Feb. 2006. URL: https://link.gale.com/apps/doc/A142387350/AONE?u=fub&sid=bookmark-AONE&xid=962cce75.

[538] *Society 3: Epublic: E-democracy: Westminster tunes in to e-channels: As e-democracy begins to creep towards the mainstream, the influential Hansard Society says lack of innovation remains a stumbling block*. The Guardian. 23. Nov. 2005. URL: https://link.gale.com/apps/doc/A139043022/AONE?u=fub&sid=bookmark-AONE&xid=146502ed.

[539] *Society 3: Epublic: E-democracy: Voting searches for the x-factor: Electronic voting fell at the first hurdle during its 2003 trial run. Now attention has been turned to developing software to improve the current voting system*. The Guardian. 23. Nov. 2005. URL: https://link.gale.com/apps/doc/A139043023/AONE?u=fub&sid=bookmark-AONE&xid=13b15921.

[540] *Society: Europe unlimited: Estonia: Good things come in small packages: Estonia is a tiny, new country but that's given it an impetus to find online government solutions*. The Guardian. 23. Nov. 2005. URL: https://link.gale.com/apps/doc/A139043043/AONE?u=fub&sid=bookmark-AONE&xid=b62ba6c1.

[541] *ePublic: Government is getting there: Plans for an e-government revolution are being drawn up in Whitehall but they won't work unless people can be persuaded to think digitally about government. Michael Cross reports*. The Guardian. 26. Okt. 2005. URL: https://link.gale.com/apps/doc/A137971424/AONE?u=fub&sid=bookmark-AONE&xid=d3d8f51e.

[542] *ePublic: News: E-democracy: Government shelves internet voting trials*. The Guardian. 26. Okt. 2005. URL: https://link.gale.com/apps/doc/A137971429/AONE?u=fub&sid=bookmark-AONE&xid=9c0930b7.

[543] *Epublic: Crime prevention: Events What's on October-April*. The Guardian. 26. Okt. 2005. URL: https://link.gale.com/apps/doc/A137971446/AONE?u=fub&sid=bookmark-AONE&xid=b488dacf.

[544] *Policy &; Politics: E-voting plans shelved after extensive trials*. The Guardian. 7. Sep. 2005. URL: https://link.gale.com/apps/doc/A135892506/AONE?u=fub&sid=bookmark-AONE&xid=910a0ef8.

[545] *Online: Inside IT: May the source be with you: BitTorrent came under fire last week after it was used to distribute pirated copies of the latest Star Wars film. Quinn Norton investigates whether the software can ever shake off its illegal uses*. The Guardian. 2. Juni 2005. URL: https://link.gale.com/apps/doc/A132933823/AONE?u=fub&sid=bookmark-AONE&xid=1d24b55c.

[546] *ePublic: Cover story: Traditional systems get our vote: The internet may have revolutionised how we live, but it has yet to transform how we vote - despite strong government support. Michael Cross discovers that there's more to e-democracy than e-voting*. The Guardian. 20. Apr. 2005. URL: https://link.gale.com/apps/doc/A131755625/AONE?u=fub&sid=bookmark-AONE&xid=7cab4cce.

[547] *Life: This Week: The science behind the news: How long until I can vote electronically?* The Guardian. 7. Apr. 2005. URL: https://link.gale.com/apps/doc/A131230834/AONE?u=fub&sid=bookmark-AONE&xid=77456b09.

[548] *Online: Public domain: Michael Cross*. The Guardian. 24. März 2005. URL: https://link.gale.com/apps/doc/A130762291/AONE?u=fub&sid=bookmark-AONE&xid=dc599ec9.

[549] *Life: online: Feed Back: Free the software*. The Guardian. 10. März 2005. URL: https://link.gale.com/apps/doc/A130033244/AONE?u=fub&sid=bookmark-AONE&xid=8dc47998.

[550] *ePublic: Channels 2: Councils rise to the digital challenge: Plenty of services are now available online, but are people without web access being left out? Kim Thomas finds out what other digital channels are being employed by councils*. The Guardian. 23. Feb. 2005. URL: https://link.gale.com/apps/doc/A129085764/AONE?u=fub&sid=bookmark-AONE&xid=2ae89147.

[551] *Voters to challenge US election*. The Guardian. 1. Dez. 2004. URL: https://link.gale.com/apps/doc/A125563513/AONE?u=fub&sid=bookmark-AONE&xid=c028e349.

[552] *Comment &; Analysis: Letters: Rose may not bloom*. The Guardian. 12. Nov. 2004. URL: https://link.gale.com/apps/doc/A124566378/AONE?u=fub&sid=bookmark-AONE&xid=e7961a3f.

[553] *Comment &; Analysis: Letters: Christian values*. The Guardian. 11. Nov. 2004. URL: https://link.gale.com/apps/doc/A124490860/AONE?u=fub&sid=bookmark-AONE&xid=832b434a.

[554] *Close race rouses America: High turnout could break 44-year record of 63%: Kerry camp encouraged by early returns in key states*. The Guardian. 3. Nov. 2004. URL: https://link.gale.com/apps/doc/A124004163/AONE?u=fub&sid=bookmark-AONE&xid=133097f1.

[555] *Voters angry at chaos in early US polls*. The Guardian. 20. Okt. 2004. URL: https://link.gale.com/apps/doc/A123412341/AONE?u=fub&sid=bookmark-AONE&xid=b012e04c.

[556] *Comment &; Analysis: In the 60s, police dogs and billy clubs kept black Americans from the polls. Today's methods are more refined: Any means necessary*. The Guardian. 18. Okt. 2004. URL: https://link.gale.com/apps/doc/A123336336/AONE?u=fub&sid=bookmark-AONE&xid=b3ac9709.

[557] *Public Domain*. The Guardian. 2. Sep. 2004. URL: https://link.gale.com/apps/doc/A121541548/AONE?u=fub&sid=bookmark-AONE&xid=9e2bd058.

[558] *Online: What a way to run the country: As the government's outgoing e-envoy Andrew Pinder hands over the reins to his successor, he offers SA Mathieson an insight into the electronic revolution sweeping through Whitehall: Pushing against the tide: Andrew Pinder, soon after his appointment as e-envoy four years ago*. The Guardian. 2. Sep. 2004. URL: https://link.gale.com/apps/doc/A121541554/AONE?u=fub&sid=bookmark-AONE&xid=c30f4f14.

[559] *Massive turnout as Venezuela goes to polls: Fate of president mired in delays and alleged foul play*. The Guardian. 16. Aug. 2004. URL: https://link.gale.com/apps/doc/A120708596/AONE?u=fub&sid=bookmark-AONE&xid=a5e8f892.

[560] *Florida caught in political crosswinds again: Poll candidates fight for crucial US state as concerns linger*. The Guardian. 14. Aug. 2004. URL: https://link.gale.com/apps/doc/A120670609/AONE?u=fub&sid=bookmark-AONE&xid=af9dcda2.

[561] *Pin number to thwart vote cheats*. The Guardian. 7. Aug. 2004. URL: https://link.gale.com/apps/doc/A120324994/AONE?u=fub&sid=bookmark-AONE&xid=b19b8042.

[562] *Online: Talk Time: Al Franken: Satirist and broadcaster Al Franken's new book, Lies and Lying Liars Who Tell Them, is out now*. The Guardian. 5. Aug. 2004. URL: https://link.gale.com/apps/doc/A120198323/AONE?u=fub&sid=bookmark-AONE&xid=dba853ef.

[563] *Elections 2004: Legal threat over 'photo finish' in Hull after postal forms go astray: Delivered Raised turnout could be due to 'novelty' factor*. The Guardian. 12. Juni 2004. URL: https://link.gale.com/apps/doc/A118078362/AONE?u=fub&sid=bookmark-AONE&xid=ba647269.

[564] *Public Domain: Michael Cross*. The Guardian. 10. Juni 2004. URL: https://link.gale.com/apps/doc/A117993900/AONE?u=fub&sid=bookmark-AONE&xid=fcbb05d7.

[565] *Online: Man with a mission: Michael Cross on the task ahead for Ian Watmore, the new head of e-government*. The Guardian. 3. Juni 2004. URL: https://link.gale.com/apps/doc/A117604206/AONE?u=fub&sid=bookmark-AONE&xid=b18e7928.

[566] *Policy &; Politics: Elections June 2004: Delays threaten postal voting: North West returning officers in emergency meeting as printing problems add to the controversy dogging booth, free polling experiment*. The Guardian. 27. Mai 2004. URL: https://link.gale.com/apps/doc/A117256092/AONE?u=fub&sid=bookmark-AONE&xid=37208584.

[567] *Letters: India's win*. The Guardian. 14. Mai 2004. URL: https://link.gale.com/apps/doc/A116582931/AONE?u=fub&sid=bookmark-AONE&xid=208e56c9.

[568] *'Luckiest tenant' tackles parliament*. The Guardian. 3. Mai 2004. URL: https://link.gale.com/apps/doc/A116150455/AONE?u=fub&sid=bookmark-AONE&xid=ce44327f.

[569] *ePublic: In brief*. The Guardian. 21. Apr. 2004. URL: https://link.gale.com/apps/doc/A115626741/AONE?u=fub&sid=bookmark-AONE&xid=cb6047f4.

[570] *Killings overshadow India's general election*. The Guardian. 21. Apr. 2004. URL: https://link.gale.com/apps/doc/A115626693/AONE?u=fub&sid=bookmark-AONE&xid=059e8155.

[571] *Kerry sees off last rival in poll race*. The Guardian. 3. März 2004. URL: https://link.gale.com/apps/doc/A113857809/AONE?u=fub&sid=bookmark-AONE&xid=3b595a3a.

[572] *MCA Awards 2004: Highlighting Best Practice in Management Conslutancy: NEW WAYS TO VOTE: Now that turning up at the nearest polling station is not enticing enough people to vote, the Office of the Deputy Prime Minister, with Unisys, is considering a better way: Electronic Trading Gold award Unisys Client: Office of the Deputy Prime Minister*. The Guardian. 19. Feb. 2004. URL: https://link.gale.com/apps/doc/A113426718/AONE?u=fub&sid=bookmark-AONE&xid=4f437e4c.

[573] *Hi-tech voting machines 'threaten' US polls: Scientist warns that electronic votes cannot be safeguarded*. The Guardian. 16. Feb. 2004. URL: https://link.gale.com/apps/doc/A113308188/AONE?u=fub&sid=bookmark-AONE&xid=e5434e2c.

[574] *Technical hitch in US elections*. The Guardian. 16. Feb. 2004. URL: https://link.gale.com/apps/doc/A113308191/AONE?u=fub&sid=bookmark-AONE&xid=fa1d5e13.

[575] *Why politics has become too clean for comfort: Interview Election Commission chief Sam Younger fears the standards set for public life may be too high*. The Guardian. 12. Feb. 2004. URL: https://link.gale.com/apps/doc/A113214880/AONE?u=fub&sid=bookmark-AONE&xid=0f74c002.

[576] *Online: Feedback: Election nerves*. The Guardian. 29. Jan. 2004. URL: https://link.gale.com/apps/doc/A112689969/AONE?u=fub&sid=bookmark-AONE&xid=e58e0959.

[577] *EPublic: E-voting: Digital ballot gets government's vote: Citizens may one day be free to vote anywhere in the country thanks to the introduction of a standardised electronic register. SA Mathieson reports on the move away from the paper ballot*. The Guardian. 28. Jan. 2004. URL: https://link.gale.com/apps/doc/A112649895/AONE?u=fub&sid=bookmark-AONE&xid=78891b0b.

[578] *Life: Online: Inside IT: News*. The Guardian. 22. Jan. 2004. URL: https://link.gale.com/apps/doc/A112445235/AONE?u=fub&sid=bookmark-AONE&xid=1dbfc878.

[579] *G2: When it comes to Pop Idol, the young love to vote (Michelle got mine). So why wont they turn out for politicians: Just 70 Joan Bakewell*. The Guardian. 12. Dez. 2003. URL: https://link.gale.com/apps/doc/A111191991/AONE?u=fub&sid=bookmark-AONE&xid=56244e52.

[580] *Life: Inside IT: News: E voting doubts*. The Guardian. 11. Dez. 2003. URL: https://link.gale.com/apps/doc/A111150216/AONE?u=fub&sid=bookmark-AONE&xid=efcf6e07.

[581] *Epublic : Interview: Speaking with authority: In his first interview since he took up the post of minister for local government and e-government, Phil Hope talks to Michael Cross about getting councils to reach the 2005 deadline*. The Guardian. 10. Dez. 2003. URL: https://link.gale.com/apps/doc/A111150178/AONE?u=fub&sid=bookmark-AONE&xid=a6aa44f9.

[582] *Epublic : A very flexible friend: Two projects in Southampton and Cornwall are finding a piece of plastic can handle everything from truancy to shopping discounts - and make big admin savings for councils, says SA Mathieson: How to set up a smartcard*. The Guardian. 10. Dez. 2003. URL: https://link.gale.com/apps/doc/A111150180/AONE?u=fub&sid=bookmark-AONE&xid=c2e340f9.

[583] *Ask Jack: Bars to e-voting*. The Guardian. 9. Okt. 2003. URL: https://link.gale.com/apps/doc/A108689188/AONE?u=fub&sid=bookmark-AONE&xid=d9b74439.

[584] *Public Domain*. The Guardian. 9. Okt. 2003. URL: https://link.gale.com/apps/doc/A108689185/AONE?u=fub&sid=bookmark-AONE&xid=44727e4a.

[585] *Opinion: Local Government is failing to engage the public, writes Peter Hetherington*. The Guardian. 8. Okt. 2003. URL: https://link.gale.com/apps/doc/A108642199/AONE?u=fub&sid=bookmark-AONE&xid=4dc0228c.

[586] *Society: epublic: How to make those mobiles count: Did you know that 56 million text messages are being sent every day in the UK? The government wants to capitalise on the nation's increasingly preferred method of communcation to keep public services connected. Dan Jellinek reports*. The Guardian. 8. Okt. 2003. URL: https://link.gale.com/apps/doc/A108689074/AONE?u=fub&sid=bookmark-AONE&xid=47616cc9.

[587] *Letter: How to remake our democracy*. The Guardian. 26. Sep. 2003. URL: https://link.gale.com/apps/doc/A108198805/AONE?u=fub&sid=bookmark-AONE&xid=de6cad0d.

[588] *Last post for the ballot box*. The Guardian. 19. Sep. 2003. URL: https://link.gale.com/apps/doc/A107937067/AONE?u=fub&sid=bookmark-AONE&xid=d365e24d.

[589] *Online : Public Domain*. The Guardian. 18. Sep. 2003. URL: https://link.gale.com/apps/doc/A107903221/AONE?u=fub&sid=bookmark-AONE&xid=b1b04de7.

[590] *Online: Get in touch with Tony: Downing Street has finally granted the general public access to the prime minister's email address, but is he ready for the onslaught of heated opinions and the inevitable spam? Avi Silverman reports*. The Guardian. 21. Aug. 2003. URL: https://link.gale.com/apps/doc/A106761527/AONE?u=fub&sid=bookmark-AONE&xid=4ad26d3a.

[591] *Online: Inside IT: Public Domain*. The Guardian. 7. Aug. 2003. URL: https://link.gale.com/apps/doc/A106395499/AONE?u=fub&sid=bookmark-AONE&xid=5addebda.

[592] *Jobs &; Money: Security: Dating or voting -take your keypad along too*. The Guardian. 2. Aug. 2003. URL: https://link.gale.com/apps/doc/A106195475/AONE?u=fub&sid=bookmark-AONE&xid=7d0e5406.

[593] *Online: Inside IT: Consultancy pins e-voting hopes on UK: But the jury is still out on whether that option increases turnout. Michael Cross reports*. The Guardian. 10. Juli 2003. URL: https://link.gale.com/apps/doc/A105076328/AONE?u=fub&sid=bookmark-AONE&xid=1d20984d.

[594] *Online: Inside IT: News*. The Guardian. 3. Juli 2003. URL: https://link.gale.com/apps/doc/A104653632/AONE?u=fub&sid=bookmark-AONE&xid=e8d67538.

[595] *Online: Inside IT: News*. The Guardian. 26. Juni 2003. URL: https://link.gale.com/apps/doc/A104369280/AONE?u=fub&sid=bookmark-AONE&xid=20989b19.

[596] *Education: Resources: Key stage 3 Age 11-14: Political lessons from Big Brother:* The Guardian. 17. Juni 2003. URL: https://link.gale.com/apps/doc/A103658889/AONE?u=fub&sid=bookmark-AONE&xid=575b1ad2.

[597] *Media: New Media: Big Brother's message to the government*. The Guardian. 2. Juni 2003. URL: https://link.gale.com/apps/doc/A102670587/AONE?u=fub&sid=bookmark-AONE&xid=a4d97c27.

[598] *Inside IT: Beat the town hall clock: Councils are being swamped by e-initiatives dished out from Whitehall. Justin Hunt asks how they will cope*. The Guardian. 29. Mai 2003. URL: https://link.gale.com/apps/doc/A102531791/AONE?u=fub&sid=bookmark-AONE&xid=2413c79d.

[599] *Weekend: E-VOTE EARLY, VOTE OFTEN*. The Guardian. 10. Mai 2003. URL: https://link.gale.com/apps/doc/A101522458/AONE?u=fub&sid=bookmark-AONE&xid=dd6d73d6.

[600] *Life: Inside IT: News*. The Guardian. 8. Mai 2003. URL: https://link.gale.com/apps/doc/A101430400/AONE?u=fub&sid=bookmark-AONE&xid=bb86d406.

[601] *Society: readers' letters*. The Guardian. 7. Mai 2003. URL: https://link.gale.com/apps/doc/A101358044/AONE?u=fub&sid=bookmark-AONE&xid=05bd2dad.

[602] *Elections: Turnout: Big boost from postal voting*. The Guardian. 3. Mai 2003. URL: https://link.gale.com/apps/doc/A101089458/AONE?u=fub&sid=bookmark-AONE&xid=588d817e.

[603] *Local elections: The ones to watch out for*. The Guardian. 1. Mai 2003. URL: https://link.gale.com/apps/doc/A100975733/AONE?u=fub&sid=bookmark-AONE&xid=5925615f.

[604] *Office Hours: Wired up to electoral ballot: Mabel Msonthi asks the returning officer in charge of Norwich's e-voting system how his job has changed*. The Guardian. 28. Apr. 2003. URL: https://link.gale.com/apps/doc/A100753541/AONE?u=fub&sid=bookmark-AONE&xid=553eb036.

[605] *Inside IT: Public Domain*. The Guardian. 24. Apr. 2003. URL: https://link.gale.com/apps/doc/A100549872/AONE?u=fub&sid=bookmark-AONE&xid=bb11cc3e.

[606] *Online: Public domain: Unpopular touch: The first professor of e-democracy wants to improve the UKs poor attempts at consultation*. The Guardian. 27. Feb. 2003. URL: https://link.gale.com/apps/doc/A98144756/AONE?u=fub&sid=bookmark-AONE&xid=833c37c2.

[607] *Comment & Analysis: Paranoid party rights: Engel in America*. The Guardian. 12. Feb. 2003. URL: https://link.gale.com/apps/doc/A105832431/AONE?u=fub&sid=bookmark-AONE&xid=5b9f3107.

[608] *In brief*. The Guardian. 24. Jan. 2003. URL: https://link.gale.com/apps/doc/A96823394/AONE?u=fub&sid=bookmark-AONE&xid=32fab0ba.

[609] *Online: Feedback: Vote and click*. The Guardian. 12. Dez. 2002. URL: https://link.gale.com/apps/doc/A95264199/AONE?u=fub&sid=bookmark-AONE&xid=79c317b7.

[610] *Online: Life in the slow lane: Whitehall has ordered councils to ramp up their IT services*. The Guardian. 5. Dez. 2002. URL: https://link.gale.com/apps/doc/A94985545/AONE?u=fub&sid=bookmark-AONE&xid=c3d3a0d6.

[611] *Letters: Rock of democratic choice*. The Guardian. 5. Nov. 2002. URL: https://link.gale.com/apps/doc/A93975209/AONE?u=fub&sid=bookmark-AONE&xid=9e5bcefc.

[612] *Letter: Rebuild parliament from scratch*. The Guardian. 31. Okt. 2002. URL: https://link.gale.com/apps/doc/A93755874/AONE?u=fub&sid=bookmark-AONE&xid=8962f233.

[613] *Don't trust computers with e-votes, warns expert*. The Guardian. 17. Okt. 2002. URL: https://link.gale.com/apps/doc/A92937468/AONE?u=fub&sid=bookmark-AONE&xid=92c59779.

[614] *Comment & Analysis: Letters: Bullets and ballot-rigging*. The Guardian. 27. Sep. 2002. URL: https://link.gale.com/apps/doc/A92132285/AONE?u=fub&sid=bookmark-AONE&xid=1994bf58.

[615] *Society: Vote early: Middlesbrough has the first elected youth mayor and other cities have set up youth parliaments. But will this encourage more young people to get involved in public service and, even if they do, will it make a difference? Alex Klaushofer reports*. The Guardian. 28. Aug. 2002. URL: https://link.gale.com/apps/doc/A90820241/AONE?u=fub&sid=bookmark-AONE&xid=14931fb9.

[616] *Sceptical voters may be allowed to vote for no one*. The Guardian. 13. Aug. 2002. URL: https://link.gale.com/apps/doc/A90330258/AONE?u=fub&sid=bookmark-AONE&xid=3283c630.

[617] *Leading article: Electrifying elections: Changing the way the country abstains*. The Guardian. 5. Aug. 2002. URL: https://link.gale.com/apps/doc/A90096312/AONE?u=fub&sid=bookmark-AONE&xid=072e5d81.

[618] *Blair told not to rush voting online*. The Guardian. 2. Aug. 2002. URL: https://link.gale.com/apps/doc/A91057039/AONE?u=fub&sid=bookmark-AONE&xid=9133b620.

[619] *Spending review: E-votes will push out ballot box 'from 2006'*. The Guardian. 17. Juli 2002. URL: https://link.gale.com/apps/doc/A89144372/AONE?u=fub&sid=bookmark-AONE&xid=50cf8aba.

[620] *Identity card debate: Used in Europe since the last century*. The Guardian. 4. Juli 2002. URL: https://link.gale.com/apps/doc/A88314342/AONE?u=fub&sid=bookmark-AONE&xid=5694820b.

[621] *Education: Key stage 4: Age 14-16: The story in statistics: Local elections*. The Guardian. 14. Mai 2002. URL: https://link.gale.com/apps/doc/A85924606/AONE?u=fub&sid=bookmark-AONE&xid=47f4ab83.

[622] *Comment &; Analysis: Today it's the non-voters who have logic on their side: The government must give money and power back to local councils*. The Guardian. 2. Mai 2002. URL: https://link.gale.com/apps/doc/A85373423/AONE?u=fub&sid=bookmark-AONE&xid=5da58381.

[623] *Labour prepares for tough fight*. The Guardian. 12. Apr. 2002. URL: https://link.gale.com/apps/doc/A84734065/AONE?u=fub&sid=bookmark-AONE&xid=9977ffd2.

[624] *Phone voting 'will entice young'*. The Guardian. 10. Apr. 2002. URL: https://link.gale.com/apps/doc/A84642592/AONE?u=fub&sid=bookmark-AONE&xid=0993602c.

[625] *Comment &; Analysis: Leader: Digital democracy: It has a role but it can't replace elections*. The Guardian. 22. Feb. 2002. URL: https://link.gale.com/apps/doc/A83145548/AONE?u=fub&sid=bookmark-AONE&xid=0a67f7c4.

[626] *Comment &; Analysis: Bring back our tribes: Politicians fret that the young aren't interested. But without ideology, politics is for anoraks*. The Guardian. 5. Feb. 2002. URL: https://link.gale.com/apps/doc/A82523462/AONE?u=fub&sid=bookmark-AONE&xid=5ddcda9b.

[627] *Letter: A low poll for internet voting*. The Guardian. 8. Jan. 2002. URL: https://link.gale.com/apps/doc/A81522405/AONE?u=fub&sid=bookmark-AONE&xid=40333ea8.

[628] *Media: MP.com: A new website offers streaming video coverage of parliament. But will anyone actually use it, wonders Owen Gibson*. The Guardian. 7. Jan. 2002. URL: https://link.gale.com/apps/doc/A81479658/AONE?u=fub&sid=bookmark-AONE&xid=b8011fce.

[629] *Comment &; Analysis: Rise of the non-voter: There is another group leading parallel lives in Britain - and they really do threaten our democracy*. The Guardian. 12. Dez. 2001. URL: https://link.gale.com/apps/doc/A80750866/AONE?u=fub&sid=bookmark-AONE&xid=0e2e9946.

[630] *Internet voting planned to get better turnouts*. The Guardian. 23. Nov. 2001. URL: https://link.gale.com/apps/doc/A80256541/AONE?u=fub&sid=bookmark-AONE&xid=ba55a574.

[631] *Hi-tech voting aims to raise turnout*. The Guardian. 23. Nov. 2001. URL: https://link.gale.com/apps/doc/A80256542/AONE?u=fub&sid=bookmark-AONE&xid=b5444e91.

[632] *In brief: Trial for new ways to vote*. The Guardian. 5. Okt. 2001. URL: https://link.gale.com/apps/doc/A78916325/AONE?u=fub&sid=bookmark-AONE&xid=9b7fedef.

[633] *Florida recount chief seeks a safe seat in Congress*. The Guardian. 4. Okt. 2001. URL: https://link.gale.com/apps/doc/A78889174/AONE?u=fub&sid=bookmark-AONE&xid=24ca1da3.

[634] *Online: WORKING IT OUT: CHARLES KENNEDY: Charles Kennedy is the leader of the Liberal Democrats and MP for Ross, Sky and Inverness West*. The Guardian. 26. Juli 2001. URL: https://link.gale.com/apps/doc/A76771858/AONE?u=fub&sid=bookmark-AONE&xid=70726992.

[635] *Leading article: Voting in view: When parties fail, we need scrutineers*. The Guardian. 25. Juli 2001. URL: https://link.gale.com/apps/doc/A76750171/AONE?u=fub&sid=bookmark-AONE&xid=11ecf2db.

[636] *Online: Second sight*. The Guardian. 5. Juli 2001. URL: https://link.gale.com/apps/doc/A76282144/AONE?u=fub&sid=bookmark-AONE&xid=bcac6308.

[637] *Online: Feedback: E-vote of no confidence*. The Guardian. 14. Juni 2001. URL: https://link.gale.com/apps/doc/A75520251/AONE?u=fub&sid=bookmark-AONE&xid=5e9d8b10.

[638] *New Media: Thatcher's mothership: a wasted chance*. The Guardian. 11. Juni 2001. URL: https://link.gale.com/apps/doc/A75432338/AONE?u=fub&sid=bookmark-AONE&xid=8f9c72fb.

[639] *Education: Further: The winner by, er, how much?: Election counters wanted: numeracy not essential . . . John Crace applies*. The Guardian. 29. Mai 2001. URL: https://link.gale.com/apps/doc/A75084526/AONE?u=fub&sid=bookmark-AONE&xid=629aa9fa.

[640] *Society: Poll position: Election day check on access for disabled*. The Guardian. 16. Mai 2001. URL: https://link.gale.com/apps/doc/A74568206/AONE?u=fub&sid=bookmark-AONE&xid=9fb2612d.

[641] *City 'mishandled exercise in local democracy': Voters opt for school cuts over tax rise prompting fears of teacher strike action*. The Guardian. 16. Feb. 2001. URL: https://link.gale.com/apps/doc/A71415798/AONE?u=fub&sid=bookmark-AONE&xid=99bb2448.

[642] *Online: Second sight*. The Guardian. 30. Nov. 2000. URL: https://link.gale.com/apps/doc/A75684318/AONE?u=fub&sid=bookmark-AONE&xid=10c99126.

[643] *Leading article: Sweep out the stables: The Commons needs radical change*. The Guardian. 26. Okt. 2000. URL: https://link.gale.com/apps/doc/A75687734/AONE?u=fub&sid=bookmark-AONE&xid=a936baae.

[644] *National Roundup: In-store poll booths fail to lift voting*. The Guardian. 17. Aug. 2000. URL: https://link.gale.com/apps/doc/A75727017/AONE?u=fub&sid=bookmark-AONE&xid=141ab369.

[645] *Towards a second term: Road to the manifesto: Labour's vital mission to carry on reforming*. The Guardian. 7. Aug. 2000. URL: https://link.gale.com/apps/doc/A75735379/AONE?u=fub&sid=bookmark-AONE&xid=63be3500.

[646] *CORRECTED: Comment &; Analysis: Analysis: Making it easy: Experiments to improve the turnout in local elections have had an impact, although some voters still want to use a polling station*. The Guardian. 15. Mai 2000. URL: https://link.gale.com/apps/doc/A75767956/AONE?u=fub&sid=bookmark-AONE&xid=c485b7f1.

[647] *Election special: Tories back on the map after heartland wins: Local polls: Symbolic successes as Torbay, Eastbourne and Solihull are recaptured*. The Guardian. 5. Mai 2000. URL: https://link.gale.com/apps/doc/A75765909/AONE?u=fub&sid=bookmark-AONE&xid=fa19c6fb.

[648] *Online:Feedback: Online letter: Secret's out*. The Guardian. 4. Mai 2000. URL: https://link.gale.com/apps/doc/A75775544/AONE?u=fub&sid=bookmark-AONE&xid=9e6f900b.

[649] *Online:Feedback: Online letter:Secreat's Out*. The Guardian. 4. Mai 2000. URL: https://link.gale.com/apps/doc/A75775545/AONE?u=fub&sid=bookmark-AONE&xid=0adb3b37.

[650] *Click the vote: Is there anything behind the government's bluster about e-government? asks Patrick Barkham*. The Guardian. 27. Apr. 2000. URL: https://link.gale.com/apps/doc/A75774331/AONE?u=fub&sid=bookmark-AONE&xid=ca0deaaa.

[651] *Sketch: A lot of Community Rehabilitation And Protection*. The Guardian. 14. März 2000. URL: https://link.gale.com/apps/doc/A75789249/AONE?u=fub&sid=bookmark-AONE&xid=e484286e.

[652] *In brief: Council polls go electronic*. The Guardian. 17. Feb. 2000. URL: https://link.gale.com/apps/doc/A75794329/AONE?u=fub&sid=bookmark-AONE&xid=0d6cfe22.

[653] *Comment &; Analysis: The internet will take over politics in good or bad ways: Arizona's Democratic party primary points the way to the future*. The Guardian. 6. Jan. 2000. URL: https://link.gale.com/apps/doc/A75795671/AONE?u=fub&sid=bookmark-AONE&xid=c6a76893.

Rohdaten der QIA der Artikel der *Neuen Zürcher Zeitung*

NZZ	07.05.22 [185]	22.03.22 [186]	05.02.22 [187]	13.01.22 [188]	06.11.21 [189]	05.11.21 [190]	17.09.21 [191]	08.09.21 [192]	29.04.21 [193]	03.04.21 [32]	25.03.21 [194]	23.02.21 [195]	19.02.21 [196]	10.02.21 [102]	08.02.21 [197]	27.01.21 [198]	26.01.21 [199]	14.01.21 [200]	22.12.20 [201]
System entweder sicher oder unsicher														■					
Sicherheit ist relativ								■											■
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers										■									
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme																			
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne																			
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit						■			■										
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung								■						■					
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																			
Verfügbarkeit	■																		
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes						■			■					■	■				■
funktionelle Fehler *(bugs)*															■				
Softwaretests																			
Intrusionstests									■						■				
Softwareinspektion									■						■				
Zertifizierung	■											■		■					
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹	■				■	■	■		■										
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹					■				■						■				
Innentäter																			
Schwachstellen *(exploits)*															■				
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert						■		■	■		■			■					■

NZZ	11.11.20 [202]	27.10.20 [203]	17.10.20 [113]	06.10.20 [204]	25.05.20 [205]	23.05.20 [90]	16.05.20 [206]	04.01.20 [207]	11.11.19 [208]	14.10.19 [209]	09.09.19 [210]	02.09.19 [211]	27.08.19 [212]	06.07.19 [63]	29.06.19 [213]	28.06.19 [59]	20.06.19 [214]	11.05.19 [215]	29.04.19 [216]
System entweder sicher oder unsicher	■																		
Sicherheit ist relativ			■					■								■			
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers			■							■									
Integrität der Stimme									■										
individuelle Verifizierbarkeit			■													■			
Vertraulichkeit der Stimme																			
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne									■										
universelle Verifizierbarkeit														■		■			
vollständige Verifizierbarkeit																■			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung						■										■			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																			
Verfügbarkeit			■																
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)						■													
Veröffentlichung des Quellcodes						■								■		■	■		
funktionelle Fehler *(bugs)*						■													
Softwaretests									■										
Intrusionstests			■			■								■			■		
Softwareinspektion						■													
Zertifizierung						■											■		
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹			■																
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹			■			■								■			■		
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*			■																
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert						■		■	■			■			■	■	■		

NZZ	27.04.19 [97]	09.04.19 [217]	30.03.19 [95]	29.03.19 [218]	27.03.19 [13]	21.03.19 [219]	13.03.19 [61]	06.03.19 [220]	05.03.19 [221]	04.03.19 [222]	26.02.19 [106]	08.02.19 [166]	07.02.19 [223]	28.01.19 [224]	26.01.19 (a) [225]	26.01.19 (b) [226]	24.01.19 [227]	22.12.18 [228]	20.12.18 [229]
System entweder sicher oder unsicher	■		■		■														
Sicherheit ist relativ															■				■
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers																			
Integrität der Stimme											■	■							
individuelle Verifizierbarkeit			■		■														
Vertraulichkeit der Stimme					■						■								■
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne	■		■									■							
universelle Verifizierbarkeit	■				■		■												
vollständige Verifizierbarkeit											■								
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung					■		■				■	■							
digitale Signatur																			
Annahme: REV ist technisch machbar					■														
Ist REV technisch evtl. nicht machbar?	■											■							
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit	■															■			
Verfügbarkeit	■										■								
keine ungültigen Stimmen															■				
Auszählung ohne Fehler															■				
Das Manipulationsrisiko skaliert hoch												■							
Quellcode (ohne Veröffentlichung)					■						■								
Veröffentlichung des Quellcodes	■						■				■	■							■
funktionelle Fehler *(bugs)*					■		■												
Softwaretests																			
Intrusionstests	■		■		■		■				■	■							■
Softwareinspektion			■				■												
Zertifizierung	■		■		■	■	■				■								
Ein Informatiksystem ist eine *Blackbox*									■										
ohne bes. Sachkenntnis nachvollziehbar?		■													■				
›Manipulation‹, ›manipulier…‹	■				■		■				■	■			■	■			
Werden Manipulationen erkannt?					■							■							
›Hacker‹, ›hacken‹, ›gehackt‹	■		■		■		■				■	■			■	■		■	■
Innentäter					■		■												
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*											■								
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf											■								
Konkrete Lücken werden geschildert	■		■		■		■												■

NZZ	08.12.18 [230]	01.12.18 [231]	29.11.18 (a) [232]	29.11.18 (b) [233]	03.11.18 [234]	13.10.18 [235]	15.09.18 [236]	11.08.18 [237]	26.07.18 [77]	25.07.18 [238]	09.07.18 [239]	28.06.18 [240]	16.06.18 [241]	12.06.18 [167]	06.06.18 [242]	19.05.18 [107]	15.05.18 [243]	11.05.18 [118]	03.05.18 [244]
System entweder sicher oder unsicher						■			■					■		■		■	
Sicherheit ist relativ												■		■		■		■	
maßgeblich ist das schwächste Glied														■		■			
Autorisierung des Wählers									■										
Integrität der Stimme									■										■
individuelle Verifizierbarkeit																■		■	
Vertraulichkeit der Stimme				■														■	
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne									■										■
universelle Verifizierbarkeit			■															■	
vollständige Verifizierbarkeit				■		■						■							
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung				■					■							■		■	
digitale Signatur					■														
Annahme: REV ist technisch machbar																		■	
Ist REV technisch evtl. nicht machbar?			■																
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																■			
Verfügbarkeit																			■
keine ungültigen Stimmen												■				■		■	
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch									■					■				■	
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes				■														■	
funktionelle Fehler *(bugs)*																			
Softwaretests			■																
Intrusionstests				■															
Softwareinspektion																			
Zertifizierung				■		■						■			■				
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?						■							■						
›Manipulation‹, ›manipulier…‹			■		■	■			■					■		■		■	
Werden Manipulationen erkannt?					■				■										
›Hacker‹, ›hacken‹, ›gehackt‹			■		■				■							■			
Innentäter																			
Schwachstellen *(exploits)*				■	■														
Hintertüren																		■	
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																		■	
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert	■			■	■				■									■	

NZZ	28.04.18 [245]	18.04.18 [246]	11.04.18 [247]	06.04.18 (a) [248]	06.04.18 (b) [126]	03.03.18 [249]	02.03.18 [117]	27.02.18 [250]	17.02.18 (a) [251]	17.02.18 (b) [252]	13.12.17 [253]	12.12.17 [254]	22.11.17 [255]	04.11.17 [256]	02.10.17 [257]	19.09.17 [258]	22.08.17 [259]	04.08.17 [260]	29.06.17 [261]
System entweder sicher oder unsicher				■	■				■					■					
Sicherheit ist relativ	■			■			■	■	■					■				■	
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers									■										
Integrität der Stimme									■										
individuelle Verifizierbarkeit	■				■														
Vertraulichkeit der Stimme																			
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne					■														
universelle Verifizierbarkeit					■														
vollständige Verifizierbarkeit	■								■	■									
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung	■																		
digitale Signatur																			
Annahme: REV ist technisch machbar	■																		
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen					■														
Bedienbarkeit		■																	
Verfügbarkeit	■																		
keine ungültigen Stimmen		■			■														
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch	■			■	■				■	■									
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes	■								■	■									
funktionelle Fehler *(bugs)*																			
Softwaretests																			
Intrusionstests	■								■	■									
Softwareinspektion																			
Zertifizierung	■						■				■			■					
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?	■				■														
›Manipulation‹, ›manipulier…‹	■	■		■	■	■	■	■	■	■								■	
Werden Manipulationen erkannt?							■												
›Hacker‹, ›hacken‹, ›gehackt‹	■			■	■	■	■	■	■	■								■	
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf				■															
Konkrete Lücken werden geschildert										■									

NZZ	07.06.17 [262]	31.05.17 [263]	24.04.17 [264]	06.04.17 (a) [265]	06.04.17 (b) [266]	17.03.17 [267]	10.03.17 [268]	07.02.17 [269]	07.12.16 [270]	03.12.16 [146]	14.11.16 [271]	11.11.16 (a) [272]	11.11.16 (b) [36]	11.11.16 (c) [273]	06.10.16 [274]	28.09.16 [275]	17.09.16 [276]	31.08.16 [277]	06.08.16 [278]
System entweder sicher oder unsicher										■									
Sicherheit ist relativ				■	■			■		■		■	■	■					
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers	■				■													■	
Integrität der Stimme																			
individuelle Verifizierbarkeit								■											
Vertraulichkeit der Stimme					■			■											
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne													■						
universelle Verifizierbarkeit								■		■									
vollständige Verifizierbarkeit				■	■														
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung					■											■			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																			
Verfügbarkeit																			
keine ungültigen Stimmen								■					■						
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																		■	
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes				■	■	■													
funktionelle Fehler *(bugs)*																			
Softwaretests																			
Intrusionstests														■					
Softwareinspektion																			
Zertifizierung			■											■					
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹				■	■					■			■					■	
Werden Manipulationen erkannt?					■														
›Hacker‹, ›hacken‹, ›gehackt‹								■					■					■	
Innentäter																			
Schwachstellen *(exploits)*																		■	
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert								■										■	

NZZ	07.07.16 [279]	05.07.16 [280]	17.06.16 [281]	14.01.16 [282]	22.12.15 [82]	12.12.15 (a) [283]	12.12.15 (b) [284]	12.12.15 (c) [26]	08.12.15 [285]	16.11.15 [94]	05.11.15 [60]	27.10.15 [286]	22.10.15 [287]	15.10.15 [288]	03.10.15 [289]	01.10.15 [182]	25.09.15 [31]	22.09.15 [58]	17.09.15 [56]
System entweder sicher oder unsicher										■	■					■		■	
Sicherheit ist relativ																	■		■
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers			■																
Integrität der Stimme																			
individuelle Verifizierbarkeit										■	■		■						
Vertraulichkeit der Stimme					■			■			■					■	■	■	
Bruch der Vertraulichkeit der Stimme											■					■			
Integrität der Urne					■					■			■						
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit											■					■			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?											■								
Zielkonflikte bei Schutzzielen										■						■			
Bedienbarkeit											■								
Verfügbarkeit										■									
keine ungültigen Stimmen								■									■		
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch											■								
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes					■					■	■					■			
funktionelle Fehler *(bugs)*																			
Softwaretests					■														
Intrusionstests																			
Softwareinspektion																			
Zertifizierung					■														
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹										■	■					■			■
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹										■	■								
Innentäter																			
Schwachstellen *(exploits)*										■	■								
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*										■									
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert						■											■		■

NZZ	07.09.15 [290]	03.09.15 [291]	20.08.15 [100]	17.08.15 [292]	15.08.15 (b) [144]	15.08.15 (a) [293]	14.08.15 [294]	13.08.15 [55]	12.08.15 [295]	25.07.15 [296]	21.07.15 [297]	30.06.15 [298]	15.06.15 [299]	02.06.15 [300]	27.05.15 [301]	17.04.15 [165]	11.04.15 [302]	27.02.15 [303]	24.01.15 [304]
System entweder sicher oder unsicher				■															
Sicherheit ist relativ		■			■			■											
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers																			■
Integrität der Stimme																			
individuelle Verifizierbarkeit																			■
Vertraulichkeit der Stimme				■						■									
Bruch der Vertraulichkeit der Stimme								■											
Integrität der Urne																			
universelle Verifizierbarkeit					■														
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																			
Verfügbarkeit																			
keine ungültigen Stimmen																	■		
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes		■	■		■			■											
funktionelle Fehler *(bugs)*										■									
Softwaretests																			
Intrusionstests																			
Softwareinspektion								■											
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹						■				■						■	■		
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹		■						■						■					
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert					■			■											

NZZ	18.12.14 [62]	11.09.14 [305]	29.08.14 [306]	15.08.14 [125]	29.07.14 [307]	28.06.14 [308]	08.05.14 [309]	17.03.14 [310]	27.02.14 [311]	23.01.14 [99]	14.12.13 (a) [312]	14.12.13 (b) [313]	11.12.13 [314]	30.11.13 [315]	19.11.13 [41]	24.10.13 [316]	14.10.13 [317]	02.10.13 [318]	17.09.13 [319]
System entweder sicher oder unsicher										■					■				
Sicherheit ist relativ	■														■				
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers																	■		
Integrität der Stimme											■								
individuelle Verifizierbarkeit									■						■				■
Vertraulichkeit der Stimme					■		■												■
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne	■																		
universelle Verifizierbarkeit	■			■					■						■				
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar					■														■
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen															■				
Bedienbarkeit															■				
Verfügbarkeit																			■
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch															■				
Quellcode (ohne Veröffentlichung)															■				
Veröffentlichung des Quellcodes								■		■					■				
funktionelle Fehler *(bugs)*								■											
Softwaretests																			
Intrusionstests								■											
Softwareinspektion															■				
Zertifizierung	■											■							
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?					■														
›Manipulation‹, ›manipulier…‹	■				■		■		■			■		■	■				■
Werden Manipulationen erkannt?															■				■
›Hacker‹, ›hacken‹, ›gehackt‹				■	■			■	■			■			■				■
Innentäter																			■
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*											■								■
Ausspähen von Informationen *(phishing)*																			■
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert								■	■		■				■				■

NZZ	30.08.13 [320]	22.08.13 [12]	20.08.13 [121]	15.08.13 [122]	03.05.13 [321]	06.04.13 [322]	08.01.13 [323]	24.10.12 [324]	09.10.12 [325]	31.08.12 [326]	28.06.12 [327]	22.05.12 [328]	06.01.12 [329]	28.12.11 [330]	21.12.11 [331]	26.11.11 [332]	02.11.11 [333]	29.10.11 [334]	29.08.11 [335]
System entweder sicher oder unsicher																			
Sicherheit ist relativ			■																
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers												■		■		■			
Integrität der Stimme																			
individuelle Verifizierbarkeit			■	■															
Vertraulichkeit der Stimme																			
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne	■																		
universelle Verifizierbarkeit			■																
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen			■																
Bedienbarkeit																			
Verfügbarkeit				■															
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch				■															
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*																			
Softwaretests																			
Intrusionstests				■															
Softwareinspektion																			
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹	■		■	■															
Werden Manipulationen erkannt?				■															
›Hacker‹, ›hacken‹, ›gehackt‹				■				■											
Innentäter				■															
Schwachstellen *(exploits)*				■															
Hintertüren				■															
Schadsoftware *(malware)*				■															
Ausspähen von Informationen *(phishing)*				■															
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf			■																
Konkrete Lücken werden geschildert				■															

NZZ	23.06.11 [336]	11.06.11 [337]	17.05.11 [8]	16.05.11 [338]	02.05.11 [98]	29.03.11 [339]	28.03.11 [340]	08.03.11 (a) [341]	08.03.11 (b) [342]	06.12.10 [343]	03.11.10 [344]	09.09.10 [345]	07.09.10 [346]	20.08.10 [347]	26.04.10 [348]	26.02.10 [349]	24.11.09 [350]	27.10.09 [351]	05.09.09 [352]
System entweder sicher oder unsicher																			
Sicherheit ist relativ					■														
maßgeblich ist das schwächste Glied													■						
Autorisierung des Wählers							■												
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme																			
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne																			
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs					■								■						
Zusammenwirken Mehrerer erforderlich													■						
Verschlüsselung					■														
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																			
Verfügbarkeit									■										
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch					■														
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*																			
Softwaretests													■			■			
Intrusionstests													■						
Softwareinspektion																			
Zertifizierung					■														
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹			■		■														
Werden Manipulationen erkannt?					■														
›Hacker‹, ›hacken‹, ›gehackt‹													■						
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren					■														
Schadsoftware *(malware)*													■						
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert									■	■									

NZZ	10.08.09 [353]	16.06.09 [354]	27.03.09 [355]	10.02.09 [356]	09.02.09 [357]	05.02.09 [358]	28.11.08 [359]	28.08.08 [360]	28.05.08 [361]	17.12.07 [362]	01.12.07 [363]	08.11.07 [364]	07.11.07 [365]	15.10.07 [366]	18.08.07 [367]	06.08.07 [368]	04.08.07 [369]	18.06.07 [370]	24.05.07 [371]
System entweder sicher oder unsicher																			
Sicherheit ist relativ	■					■													
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers	■										■					■		■	
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme																			
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne																			
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar					■														
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																			
Verfügbarkeit																			
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*																			
Softwaretests																			
Intrusionstests																			
Softwareinspektion																			
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier...‹																			
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹																			
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert																			

NZZ	25.04.07 [372]	02.04.07 [373]	03.03.07 [374]	15.12.06 [375]	05.12.06 (a) [376]	05.12.06 (b) [377]	01.11.06 [378]	14.09.06 [379]	31.08.06 [380]	24.07.06 [381]	01.06.06 [382]	29.04.06 [383]	11.04.06 [384]	03.04.06 (a) [385]	03.04.06 (b) [386]	30.03.06 [83]	13.02.06 [387]	19.12.05 [388]	28.11.05 (a) [389]
System entweder sicher oder unsicher																			
Sicherheit ist relativ																			
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers		■																	
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme	■											■							
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne	■																		
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs	■																		
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																■			
Verfügbarkeit																			
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*																			
Softwaretests																			
Intrusionstests																			
Softwareinspektion																			
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹												■							
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹	■																		
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert	■																		

NZZ	28.11.05 (b) [390]	31.10.05 [391]	15.10.05 [392]	12.10.05 [181]	11.10.05 [393]	16.09.05 [394]	09.09.05 [395]	11.08.05 [396]	12.07.05 (a) [397]	12.07.05 (b) [398]	09.07.05 [399]	26.04.05 [400]	22.04.05 [401]	22.03.05 [402]	15.02.05 [403]	06.01.05 [404]	03.01.05 [405]	15.12.04 [406]	20.11.04 [407]
System entweder sicher oder unsicher																			
Sicherheit ist relativ																■			
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers		■		■		■							■					■	■
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme						■										■			
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne				■															
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit			■			■												■	
Verfügbarkeit						■													
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*				■															
Softwaretests													■						
Intrusionstests																			
Softwareinspektion																			
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹																			
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹																			
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert																			

NZZ	16.11.04 [408]	12.11.04 [409]	11.11.04 [410]	02.10.04 [411]	27.09.04 [39]	23.09.04 [412]	15.09.04 [413]	11.09.04 [414]	27.08.04 [415]	12.03.04 [416]	16.01.04 [417]	07.11.03 [418]	31.10.03 [419]	11.10.03 [420]	06.10.03 [421]	23.09.03 (a) [422]	23.09.03 (b) [423]	10.06.03 [424]	19.05.03 [425]
System entweder sicher oder unsicher																			
Sicherheit ist relativ		■																	
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers		■					■		■								■		
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme		■																	
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne																			
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung					■														
digitale Signatur		■																	
Annahme: REV ist technisch machbar							■												
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																			
Verfügbarkeit																			
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*																			
Softwaretests		■																	
Intrusionstests																			
Softwareinspektion																			
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹		■					■		■										
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹																			
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert																	■		

NZZ	08.04.03 [426]	04.02.03 [88]	20.01.03 [38]	02.10.02 [427]	16.08.02 [428]	02.07.02 [429]	27.05.02 [430]	15.05.02 (a) [431]	15.05.02 (b) [432]	15.05.02 (c) [433]	15.05.02 (d) [434]	04.05.02 [435]	20.03.02 (a) [436]	20.03.02 (b) [437]	15.02.02 [438]	10.01.02 [439]	01.12.01 [440]	22.06.01 [441]	19.06.01 [442]
System entweder sicher oder unsicher																			
Sicherheit ist relativ							■											■	
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers		■				■	■	■		■						■	■	■	
Integrität der Stimme		■																	
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme		■					■	■		■							■		
Bruch der Vertraulichkeit der Stimme																■			
Integrität der Urne			■					■		■							■		
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich			■																
Verschlüsselung		■																	
digitale Signatur		■																■	
Annahme: REV ist technisch machbar																■			
Ist REV technisch evtl. nicht machbar?		■																	
Zielkonflikte bei Schutzzielen							■												
Bedienbarkeit																			
Verfügbarkeit																■			
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*																			
Softwaretests																			
Intrusionstests																			
Softwareinspektion																			
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹	■	■							■							■			
Werden Manipulationen erkannt?		■																	
›Hacker‹, ›hacken‹, ›gehackt‹																			
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*		■																	
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert																			

NZZ	08.06.01 [443]	16.05.01 [444]	06.04.01 [445]	26.03.01 [138]	23.03.01 [446]	21.02.01 [447]	19.01.01 [448]	13.01.01 (a) [449]	13.01.01 (b) [450]	13.01.01 (c) [10]	15.12.00 [451]	28.09.00 [452]	26.09.00 (a) [453]	26.09.00 (b) [454]	21.08.00 [455]	11.07.00 [456]
System entweder sicher oder unsicher																
Sicherheit ist relativ																
maßgeblich ist das schwächste Glied																
Autorisierung des Wählers	■													■		
Integrität der Stimme														■		
individuelle Verifizierbarkeit																
Vertraulichkeit der Stimme								■						■		
Bruch der Vertraulichkeit der Stimme																
Integrität der Urne								■								
universelle Verifizierbarkeit																
vollständige Verifizierbarkeit																
physischer Schutz der Server																
Autorisierung des Zugriffs																
Zusammenwirken Mehrerer erforderlich																
Verschlüsselung														■		
digitale Signatur				■				■		■				■		■
Annahme: REV ist technisch machbar										■						
Ist REV technisch evtl. nicht machbar?																
Zielkonflikte bei Schutzzielen																
Bedienbarkeit																
Verfügbarkeit																
keine ungültigen Stimmen																
Auszählung ohne Fehler																
Das Manipulationsrisiko skaliert hoch										■						
Quellcode (ohne Veröffentlichung)																
Veröffentlichung des Quellcodes																
funktionelle Fehler *(bugs)*																
Softwaretests																
Intrusionstests																
Softwareinspektion																
Zertifizierung																■
Ein Informatiksystem ist eine *Blackbox*																
ohne bes. Sachkenntnis nachvollziehbar?																
›Manipulation‹, ›manipulier…‹													■			
Werden Manipulationen erkannt?																
›Hacker‹, ›hacken‹, ›gehackt‹																
Innentäter																
Schwachstellen *(exploits)*																
Hintertüren																
Schadsoftware *(malware)*														■		
Ausspähen von Informationen *(phishing)*														■		
trojanische Pferde																
Sicherheit ist ein ständiger Wettlauf																
Konkrete Lücken werden geschildert																

Rohdaten der QIA der Artikel des *Guardian*

The Guardian	05.05.22 [457]	13.01.22 [458]	16.12.21 [459]	11.12.21 [460]	29.10.21 [461]	08.09.21 [462]	29.08.21 [463]	16.07.21 [464]	18.06.21 [465]	17.01.21 [466]	21.06.20 [467]	29.03.20 [468]	13.03.20 [469]	02.01.20 [470]	27.08.19 [471]	08.04.19 [115]	30.12.18 [472]	05.12.18 [473]	08.10.18 [474]
System entweder sicher oder unsicher														■					
Sicherheit ist relativ														■		■			
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers		■												■	■	■		■	
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme																			
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne														■	■	■			
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server		■														■			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																	■		
Verfügbarkeit														■			■		
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*																			
Softwaretests																			
Intrusionstests																■			
Softwareinspektion																			
Zertifizierung														■					
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹		■			■		■												
Werden Manipulationen erkannt?															■				
›Hacker‹, ›hacken‹, ›gehackt‹														■	■	■			
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*															■	■			
Ausspähen von Informationen *(phishing)*															■				
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf														■					
Konkrete Lücken werden geschildert														■	■				

The Guardian	26.04.18 [475]	28.01.18 [476]	09.12.17 [477]	23.07.17 [478]	18.05.17 [479]	14.04.17 [154]	05.01.17 [11]	10.12.16 [480]	24.11.16 [481]	23.11.16 [482]	06.08.16 [20]	11.07.16 [483]	10.07.16 [484]	23.04.16 [485]	11.01.16 [486]	09.12.15 [487]	16.10.15 [488]	04.10.15 (a) [489]	04.10.15 (b) [490]
System entweder sicher oder unsicher																			
Sicherheit ist relativ															■				
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers						■						■							
Integrität der Stimme														■					
individuelle Verifizierbarkeit						■													
Vertraulichkeit der Stimme						■						■		■					
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne						■				■									
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server											■					■			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung							■												
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit												■							
Verfügbarkeit				■															
keine ungültigen Stimmen																			
Auszählung ohne Fehler						■													
Das Manipulationsrisiko skaliert hoch	■					■	■												
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*																			
Softwaretests																			
Intrusionstests																			
Softwareinspektion																			
Zertifizierung														■					
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹	■						■	■	■		■							■	
Werden Manipulationen erkannt?							■			■									
›Hacker‹, ›hacken‹, ›gehackt‹						■	■	■	■	■	■		■						
Innentäter											■								
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*														■					
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert													■						

The Guardian	18.08.15 [491]	11.08.15 [492]	20.04.15 [493]	15.04.15 [494]	01.04.15 [495]	30.03.15 [87]	23.03.15 [149]	18.03.15 [496]	26.02.15 [37]	21.01.15 [183]	05.09.14 [497]	13.05.14 [498]	27.03.14 [499]	27.12.13 [500]	28.11.13 [501]	09.09.13 [502]	11.03.13 [503]	08.10.12 [180]	26.11.11 [504]
System entweder sicher oder unsicher						■			■									■	
Sicherheit ist relativ						■			■										
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers			■	■		■			■				■					■	
Integrität der Stimme									■										
individuelle Verifizierbarkeit						■													
Vertraulichkeit der Stimme						■			■	■									
Bruch der Vertraulichkeit der Stimme										■								■	
Integrität der Urne						■	■		■							■			
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung							■		■										
digitale Signatur						■			■										
Annahme: REV ist technisch machbar					■														
Ist REV technisch evtl. nicht machbar?						■													
Zielkonflikte bei Schutzzielen						■			■										
Bedienbarkeit								■											
Verfügbarkeit						■		■									■		
keine ungültigen Stimmen								■											
Auszählung ohne Fehler									■										
Das Manipulationsrisiko skaliert hoch						■			■	■									
Quellcode (ohne Veröffentlichung)							■												
Veröffentlichung des Quellcodes									■										
funktionelle Fehler *(bugs)*									■										
Softwaretests																			
Intrusionstests																			
Softwareinspektion									■										
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?						■													
›Manipulation‹, ›manipulier…‹						■	■		■								■		
Werden Manipulationen erkannt?						■	■												
›Hacker‹, ›hacken‹, ›gehackt‹						■	■											■	
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*						■	■		■										
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert						■	■												

The Guardian	16.04.11 [505]	01.03.11 [506]	08.10.10 [507]	28.07.10 [508]	22.04.10 [509]	09.12.09 [510]	23.10.09 [511]	01.10.09 [512]	30.04.09 [84]	17.04.09 [513]	16.04.09 [514]	20.11.08 [515]	13.11.08 [516]	22.10.08 [21]	26.09.08 [517]	29.11.07 [518]	24.10.07 [519]	02.08.07 [520]	04.07.07 [521]
System entweder sicher oder unsicher																			
Sicherheit ist relativ																		■	
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers			■											■					
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme																			
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne								■											
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server										■									
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit									■								■	■	
Verfügbarkeit								■							■		■	■	
keine ungültigen Stimmen																	■		
Auszählung ohne Fehler								■											
Das Manipulationsrisiko skaliert hoch									■										
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*								■	■										
Softwaretests								■	■									■	
Intrusionstests																			
Softwareinspektion																			
Zertifizierung									■										
Ein Informatiksystem ist eine *Blackbox*									■										
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹							■						■						
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹									■										
Innentäter									■										
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde									■										
Sicherheit ist ein ständiger Wettlauf									■										
Konkrete Lücken werden geschildert																			

The Guardian	30.05.07 [522]	05.05.07 [523]	03.05.07 [101]	30.04.07 [524]	21.04.07 [525]	14.04.07 [526]	10.02.07 [527]	09.11.06 (a) [528]	09.11.06 (b) [529]	08.11.06 (a) [530]	08.11.06 (b) [531]	08.11.06 (c) [532]	03.11.06 [533]	28.10.06 [534]	27.10.06 [535]	17.08.06 [536]	22.02.06 [537]	23.11.05 (a) [538]	23.11.05 (b) [539]
System entweder sicher oder unsicher																			
Sicherheit ist relativ							■												
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers													■		■	■		■	■
Integrität der Stimme			■									■							
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme																			■
Bruch der Vertraulichkeit der Stimme				■															
Integrität der Urne			■										■		■				
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																■			
Annahme: REV ist technisch machbar																■			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit											■				■			■	
Verfügbarkeit		■	■								■	■	■		■				
keine ungültigen Stimmen											■								
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch			■																
Quellcode (ohne Veröffentlichung)											■								
Veröffentlichung des Quellcodes			■																
funktionelle Fehler *(bugs)*										■	■	■			■				
Softwaretests			■																
Intrusionstests																			
Softwareinspektion																			
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*			■																
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹			■	■					■			■	■		■	■		■	
Werden Manipulationen erkannt?													■						
›Hacker‹, ›hacken‹, ›gehackt‹			■			■							■	■	■				
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*							■						■		■				
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde			■																
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert			■										■						■

The Guardian	23.11.05 (c) [540]	26.10.05 (a) [541]	26.10.05 (b) [542]	26.10.05 (c) [543]	07.09.05 [544]	02.06.05 [545]	20.04.05 [546]	07.04.05 [547]	24.03.05 [548]	10.03.05 [549]	23.02.05 [550]	02.02.05 [91]	01.12.04 [551]	12.11.04 [552]	11.11.04 [553]	03.11.04 [554]	20.10.04 [555]	19.10.04 [147]	18.10.04 [556]
System entweder sicher oder unsicher								■	■			■							
Sicherheit ist relativ								■											
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers	■	■					■				■						■	■	■
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme							■	■											
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne														■		■			■
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen								■											
Bedienbarkeit							■									■		■	
Verfügbarkeit					■		■						■				■	■	
keine ungültigen Stimmen																			
Auszählung ohne Fehler													■						
Das Manipulationsrisiko skaliert hoch												■							
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes							■					■							
funktionelle Fehler *(bugs)*															■				
Softwaretests												■							
Intrusionstests							■												
Softwareinspektion																			
Zertifizierung							■					■						■	
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹					■							■	■						■
Werden Manipulationen erkannt?												■							
›Hacker‹, ›hacken‹, ›gehackt‹							■	■				■							
Innentäter												■							
Schwachstellen *(exploits)*																			
Hintertüren												■							
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert						■						■							

The Guardian	02.09.04 (a) [557]	02.09.04 (b) [558]	16.08.04 [559]	14.08.04 [560]	07.08.04 [561]	05.08.04 [562]	12.06.04 [563]	10.06.04 [564]	03.06.04 [565]	27.05.04 [566]	14.05.04 [567]	03.05.04 [568]	21.04.04 (a) [569]	21.04.04 (b) [570]	03.03.04 [571]	19.02.04 [572]	16.02.04 (a) [573]	16.02.04 (b) [574]	12.02.04 (a) [116]
System entweder sicher oder unsicher																	■	■	
Sicherheit ist relativ																	■	■	
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers			■	■	■			■								■			■
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme																			■
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne					■													■	
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																	■		
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar																			■
Ist REV technisch evtl. nicht machbar?																■			■
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit				■												■			
Verfügbarkeit			■												■				■
keine ungültigen Stimmen																		■	
Auszählung ohne Fehler																	■		
Das Manipulationsrisiko skaliert hoch																			■
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																	■		
funktionelle Fehler *(bugs)*																			
Softwaretests																■			
Intrusionstests																			
Softwareinspektion																			
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹			■			■								■			■		
Werden Manipulationen erkannt?																		■	■
›Hacker‹, ›hacken‹, ›gehackt‹																	■		
Innentäter																			■
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			■
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert																			■

The Guardian	12.02.04 (b) [575]	29.01.04 [576]	28.01.04 [577]	22.01.04 [578]	12.12.03 [579]	11.12.03 [580]	10.12.03 (a) [581]	10.12.03 (b) [582]	09.10.03 (a) [583]	09.10.03 (b) [584]	08.10.03 (a) [40]	08.10.03 (b) [585]	08.10.03 (c) [586]	26.09.03 [587]	19.09.03 [588]	18.09.03 [589]	21.08.03 [590]	07.08.03 [591]	02.08.03 [592]
System entweder sicher oder unsicher																			
Sicherheit ist relativ																			
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers			■	■				■			■					■		■	
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme			■																
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne																			
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																			
digitale Signatur																			
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?																			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																			
Verfügbarkeit																		■	
keine ungültigen Stimmen																			
Auszählung ohne Fehler										■									
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes		■																	
funktionelle Fehler *(bugs)*																			
Softwaretests						■												■	
Intrusionstests																			
Softwareinspektion																			
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹																			
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹																			
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert																			

The Guardian	10.07.03 [593]	03.07.03 [594]	26.06.03 [595]	17.06.03 [596]	02.06.03 [597]	29.05.03 [598]	10.05.03 [599]	08.05.03 [600]	07.05.03 [601]	03.05.03 [602]	01.05.03 (a) [34]	01.05.03 (b) [603]	30.04.03 [129]	28.04.03 [604]	25.04.03 [176]	24.04.03 [605]	27.02.03 [606]	12.02.03 [607]	24.01.03 [608]
System entweder sicher oder unsicher													■						
Sicherheit ist relativ																			
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers	■					■		■			■								
Integrität der Stimme																			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme	■										■		■					■	
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne																			
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich											■								
Verschlüsselung											■								
digitale Signatur																			
Annahme: REV ist technisch machbar					■														
Ist REV technisch evtl. nicht machbar?													■						
Zielkonflikte bei Schutzzielen							■												
Bedienbarkeit									■										
Verfügbarkeit								■			■								
keine ungültigen Stimmen											■								
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch																			
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*																			
Softwaretests																		■	
Intrusionstests																			
Softwareinspektion											■								
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?											■								
›Manipulation‹, ›manipulier…‹							■				■								
Werden Manipulationen erkannt?							■												
›Hacker‹, ›hacken‹, ›gehackt‹		■											■						
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert																			

The Guardian	12.12.02 [609]	05.12.02 [610]	28.11.02 [134]	05.11.02 [611]	31.10.02 [612]	17.10.02 [613]	27.09.02 [614]	28.08.02 [615]	13.08.02 [616]	05.08.02 [617]	02.08.02 [618]	17.07.02 [619]	04.07.02 [620]	14.05.02 [621]	02.05.02 [622]	12.04.02 [623]	10.04.02 [624]	22.02.02 [625]	05.02.02 [626]
System entweder sicher oder unsicher						■													
Sicherheit ist relativ																			
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers			■			■		■				■	■						
Integrität der Stimme						■													
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme	■		■						■										
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne			■			■													
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung			■																
digitale Signatur																		■	
Annahme: REV ist technisch machbar																			
Ist REV technisch evtl. nicht machbar?						■													
Zielkonflikte bei Schutzzielen						■													
Bedienbarkeit							■												
Verfügbarkeit						■													
keine ungültigen Stimmen																			
Auszählung ohne Fehler																			
Das Manipulationsrisiko skaliert hoch						■													
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes			■																
funktionelle Fehler *(bugs)*																			
Softwaretests																			
Intrusionstests																			
Softwareinspektion			■																
Zertifizierung																			
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?																			
›Manipulation‹, ›manipulier…‹							■			■									
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹												■							
Innentäter																			
Schwachstellen *(exploits)*																			
Hintertüren																			
Schadsoftware *(malware)*																			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert																			

The Guardian	08.01.02 [627]	07.01.02 [628]	12.12.01 [629]	23.11.01 (a) [630]	23.11.01 (b) [631]	05.10.01 [632]	04.10.01 [633]	26.07.01 [634]	25.07.01 [635]	05.07.01 [636]	14.06.01 [637]	11.06.01 [638]	29.05.01 [639]	16.05.01 [640]	16.02.01 [641]	30.11.00 [642]	26.10.00 [643]	17.08.00 [644]	07.08.00 [645]
System entweder sicher oder unsicher								■											
Sicherheit ist relativ										■						■			
maßgeblich ist das schwächste Glied																			
Autorisierung des Wählers				■												■			
Integrität der Stimme																■			
individuelle Verifizierbarkeit																			
Vertraulichkeit der Stimme										■						■			
Bruch der Vertraulichkeit der Stimme																			
Integrität der Urne																■			
universelle Verifizierbarkeit																			
vollständige Verifizierbarkeit																			
physischer Schutz der Server																■			
Autorisierung des Zugriffs																			
Zusammenwirken Mehrerer erforderlich																			
Verschlüsselung																■			
digitale Signatur										■						■			
Annahme: REV ist technisch machbar										■						■			
Ist REV technisch evtl. nicht machbar?					■											■			
Zielkonflikte bei Schutzzielen																			
Bedienbarkeit																			
Verfügbarkeit																			
keine ungültigen Stimmen							■												
Auszählung ohne Fehler													■						
Das Manipulationsrisiko skaliert hoch											■								
Quellcode (ohne Veröffentlichung)																			
Veröffentlichung des Quellcodes																			
funktionelle Fehler *(bugs)*																			
Softwaretests																			
Intrusionstests																			
Softwareinspektion																			
Zertifizierung										■	■								
Ein Informatiksystem ist eine *Blackbox*																			
ohne bes. Sachkenntnis nachvollziehbar?											■								
›Manipulation‹, ›manipulier…‹										■	■					■			
Werden Manipulationen erkannt?																			
›Hacker‹, ›hacken‹, ›gehackt‹																			
Innentäter																			
Schwachstellen *(exploits)*																■			
Hintertüren																			
Schadsoftware *(malware)*																■			
Ausspähen von Informationen *(phishing)*																			
trojanische Pferde																■			
Sicherheit ist ein ständiger Wettlauf																			
Konkrete Lücken werden geschildert										■									

The Guardian	15.05.00 [646]	06.05.00 [9]	05.05.00 [647]	04.05.00 (a) [648]	04.05.00 (b) [649]	27.04.00 [650]	05.04.00 [35]	14.03.00 [651]	17.02.00 [652]	06.01.00 [653]
System entweder sicher oder unsicher										
Sicherheit ist relativ										■
maßgeblich ist das schwächste Glied										
Autorisierung des Wählers	■									
Integrität der Stimme										
individuelle Verifizierbarkeit										
Vertraulichkeit der Stimme										■
Bruch der Vertraulichkeit der Stimme										
Integrität der Urne	■			■						
universelle Verifizierbarkeit										
vollständige Verifizierbarkeit										
physischer Schutz der Server										
Autorisierung des Zugriffs										
Zusammenwirken Mehrerer erforderlich										
Verschlüsselung										
digitale Signatur										
Annahme: REV ist technisch machbar										
Ist REV technisch evtl. nicht machbar?										
Zielkonflikte bei Schutzzielen										
Bedienbarkeit										
Verfügbarkeit		■								
keine ungültigen Stimmen		■								
Auszählung ohne Fehler			■				■			
Das Manipulationsrisiko skaliert hoch				■						
Quellcode (ohne Veröffentlichung)										
Veröffentlichung des Quellcodes										
funktionelle Fehler *(bugs)*										
Softwaretests										
Intrusionstests										
Softwareinspektion										
Zertifizierung										
Ein Informatiksystem ist eine *Blackbox*										
ohne bes. Sachkenntnis nachvollziehbar?										
›Manipulation‹, ›manipulier…‹										
Werden Manipulationen erkannt?										
›Hacker‹, ›hacken‹, ›gehackt‹										
Innentäter										
Schwachstellen *(exploits)*										
Hintertüren										
Schadsoftware *(malware)*										
Ausspähen von Informationen *(phishing)*										
trojanische Pferde										
Sicherheit ist ein ständiger Wettlauf										
Konkrete Lücken werden geschildert										