Humboldt-Universität zu Berlin
Institut für Informatik

Sicherheit und Sicherheitsdiskurs bei Wahlgeräten und Wahlcomputern in der BRD

Jörg Pohle

Diplomarbeit im Diplomstudiengang Informatik

Betreuer:

Prof. Dr. Ernst-Günter Giessmann

Prof. Dr. Wolfgang Coy

eingereicht am 31.07.2008
überarbeitete Version vom 06.09.2010

Das Heil der Demokratien, von welchem Typus und Rang sie immer seien, hängt von einer geringfügigen technischen Einzelheit ab: vom Wahlrecht... Ohne die Stütze einer vertrauenswürdigen Abstimmung hängen die demokratischen Institutionen in der Luft.

José Ortega y Gasset: ≫Der Aufstand der Massen≪

Inhaltsverzeichnis

0 Vorbemerkungen **1**

1 Einleitung **2**
1.1 Definitionen . . . 3

2 Verfassungs- und Wahlrecht **6**
2.1 Das Grundgesetz und die Wahlrechtsgrundsätze . . . 7
2.1.1 Demokratieprinzip . . . 7
2.1.2 Allgemeine Wahl . . . 8
2.1.3 Unmittelbare Wahl . . . 8
2.1.4 Freie Wahl . . . 9
2.1.5 Gleiche Wahl . . . 9
2.1.6 Geheime Wahl . . . 10
2.2 Rechtliche Regelungen zu Wahltechniken . . . 12
2.2.1 Öffentlichkeitsprinzip . . . 12
2.2.2 Amtlichkeitsgrundsatz . . . 12
2.2.3 Prinzip der Überprüfbarkeit . . . 13
2.3 Zulassungs- und Genehmigungsvoraussetzungen . . . 14
2.3.1 Bundeswahlgesetz . . . 14
2.3.2 Bundeswahlgeräteverordnung . . . 15
2.3.3 Richtlinien für die Bauart von Wahlgeräten und Wahlcomputern . . . 18
2.3.4 Technischer Aufbau von Wahlgeräten und Wahlcomputern . . . 18
2.3.5 Funktionsweise von Wahlgeräten und Wahlcomputern . . . 20
2.3.6 Anforderungen für Wahlcomputer-Software . . . 21
2.4 Anforderungen an den Umgang mit Wahlgeräten und Wahlcomputern . . . 21
2.4.1 Probleme und Regelungslücken . . . 24

3 Sicherheit **25**
3.1 Schutzziele bei Wahlen . . . 26
3.2 Angriffe . . . 28
3.2.1 Wahlmanipulation . . . 30
3.2.2 Stimmenverkauf und andere Vorteilsgewinnung . . . 40
3.2.3 Vertrauensangriffe . . . 41
3.2.4 Analyse der Risiken . . . 42
3.3 Forensik . . . 43
3.4 Sicherheitsregeln . . . 45
3.5 Common Criteria . . . 46
3.6 Zwischenfazit . . . 49

4 Technik-, Sicherheits- und Diskursgeschichte **50**
4.1 Übergang zu Wahlcomputern . . . 53
4.2 Die Bundestagswahl 2005 . . . 56
4.3 „Nedap-Hack“ . . . 58

4.4 Zwischenstand 65

5 Zusammenfassung und Ausblick **67**

Literatur **69**

0 Vorbemerkungen

Die vorliegende Diplomarbeit entstand im Wintersemester 2007/2008 und im Sommersemester 2008 als zweite Arbeit in meiner wissenschaftlichen Auseinandersetzung mit dem Thema „Wahlgeräte und Wahlcomputer“ nach meiner Studienarbeit.

Ich möchte an erster Stelle Constanze Kurz danken, die mich vor fast zwei Jahren auf den Gedanken gebracht hat, mich ausführlicher mit der vorliegenden Thematik zu beschäftigen und mir zu überlegen, ob ich nicht darüber entweder meine Studien- oder meine Diplomarbeit schreiben wolle. Diese Arbeit ist also auch das Ergebnis ihres überzeugenden Vorschlages. Unterstützung erhielt ich im Rahmen der Recherche freundlicher Weise von Johann Groß, dem Eigentümer von Johann Groß Feinmechanik und Distributor der in der BRD zugelassenen und eingesetzten mechanischen und elektromechanischen Wahlgeräte, und Manfred Mardinskij und Peter Hoffmann vom „Haus der Geschichte“ in Bonn. Ich danke ihnen sehr für die Bereitstellung von Informationen zu Wahlgeräten, Bildmaterial und die Beantwortung meiner Nachfragen. Auch Daniel Apelt und Peter Hartig habe ich zu danken für ihre Bereitschaft, die von mir beschriebenen Angriffsvarianten in Diskussionen auf ihre Möglichkeiten, Grenzen und mögliche Gegenmaßnahmen zu überprüfen. Besonderer Dank gilt auch Ernst-Günter Giessmann für die tatkräftige Unterstützung und die vielen Verbesserungsvorschläge, die in die Arbeit eingeflossen sind. Und nicht zuletzt möchte ich meinen Eltern danken, die mich im Verlauf meines Studiums immer unterstützt haben, wie lange es am Ende auch gedauert hat.

1 Einleitung

„Den Beweis für die Aussage, dass man mit unserer Wahlmaschine auch Schach spielen kann, würde ich gerne vorgeführt bekommen." Diese Aufforderung von Jan Groenendaal im August 2006 an „die Hacker" brachte einen Stein ins Rollen. Groenendaal ist der Geschäftsführer von Groenendaal BV, einer niederländischen Software-Firma, aus derem Haus die Software für die Wahlcomputer der Firma Nedap (N.V. Nederlandsche Apparatenfabriek) stammt. „Die Hacker" sind die Mitglieder der niederländischen Bürgerinitiative „Wij vertrouwen stemcomputers niet" (*Wir vertrauen Wahlcomputern nicht*), denen es kaum zwei Monate nach Groenendaals Aufforderung gelang, einen Nedap-Wahlcomputer vom Typ ESD3B in einen Schachcomputer umzuprogrammieren. Der Stein, der ins Rollen gebracht wurde, ist eine öffentliche Debatte über Sinn, Zweck und Manipulationssicherheit von Wahlcomputern.

Obwohl sich bereits nach den Präsidentschaftswahlen in den USA 2000 und 2004 erste kritische Stimmen zu Wort meldeten und die Verwendung von Wahlcomputern bei der Bundestagswahl 2005 Auslöser mehrerer Wahleinsprüche war, beschränkte sich die Diskussion bis zum in der Öffentlichkeit als „Nedap-Hack" bekannt gewordenen Umbau des Wahlcomputers auf einen kleinen Kreis von vor allem technisch Interessierten. Andere nahmen die Geräte nur dann wahr, wenn ihre Kommune diese zur Verwendung bei Wahlen angeschafft hatte.

Diese Zurückhaltung ist vor dem Hintergrund, dass die ersten mechanischen Wahlgeräte bereits zur Bundestagswahl 1961 und die ersten Wahlcomputer zur Kommunalwahl in Köln 1999 eingesetzt wurden, durchaus überraschend. Die Verwendung von Wahlgeräten ist in der Bundesrepublik also kein neues Phänomen. Trotzdem ist eine der Begründungen von Kommunen für die Anschaffung und den Einsatz von Wahlgeräten immer noch deren vermeintliche Modernität.

Im Zusammenhang mit der Sicherheit von Wahlcomputern verhält es sich ähnlich. Die Physikalisch-Technische Bundesanstalt (PTB) hat alle derzeit eingesetzten Wahlcomputermodelle geprüft und für sicher befunden. Auf diese Prüfergebnisse beriefen und berufen sich die Befürworterinnen und Befürworter von Wahlcomputern selbst dann noch mit großer Selbstverständlichkeit, nachdem schwerwiegende Sicherheitsprobleme und Widersprüche in den Aussagen der PTB-Verantwortlichen an die Öffentlichkeit gelangten. Wie belastbar aber sind die Prüfungen durch die PTB und deren Ergebnisse? Ein großer Teil der Informationen, die eine unabhängige und objektive Bewertung der Sicherheit von Wahlcomputern erlauben würden, werden als Betriebsgeheimnisse eingestuft und sind damit der Öffentlichkeit nicht zugänglich. Dennoch lassen sich Argumentationsstrukturen und Diskussionsverläufe verfolgen und anhand der politischen und gesetzlichen Vorgaben für die Durchführung von Wahlen sowie der immanenten Eigenschaften der eingesetzten Technik bewerten. Einen Überblick über diesen Diskurs will die Arbeit vermitteln.

Wahlen finden nicht in einem gesellschaftlichen oder politischen Vakuum statt. Die Gesetzgeber stellen verfassungsrechtliche Grundsätze auf, denen alle Wahlen genügen müssen. In ihren Händen liegt die Festlegung auf ein Wahlsystem. Sie bestimmen, welche Wahl- und Zähltechniken bei Wahlen verwendet werden dürfen. Sowohl gesetzliche Vorgaben als auch immanente Eigenschaften der eingesetzten Wahl- und Zähltechniken bedingen technische und organisatorische Maßnahmen und Verfahren bei der Durchführung von Wahlen.

Im ersten Teil wird eine Einführung in die verfassungs- und wahlrechtlichen Grundlagen gegeben. Dabei wird ein Schwerpunkt auf die rechtlichen Rahmenbedingungen der Zulassung und des Einsatzes von Wahlgeräten und Wahlcomputern gelegt.

Der zweite Teil beschäftigt sich mit immanenten Eigenschaften und den daraus folgenden Anforderungen an die Sicherheit von Wahltechniken und Wahlverfahren. Dazu wird dargestellt, welche Angriffsziele im Zusammenhang mit Wahlen verfolgt werden können, welche Typen von Angreiferinnen und Angreifern existieren und welche Angriffsvektoren ihnen zur Verfügung stehen. Es wird gezeigt, ob und wie Angriffe auf verschiedene Wahlverfahren und Wahltechniken erkannt und verhindert werden können. Am Beispiel eines Schutzprofils für das Digitale Wahlstift-System wird beleuchtet, welche Fehler im Zusammenhang mit Sicherheitsbetrachtungen gemacht werden können.

Im dritten Teil wird anhand der Geschichte des Einsatzes von Wahlgeräten und Wahlcomputern in der Bundesrepublik der Diskurs über deren Sicherheit und Sicherheitsprobleme nachgezeichnet. Zwar wird der Fokus auf den tatsächlich zugelassenen und eingesetzten Geräten liegen, jedoch werden andere nicht ausgespart. Ziel ist es, Entwicklungen und Änderungen von Argumenten und Argumentationsstrukturen, die für die Sicherheit von Wahlgeräten und Wahlcomputern bzw. gegen deren Unsicherheit sprechen, in ihrer zeitlichen Abfolge mit den bekannt gewordenen Sicherheitsproblemen zu untersuchen. Auf netzgestützte Wahltechniken, die sich in ihren Anforderungen und Bedrohungen von den in dieser Arbeit behandelten Techniken deutlich unterscheiden, wird dabei nicht eingegangen.

1.1 Definitionen

Im Folgenden werden Definitionen für die in der Arbeit verwendeten Begriffe gegeben.

Das *Wahlsystem* beschreibt eine formalisierte Methode, nach der aus den abgegebenen Wahlstimmen ein Wahlergebnis konstruiert wird. Die bekanntesten Wahlsysteme sind die Mehrheitswahl und die Verhältniswahl. Für die Wahlen zum Deutschen Bundestag kommt eine personifizierte Verhältniswahl zum Einsatz.

Als *Wahltechnik* wird das Verfahren oder das Hilfsmittel bezeichnet, das bei der Abgabe der Wahlstimmen zum Einsatz kommt. Papierstimmzettel und Stift sind dabei immer noch die meist genutzte Wahltechnik, jedoch werden vermehrt Wahlgeräte und Wahlcomputer eingesetzt.

Dementsprechend heißt *Zähltechnik* das Verfahren oder Hilfsmittel, mit dem die Auszählung der Wahlstimmen durchgeführt wird. So können Papierstimmzettel entweder manuell, mit Zählgeräten oder mit Zählcomputern ausgezählt werden, während Wahlgeräte und Wahlcomputer grundsätzlich gleichzeitig auch Zählgeräte oder Zählcomputer sind. Eine manuelle Stimmenzählung bedarf bei der Verwendung von Wahlgeräten oder Wahlcomputern einer vom Gerät unabhängigen Ausgabe der Einzelstimmen. Ein Beispiel dafür ist die Ausgabe eines Papierbeleges mit der darauf ausgedruckten Wahlentscheidung.

Mit dem Begriff *Wahlverfahren* soll der gesamte organisatorische Rahmen der Wahl umschrieben werden. Er beinhaltet also insbesondere die Vorbereitung, Durchführung und Nachbereitung der Wahl und alle Handlungen, die von staatlichen Organen bzw. von diesen beauftragten Dritten dabei vornehmen.

Der Begriff *Wahlgerät* ist mehrfach belegt. Einerseits handelt es sich dabei um den rechtswissenschaftlichen Begriff für jede Art von Geräten, die der Abgabe und Zählung von Wahl-

stimmen dienen. Andererseits dient es der Abgrenzung von Wahlcomputern und beschreibt dabei all jene Geräte, die nicht rechnergesteuert, also programmierbar, sind. Aufgrund fundamentaler Unterschiede in Aufbau, Funktionsweise und Eigenschaften wird der Begriff Wahlgerät in dieser Arbeit durchgängig in letzterer Bedeutung verwendet. Ausnahmen betreffen ausschließlich die direkte Zitierung juristischer Quellen.

Wahlgeräte können dabei *mechanisch* oder *elektrisch* betrieben sein. Bei ersteren geschieht sowohl die Stimmabgabe als auch die Zählung rein mechanisch, während bei letzteren zumindest die Stimmabgabe elektrisch gesteuert wird. Alle in der Bundesrepublik eingesetzten Wahlgeräte besitzen jedoch ausschließlich mechanisch arbeitende Zählwerke.

Im Gegensatz zu Wahlgeräten sind *Wahlcomputer* programmierbar. Auch sie kommen sowohl bei der Abgabe als auch bei der Auszählung von Wahlstimmen zum Einsatz.

Zählgeräte und *Zählcomputer* dagegen dienen nur der Auszählung von Wahlstimmen. Auch hier sollen Zählcomputer die programmierbaren Geräte bezeichnen, während alle anderen als Zählgeräte gelten sollen. Hingegen hat der Begriff *Stimmenzählgerät* eine davon abweichende Bedeutung und wird im rechtswissenschaftlichen Umfeld analog zu Wahlgerät gebraucht.

Im Rahmen der Arbeit werden Wahl- und Zähltechniken wie folgt eingeteilt: Auf der obersten Ebene lassen sich papierbasierte und gerätebasierte Wahltechniken trennen, wobei bei ersteren die Stimmen auf Papierstimmzetteln abgegeben werden und bei letzteren direkt auf Geräten oder Computern. Papierbasierte Wahltechniken lassen sich weiterhin anhand der verwendeten Zähltechnik unterscheiden. Die Zählung kann dabei einerseits manuell durchgeführt werden, andererseits durch Zählcomputer und Software. Die Möglichkeit, mechanische oder elektromechanische Zählgeräte einzusetzen, wird in der BRD nicht genutzt und daher hier nicht betrachtet. Die Übernahme der Stimmdaten vom Papierstimmzettel in den Zählcomputer kann entweder zum Zeitpunkt der Stimmabgabe wie beim Digitalen Wahlstift-System oder während der Auszählung erfolgen. Gerätebasierte Wahltechniken bedienen sich entweder mechanischer oder elektromechanischer Wahlgeräte oder Wahlcomputer. Bei mechanischen Wahlgeräten – Beispiele sind „Schematus“ oder „System Darmstadt“ – erfolgt die Stimmabgabe an Bedienelementen, die die mechanischen Zählwerke durch eine direkte mechanische Verbindung auslösen. Bei elektromechanischen Wahlgeräten – etwa „Schematus E“ oder „System Darmstadt T“ – werden die mechanischen Zählwerke elektromagnetisch ausgelöst, wobei die Auslöser elektrisch von den Bedienelementen angesteuert werden. Wahlcomputer wie die Nedap „ESD“-Modelle werden über Tastaturen bedient, die die abgegebenen Stimmen über Tastaturcontroller der Wahlcomputersoftware mitteilen, die diese dann auf einem entnehmbaren Speichermodul speichert. Die Auszählung erfolgt außerhalb der Wahlcomputer mit Hilfe einer Auszählungssoftware. Wahlcomputer, die Stimmen entweder gleichzeitig speichern und zählen oder nicht speichern und nur zählen, finden in der BRD derzeit keine Verwendung.

Manipulierte Wahlergebnisse oder solche, die sonst nicht dem Wählerwillen entsprechen, sollen als *konsistent* bezeichnet werden, wenn sie von „echten“ Wahlergebnissen nicht zu unterscheiden sind. Sie besitzen eine *innere Konsistenz*, wenn bei der Gegenüberstellung der Zahlen der Wählerinnen und Wähler, der abgegebenen Stimmen und der Summen der Einzelstimmen keine Auffälligkeiten auftreten. Die Bedingungen der *äußeren Konsistenz* umfassen die Erwartungen an das Wahlergebnis, die sich aus dem aktuellen politischen Umfeld, den Ergebnissen der letzten Wahlen und den Ergebnissen der Nachbarwahlkreise sowie eventu-

ell durchgeführten Nachwahlumfragen ableiten. Andernfalls heißen solche Wahlergebnisse *inkonsistent*.

2 Verfassungs- und Wahlrecht

Der folgende Abschnitt ist eine überarbeitete und kondensierte Fassung der Ausführungen zum Wahlrecht in meiner Studienarbeit. Für eine ausführliche und juristisch korrekte Zitierung wird daher auf (Poh07) verwiesen.

Rechtliche Grundlagen der Organisation und Durchführung von Wahlen sind das im Grundgesetz (GG) verankerte Demokratieprinzip (Art. 20 Abs. 1, 2 GG) und die darauf aufbauenden Wahlrechtsgrundsätze (Art. 38 Abs. 1 GG). Alle Wahlen müssen unabhängig von der verwendeten Wahltechnik diesen Prinzipien genügen. Für Wahlen zum Deutschen Bundestag gelten darüber hinaus das Bundeswahlgesetz (BWahlG) und die Bundeswahlordnung (BWO) sowie für die Wahlen zum Europäischen Parlament das Europawahlgesetz (EuWG) und die Europawahlordnung (EuWO). Außerdem enthalten die Verfassungen der einzelnen Bundesländer Wahlgrundsatzbestimmungen und es existieren jeweils Gesetze und Verordnungen für die Durchführung von Landtags- und Kommunalwahlen. Auch sie gelten grundsätzlich unabhängig von der eingesetzten Wahltechnik. Wahltechnikspezifisch sind nur die Bundeswahlgeräteverordnung (BWahlGV), die auch für Europawahlen Anwendung findet, und die jeweiligen Wahlgeräteverordnungen für Landtags- und Kommunalwahlen. Sie ermöglichen und regeln den Einsatz von Wahl- und Zählgeräten sowie Wahl- und Zählcomputern.

Die Regelungen in den einzelnen Bundesländern für den Einsatz von Wahlgeräten und Wahlcomputern sind dabei alles andere als einheitlich. In allen Bundesländern können sie – gestützt auf BWahlGV – grundsätzlich zu Bundestags- und Europawahlen verwendet werden.

In Baden-Württemberg dürfen Wahlgeräte und Wahlcomputer darüber hinaus bei Landtagswahlen eingesetzt werden. Demgegenüber ermöglicht die Kommunalwahlordnung nur den Einsatz von Zählgeräten und Zählcomputern für Kommunalwahlen.

Die Lage in Bayern ist verworrener. Einerseits dürfen auch dort Wahlgeräte und -computer zu Landtagswahlen eingesetzt werden, aber weder die betreffenden Gesetze noch die Verordnungen für die Durchführung von Wahlen auf Gemeinde-, Landkreis- oder Bezirksebene erlauben explizit den Einsatz von Stimmenzählgeräten. Dennoch wurden bei der Kommunalwahl am 2. März 2008 Scanner und Zählcomputer eingesetzt. Dies geschah wohl unter Bezugnahme auf § 15 der Gemeinde- und Landkreiswahlordnung, die den Einsatz von „Datenverarbeitungsanlagen“ bei der Ermittlung und Feststellung des Wahlergebnisses ermöglicht.

In Berlin ist die Verwendung von Wahlgeräten und Wahlcomputern bei Wahlen zum Abgeordnetenhaus und zu den Bezirksparlamenten grundsätzlich nicht zulässig, genauso wenig wie der Einsatz von Zählgeräten und Zählcomputern. Gleiches gilt in Bremen, Sachsen und Thüringen für die Wahlen zu den jeweiligen Landes- und Kommunalvertretungen.

Brandenburg ermöglicht den Einsatz von Geräten zur Stimmabgabe und -auszählung für alle Arten von Wahlen und Abstimmungen. Eine genauso umfassende Zulässigkeit ist in Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Schleswig-Holstein, Sachsen-Anhalt sowie im Saarland gesetzlich normiert.

Im Folgenden werden ausgehend vom Grundgesetz und den darin statuierten Wahlrechtsgrundsätzen die rechtliche Rahmenbedingungen dargestellt, denen jede Wahl in der BRD genügen muss. Darauf aufbauend wird anhand der einschlägigen Gesetze und Verordnungen gezeigt, welche Eigenschaften Wahltechniken erfüllen müssen, um diesen Vorgaben zu entsprechen. Anschließend werden die Regelungen und Bedingungen beleuchtet, nach de-

nen Wahlgeräte und Wahlcomputer amtlich zugelassen und ihre Verwendung bei Wahlen genehmigt werden. Zuletzt werden – wenn auch nur anhand der BWO – die Verfahrensanforderungen erläutert, die die Wahlvorstände bei der Verwendung von Wahlgeräten und Wahlcomputern beachten müssen.

2.1 Das Grundgesetz und die Wahlrechtsgrundsätze

Im Grundgesetz hat der Verfassungsgeber die rechtlichen Regelungen festgeschrieben, an die sich jedes staatliche Handeln halten muss. Dazu gehören auch Festlegungen zum politischen Entscheidungsfindungsverfahren und eine Rahmensetzung für deren Durchführung. Die Entscheidung für eine demokratische Entscheidungsfindung nimmt daher einen besonderen Platz ein, wie deren Schutz durch die Ewigkeitsklausel des Art. 79 Abs. 3 GG belegt. Demokratische Entscheidungsfindung ist dabei mehr als nur Mehrheitsprinzip bei Abstimmungen. Sie schließt Minderheitenschutzrechte ebenso ein wie Grundsätze zur Ermittlung der Entscheidung durch Wahlen. Auf ein bestimmtes Wahlsystem hat sich der Verfassungsgeber dabei jedoch nicht festgelegt. Dies hat er dem Gesetzgeber überlassen und ihm dabei gleichwohl enge Grenzen für die Umsetzung auferlegt. Nach Art. 38 Abs. 1 GG müssen Wahlen zum Deutschen Bundestag allgemein, unmittelbar, frei, gleich und geheim sein. Die gleichen Grundsätze gelten nach Art. 28 Abs. 1 S. 2 GG auch für Wahlen in den Ländern, Kreisen und Gemeinden und als allgemeine Rechtsprinzipien für Wahlen zu allen Volksvertretungen im staatlichen und kommunalen Bereich. Sie gelten dabei nicht nur für den Wahlakt selbst, sondern auch für die Wahlvorbereitung und -nachbereitung, so diese noch mit der Wahl im Zusammenhang steht. Auch gelten sie unterschiedslos für das aktive und das passive Wahlrecht.

2.1.1 Demokratieprinzip

Die Strukturentscheidung für einen demokratischen Staat wird durch die Volkssouveränität konkretisiert, der gemäß Art. 20 Abs. 2 S. 1 GG alle Staatsgewalt vom Volk ausgeht, also keine anderen Legitimationsquellen haben kann. Sie darf nach Abs. 2 S. 2 auch nur vom Volk ausgeübt werden, entweder in Wahlen und Abstimmungen oder durch besondere Organe. Während dabei Wahlen Personalentscheidungen darstellen, entscheiden Abstimmungen über Sachfragen. Die Organe, durch die das Volk die Staatsgewalt ausübt, müssen demokratisch legitimiert sein, um einen effektiven Einfluss des Volkes auf die Ausübung der Staatsgewalt sicher zu stellen und damit jedes staatliche Handeln auf den Willen des Volkes zurück zu führen. Diese demokratische Legitimation kann dabei entweder direkt oder indirekt bestehen. Die direkte Legitimation folgt unmittelbar aus der Wahl des Organs selbst. Existiert eine solche direkte Legitimation nicht, dann muss es zumindest eine ununterbrochene Legitimationskette von einem gewählten Parlament zu diesem Organ geben. Eine demokratische Legitimation kann nicht von unbeschränkter Dauer sein. Sie muss vielmehr in regelmäßigen Abständen erneuert werden. Die aus diesem Erneuerungszwang abgeleitete Wahlperiode kann dabei unterschiedlich lang sein. Sie reicht von vier Jahren für den Bundestag und bei einigen Länder- und Kommunalparlamenten über fünf Jahre bei anderen Landtagen und Kommunalvertretungen bis zu acht Jahren bei der Wahl zahlreicher Landrätinnen und Landräte.

2.1.2 Allgemeine Wahl

Das Volk, vom dem die Staatsgewalt ausgeht, ist das Staatsvolk. Jeder Staatsbürgerin und jedem Staatsbürger muss es daher möglich sein, an Wahlen und Abstimmungen teilzunehmen. Das Prinzip der allgemeinen Wahl soll dies garantieren. Jeder unberechtigte Ausschluss von Staatsangehörigen von der Teilnahme an Wahlen und Abstimmungen ist daher unzulässig. Insbesondere ist es dem Gesetzgeber verboten, bestimmte Gruppen von Staatsangehörigen aus politischen, wirtschaftlichen oder sozialen Gründen von der Ausübung des Wahlrechts auszuschließen. Historisch bedeutsam sind vor allem das erst 1919 erkämpfte Frauenwahlrecht sowie der Ausschluss einer Koppelung des Wahlrechts an persönlichen Besitz, Steuerleistung oder berufliche Selbständigkeit, die der allgemeinen Wahl erst zum Durchbruch verhalfen. Aktuell dreht sich der Streit um die Einführung eines allgemeinen Wahlrechts für Nichtdeutsche.

Berechtigt, an den Wahlen zum Deutschen Bundestag teilzunehmen, sind alle Deutschen gemäß Art. 116 Abs. 1 GG, die am Wahltag gemäß Art. 38 Abs. 2 1. Halbsatz GG das 18. Lebensjahr vollendet haben (aktives Wahlrecht) oder nach Halbsatz 2 volljährig sind (passives Wahlrecht). Für Wahlen zum Europaparlament sowie für viele Landesparlamente sind auch Staatsangehörige der anderen EU-Staaten wahlberechtigt, die zum Zeitpunkt der Wahl ihren gewöhnlichen Aufenthalt im Geltungsbereich des Grundgesetzes haben. Ähnliche Altersgrenzen existieren auch für alle anderen Wahlen, wobei in einigen Bundesländern das Wahlalter für die Teilnahme an Kommunalwahlen auf 16 gesenkt wurde.

Einschränkungen des allgemeinen Wahlrechts sind nur in engen Grenzen zulässig. So kann das Wahlrecht durch Richterspruch abgesprochen werden. Als Wahlrechtsausschlussgründe gelten auch dauerhafte Betreuung mangels Mündigkeit und die Unterbringung in einem psychiatrischen Krankenhaus. Im Rahmen der Wahlvorbereitung gelten Unterschriftenquoren für die Einreichung von Wahlvorschlägen als verfassungsrechtlich unbedenkliche Einschränkungen des allgemeinen Wahlrechts, so lange diese nicht unangemessen hoch sind.

2.1.3 Unmittelbare Wahl

Das Ziel des Unmittelbarkeitsgrundsatzes ist, den Willen der Wählerinnen und Wähler unverfälscht in der Zusammensetzung des Parlaments zum Ausdruck zu bringen. Damit die Wählerinnen und Wähler das letzte Wort haben, darf zwischen der Stimmabgabe und der Ermittlung des Wahlergebnisses nur der rein mathematische Vorgang des Auszählens stehen.

Dieser Wahlrechtsgrundsatz wird beeinträchtigt, wenn sich zwischen den Wahlakt und das Wahlergebnis eine fremde Willensentscheidung einschiebt, die nicht die Entscheidung der Wahlbewerberin oder des Wahlbewerbers zur Annahme oder Ablehnung der Wahl ist. Wahlfrauen und -männer sind damit ausgeschlossen. Dabei steht privates Handeln staatlichem gleich, sofern das private auf der Grundlage staatlicher Regelungen geschieht. Ohne eine solche rechtliche Grundlage soll privates Handeln die Unmittelbarkeit der Wahl nicht beeinträchtigen können.

Ein Gesetz, das es Parteien ermöglichen würde, nach der Wahl bei Erschöpfung ihrer Liste weitere Personen als Ersatzleute zu nominieren, verstieße damit gegen das Unmittelbarkeitsgebot.

2.1.4 Freie Wahl

Die Wahlfreiheit hat zum Ziel, jede Art von Druck, Zwang oder sonstigem rechtswidrigen Einfluss auf Wählerinnen und Wähler sowie Wahlbewerberinnen und Wahlbewerber sowohl vor und während als auch nach der Wahl zu verhindern. In erster Linie geht es dabei um staatliches Handeln, aber auch privates Handeln kann die Wahlfreiheit beeinträchtigen, wenn sie den Rahmen der Meinungsfreiheit verlässt. Dazu gehören alle Handlungen, die die Tatbestände des § 108 StGB (Wählernötigung) oder des § 108 a StGB (Wählertäuschung) erfüllen.

Die Freiheit der Wahl umfasst auch die Freiheit der Wahlvorschläge und die freie Kandidatinnen- und Kandidatenaufstellung durch Parteien und Wahlvereinigungen. Sie kann auch nur dann gegeben sein, wenn tatsächlich eine Auswahlmöglichkeit zwischen mehreren Bewerberinnen und Bewerbern, Gruppierungen oder Entscheidungsalternativen besteht. Nachwahlumfragen dürfen nicht vor Ablauf der Wahlzeit veröffentlicht werden, weil diese den freien und offenen Prozess der Meinungs- und Willensbildung des Volkes, und damit die Freiheit der Wahl unzulässig einschränken. Aus dem gleichen Grund ist es den Staatsorganen in amtlicher Funktion untersagt, durch besondere Maßnahmen als Staatsorgane am Wahlkampf teilzunehmen.

2.1.5 Gleiche Wahl

Während der Grundsatz der allgemeinen Wahl den Einfluss aller Staatsbürgerinnen und Staatsbürger auf die Ausübung der Staatsgewalt verwirklichen soll, dient das Prinzip der gleichen Wahl der Gewährleistung des *gleichen* Einflusses im Sinne einer gleichen Stimmenwertung. Diese Gleichheit ist dabei formal zu verstehen, Differenzierungen sind ausschließlich zum Schutz anderer Verfassungsgüter zulässig. So haben alle Wahlberechtigten die gleiche Anzahl an Stimmen und alle abgegebenen Stimmen werden gleich gezählt (Gleichheit des Zählwertes). Darüber hinaus muss jede gültig abgegebene Stimme im Rahmen des Wahlsystems den gleichen Einfluss auf das Wahlergebnis und damit auf die Verteilung der Abgeordnetensitze haben (Gleichheit des Erfolgswertes). Im Verhältniswahlsystem ist dieser Grundsatz absolut, weil dieses System selbst eine möglichst genaue Abbildung der Stimmverteilung auf die Sitzverteilung herstellen will. Demgegenüber bleiben in einem Mehrheitswahlsystem alle Stimmen unberücksichtigt, die für unterlegene Kandidatinnen und Kandidaten abgegeben werden – diese haben nur noch einen potentiellen Erfolgswert. Aus diesem Grund wird teilweise vertreten, dass ein alleiniges Mehrheitswahlrecht gegen den Gleichheitsgrundsatz verstößt. Im gemischten Mehrheits- und Verhältniswahlrecht der BRD – der personalisierten Verhältniswahl – ist die Sitzverteilung grundsätzlich – abgesehen von Überhangmandaten – vom Stimmenverhältnis (bei den Zweitstimmen) abhängig, während die Hälfte der Abgeordneten persönlich (durch die Erststimmen) bestimmt wird.

Historisch bedeutet die Wahlgleichheit eine Abgrenzung z. B. zu dem in Preußen bis 1918 geltenden Drei-Klassen-Wahlrecht, das die Wähler – Frauen waren nicht wahlberechtigt – entsprechend ihren Steuerleistungen in drei Klassen einteilte und dabei den Angehörigen der höheren Klassen ein erheblich größeres Stimmengewicht zubilligte.

Für die Wahlvorbereitung gilt die Wahlgleichheit ebenfalls, dort jedoch im Sinne von Chancengleichheit und nur als Diskriminierungsverbot. Eine Pflicht des Staates, die unterschiedli-

chen Voraussetzungen der einzelnen Kandidatinnen, Kandidaten und Wahlvereinigungen zu nivellieren, wird daraus aber nicht gefolgert. Auch Unterschriftenquoren als Voraussetzung für die Zulassung eines Wahlvorschlags sollen nicht gegen die Chancengleichheit verstoßen, weil diese nur dazu dienen würden, von vornherein chancenlose Bewerbungen und sogenannte Spaßkandidaturen zu verhindern.

Während der Wahl, der Stimmenauszählung und der Ermittlung des Wahlergebnisses ist der Gleichheitsgrundsatz demgegenüber sehr weit gefasst. Es reicht nicht aus, dass der Gesetzgeber das Wahlsystem so ausgestaltet, dass abgegebenen Stimmen kein unterschiedlicher Zählwert zukommt, er muss auch durch geeignete Regelungen den typischen Ursachen von Zählfehlern entgegenwirken. Diese Regelungen sollen nicht nur die ungewollten sondern auch die durch Wahlmanipulation und Wahlfälschung gewollten Zählfehler umfassen. Und weil Reglungen allein nicht verhindern können, dass Wahlergebnisse – und damit Sitzverteilungen – in Einzelfällen nicht zutreffend ermittelt werden können, und der Gesetzgeber dies in Rechnung stellen muss, ist er zur Schaffung eines Verfahrens verpflichtet, das es erlaubt, Zweifeln an der Richtigkeit der Stimmenauszählung nachzugehen und erforderlichenfalls das Wahlergebnis richtig zu stellen sowie die Sitzverteilung zu korrigieren. Daher sieht das Grundgesetz in Art. 41 GG die Einrichtung eines solchen Wahlprüfungsverfahrens ausdrücklich vor. Gleiches gilt für die Verfassungen der Länder.

Für die Ermittlung der Sitzverteilung ist der Gleichheitsgrundsatz wiederum eingeschränkter. So werden Sperrklauseln, wie sie seit dem ersten Wahlgesetz fester Bestandteil der bundesdeutschen politischen Landschaft sind, in der Rechtswissenschaft mehrheitlich als mit dem Grundgesetz vereinbar gesehen. Mit solchen Sperrklauseln – für die Wahlen zum Deutschen Bundestag gilt eine Fünf-Prozent-Hürde genauso wie für Wahlen zu allen Landesparlamenten, während es auf kommunaler Ebene inzwischen fast durchgehend nur noch Drei-Prozent-Klauseln gibt oder die Sperrklauseln gar ganz abgeschafft wurden – sollen die Gefahr der Parteienzersplitterung gebannt und Handlungs- und Entscheidungsfähigkeit der Parlamente gesichert werden. Auch die Grundmandatsklausel, mit deren Hilfe Parteien die Fünf-Prozent-Klausel umgehen können, ruft immer wieder Kritik hervor. Gleichwohl vertritt auch hier eine Mehrheit in der Literatur die Meinung, sie sei verfassungsgemäß, weil sie den Charakter der Wahl als Integrationsvorgang bei der politischen Willensbildung des Volkes unterstütze. Während die Grundmandatsklausel eine Hilfe für kleinere Parteien darstellt, profitieren fast ausschließlich große Parteien von den Überhangmandaten, die entstehen, wenn eine Partei mehr Direktmandate erzielt, als ihr nach dem Verhältnis ihrer Zweitstimmen Mandate zustünden. Auch sie sind in den letzten Jahren verstärkt in die Diskussion geraten und werden überwiegend als verfassungswidrig betrachtet, aber ihre Profiteure – also die Parteien, die dann auch oft an der Regierung beteiligt sind – verhindern seit Jahren erfolgreich eine Abschaffung.

2.1.6 Geheime Wahl

Das Wahlgeheimnis ist sowohl ein individuelles Recht als auch – im Sinne eines objektiven Prinzips der Wahl – eine Pflicht der Wählerinnen und Wähler. Die einzelnen Wählenden dürfen nicht aus ihren abgegebenen Stimmen identifizierbar sein – weder vor, während noch nach der Wahl.

Die geheime Wahl ist unbedingte Voraussetzung einer freien Wahl, weil nur durch das Wahlgeheimnis sichergestellt werden kann, dass die oder der Wahlberechtigte keine Repressalien im Zusammenhang mit ihrer oder seiner Wahlentscheidung fürchten muss. Das Wahlgeheimnis stellt damit eine institutionelle Garantie der Wahlfreiheit dar, jeder Wahlgeheimnisbruch gefährdet die Wahlfreiheit. Die Strafbarkeit der Verletzung des Wahlgeheimnisses nach § 107 c StGB ist daher nur folgerichtig.

Während der Wahlvorbereitung kann das Wahlgeheimnis nur unvollkommen gewahrt werden, es darf aber nicht in weiterem Umfang preisgegeben werden, als zur ordnungsgemäßen Durchführung der Wahl notwendig ist. Eine solche Einschränkung ist die Notwendigkeit, dass die Kandidatinnen und Kandidaten, die sich zur Wahl stellen, bekannt sein müssen und damit auch bekannt gemacht werden können. Eine zweite Einschränkung ergibt sich aus der Pflicht für bisher nicht im Parlament vertretenen Parteien und Einzelbewerberinnen und -bewerber, ein Unterschriftenquorum als Voraussetzung für einen Wahlvorschlag zu erfüllen. Diese Notwendigkeit sei dadurch gerechtfertigt, als dass sich daraus auf die Ernsthaftigkeit des Wahlvorschlags schließen ließe. Weil es sich dabei gleichwohl um eine Selbstprivilegierung der etablierten Parteien handelt, die von der Rechtsprechung unhinterfragt toleriert wird, steht diese Regelung jedoch seit langem in der Kritik.

Der Wahlakt selbst muss geheim sein. Der Staat ist verpflichtet, die geheime Stimmenabgabe zu gewährleisten. Dafür muss der Wahlvorgang technisch derart gestaltet sein, dass es unmöglich ist, die Wahlentscheidung einer Wählerin oder eines Wählers erkennen oder rekonstruieren zu können. Insbesondere ist eine offene Wahl verfassungswidrig. Nur zugunsten des Wahlrechts selbst sind Abstriche von dieser strengen Auslegung des Wahlgeheimnisses zulässig. So verlangt der Vorrang der allgemeinen Wahl, dass sich Menschen mit Behinderung von einer Vertrauensperson beim Wahlakt helfen lassen können. Die zweite und seit jeher durchaus umstrittene Ausnahme ist die Briefwahl.

Die Briefwahl kann weder die geheime, die persönliche noch die freie Wahl garantieren. Auch für die Briefwahl wird jedoch zugunsten der Verwirklichung des Grundsatzes der allgemeinen Wahl eine Ausnahme vom strengen Schutz des Wahlgeheimnisses gemacht, allerdings ist sie nicht unbeschränkt und unbedingt zulässig. Durch die Verpflichtung für Briefwählerinnen und -wähler, die Unmöglichkeit einer persönlichen Stimmabgabe glaubhaft zu machen, sich selbst die Briefwahlunterlagen zu beschaffen und eidesstattlich zu versichern, dass sie den Stimmzettel persönlich gekennzeichnet haben, wird die Briefwahl wirksam beschränkt. Und weil der Gesetzgeber in der Pflicht steht, die Regelungen zur Briefwahl anhand aktueller Entwicklungen fortwährend zu überprüfen, für eine bestmögliche Sicherung und Gewährleistung der Wahlrechtsgrundsätze zu sorgen und alle möglicherweise auftretenden Gefahren für die Integrität der Wahl frühzeitig zu beseitigen, gilt die Briefwahl auch nicht unbedingt.

Keinen Verstoß gegen das Wahlgeheimnis stellt ein Selbstbekenntnis von Wahlberechtigten zu ihrer Wahlentscheidung dar. Dies gilt sowohl vor als auch nach der Wahl und wird damit begründet, dass eine Übereinstimmung der offenbarten Wahlentscheidung mit der tatsächlichen nicht überprüfbar ist. Jede Handlung, die eine solche Überprüfbarkeit ermöglichen würde, unterliegt der Strafandrohung des § 107 c StGB. Wahl- und Nachwahlumfragen sind damit vor dem Hintergrund des Wahlgeheimnisses unbedenklich.

2.2 Rechtliche Regelungen zu Wahltechniken

Während die oben genannten verfassungsrechtlichen Regelungen für alle im Zusammenhang mit einer Wahl oder Abstimmung stehenden Bereiche gelten, existieren auch speziell auf den Umgang mit den einzelnen Wahltechniken ausgerichtete Normen. Wahltechniken unterliegen dabei besonderen Anforderungen hinsichtlich des Öffentlichkeitsprinzips als auch des Amtlichkeitsgrundsatzes. Außerdem ist es erforderlich, dass sowohl der Verlauf als auch das Ergebnis der Wahl im Nachhinein vollständig überprüfbar sind.

2.2.1 Öffentlichkeitsprinzip

Grundlage der republikanischen Demokratie ist das Prinzip der Publizität.[1] Entscheidungen unter Ausschluss der Öffentlichkeit können daher immer nur die Ausnahme sein.

Die Notwendigkeit einer öffentlichen Stimmenauszählung folgt unmittelbar aus dem Demokratieprinzip nach Art. 20 Abs. 1 GG. Gleichwohl ist es damit nicht genug und für den gesamten Verlauf einer Wahl – von der Vorbereitung über die Durchführung bis zum Abschluss – finden sich an verschiedenen Stellen gesetzliche Regelungen, die den öffentlichen Charakter der Wahl sicherstellen sollen.

Die besonderen Wahlorgane, die der Gesetzgeber mit der Vorbereitung und Durchführung von Wahlen beauftragt hat, sind nach § 10 Abs. 1 S. 1 BWahlG verpflichtet, in öffentlicher Sitzung zu verhandeln, zu beraten und zu entscheiden. Im Gegensatz zu anderen staatlichen Organen dürfen Wahlorgane gar keine nichtöffentlichen Beratungen durchführen.

Auch die Wahlhandlung, die mit der Eröffnung durch die Wahlvorsteherin oder den Wahlvorsteher beginnt (§ 53 BWO) und mit der Schließung durch diese endet (§ 60 BWO), ist nach § 31 S. 1 BWahlG öffentlich. Obwohl die Ermittlung und Feststellung des Wahlergebnisses nicht zur eigentlichen Wahlhandlung gehören, sind auch diese öffentlich. Das bedeutet, dass alle – gleichgültig, ob wahlberechtigt oder nicht – Zutritt zum Wahlraum haben und den ordnungsgemäßen Ablauf der Wahlhandlung und die Ermittlung und Feststellung des Wahlergebnisses beobachten können.

Der Grundsatz der Öffentlichkeit kann auch nicht eingeschränkt werden, nur weil eine bestimmte Wahltechnik eine öffentliche Stimmenauszählung konstruktionsbedingt unmöglich macht. Möglich wäre eine Einschränkung nur zugunsten einer besseren Durchsetzung eines anderen Verfassungs- oder Wahlrechtsgrundsatzes. Da ein solcher hier nicht ersichtlich ist, erfüllt eine solche Wahltechnik die rechtlichen Anforderungen an eine demokratische Wahl nicht und muss daher als verfassungswidrig gelten.

2.2.2 Amtlichkeitsgrundsatz

Die Durchführung von Parlamentswahlen gehört in der Demokratie zu den wesentlichen Aufgaben des Staates. Sie liegt in den Händen von Amtsträgerinnen, Amtsträgern und staatlichen Organen, die nach einem geregelten Verfahren im Rahmen ihrer Zuständigkeit handeln. Diese Konstellation – Amtsträgerinnen und Amtsträger, gesetzlich festgelegte Zuständigkeiten und geregelte Verfahren – gibt Wahlen einen amtlichen Charakter, der auch in der Wahl selbst zu Tage treten muss. Im Zusammenhang mit der Stimmabgabe auf Stimmzetteln spricht § 34

[1] Der Begriff „Republik“ geht zurück auf die lateinische Bezeichnung *res publica* - „öffentliche Angelegenheit“.

Abs. 1 BWahlG daher auch explizit davon, dass „mit amtlichen Stimmzetteln“ gewählt wird. Gegenüber den Wahlberechtigten wird mit der Amtlichkeit der Stimmzettel garantiert, dass eine von ihnen abgegebene gültige Stimme in jedem Fall korrekt gezählt und gewertet wird.

Gleichwohl können einzelne Handlungen im Zusammenhang mit der Vorbereitung und der Durchführung von Wahlen von Privaten erbracht werden, wenn und solange der Staat die vollständige Kontrolle über den gesamten Wahlablauf behält. Der Druck von Stimmzetteln kann daher problemlos durch Private erfolgen, solange das Layout ausschließlich durch die Wahlorgane durchgeführt und die Korrektheit der Stimmzettel geprüft wird. Wie allerdings die Wahlorgane sicherstellen sollen, dass sie tatsächlich die vollständige Kontrolle über die Software und die Konfiguration von Wahl- und Zählcomputern besitzen, ist unklar. Weder die BWahlGV noch die Anlagen zur BWahlGV beinhalten diesbezügliche Regelungen. Eine Prüfung zumindest der eingesetzten Software soll trotz der fehlenden Regelungen immer durchgeführt werden ((Sie06)).

2.2.3 Prinzip der Überprüfbarkeit

Die Wahlrechtsgrundsätze als objektives Recht schützen die verfassungsmäßige Zusammensetzung des Parlaments. Ihre Einhaltung bei der Wahl zum Deutschen Bundestag lässt sich mit dem in Art. 41 GG vorgesehenen Wahlprüfungsverfahren überprüfen, für die Wahlen zu Landes- und Kommunalparlamenten existieren in den Landeswahlgesetzen ähnliche Vorschriften.

Sowohl auf Bundesebene als auch in den meisten Bundesländern stellen die jeweiligen Parlamente die erste Instanz für die Wahlprüfung. Gegen deren Entscheidung kann dann vor den zuständigen Verfassungsgerichten Beschwerde eingelegt werden. Ausnahmen stellen Berlin, Rheinland-Pfalz und Schleswig-Holstein dar. In Berlin ist das Landesverfassungsgericht die einzige Anlaufstelle der einstufigen gerichtlichen Wahlprüfung. In Rheinland-Pfalz entscheidet nicht der Landtag in erster Instanz sondern ein aus seiner Mitte bestimmter Wahlprüfungsausschuss und in Schleswig-Holstein ist mangels Landesverfassungsgericht das OVG Lüneburg die Beschwerdeinstanz.

Die Wahlprüfung erfolgt in keinem Fall von Amts wegen sondern nur auf Einspruch. Im Allgemeinen sind dabei jede und jeder Wahlberechtigte, jede Gruppe von Wahlberechtigten, manchmal auch Wahlorgane oder Amtsträgerinnen und Amtsträger antragsberechtigt.

Grundsätzlich kann im Zuge der Wahlprüfung jeder Wahlfehler gerügt werden. Im weiteren Sinne sollen als Wahlfehler alle Verstöße gegen das materielle und formelle Wahlrecht einschließlich der Wahlrechtsgrundsätze des Art. 38 GG gelten, also jede im Zusammenhang mit der Wahl vorkommende Rechtwidrigkeit, ob während der Wahlvorbereitung, der Wahlhandlung oder der Feststellung des Wahlergebnisses. Wahlprüfungszweck ist danach nicht nur die Prüfung vergangener sondern auch die zukünftige Gewährleistung gültiger Wahlakte. Im engeren Sinne – und so verstehen die Parlamente und die Verfassungsgerichte die Wahlprüfung – ist ein Wahlfehler nur dann relevant und kann damit erfolgreich angefochten werden, wenn dieser Einfluss auf die Mandatsverteilung besitzt oder besitzen könnte.

Zwar muss die Ursächlichkeit eines Wahlfehlers für das Wahlergebnis nicht positiv festgestellt werden, aber es muss sich um mehr als eine nur theoretische Möglichkeit handeln. Das Vorliegen eines Wahlfehlers selbst muss jedoch zweifelsfrei nachgewiesen werden, andernfalls spreche eine Vermutung für die Gültigkeit der Wahl. Diese Übertragung der

Beweislast auf die Einspruchsberechtigten kann jedoch nur dann verfassungsgemäß sein, wenn die benutzte Wahltechnik eine jederzeitige Überprüfbarkeit nicht grundsätzlich ausschließt. Entsprechend muss sich eine technische Gestaltung des Wahlverfahrens also als verfassungswidrig erweisen, wenn eine nachträgliche Kontrolle des Wahlergebnisses und dessen möglicherweise notwendige Korrektur konstruktionsbedingt unmöglich ist.

2.3 Zulassungs- und Genehmigungsvoraussetzungen

Der Verfassungsgeber hat der Legislative in Art. 38 Abs. 3 GG einen Regelungsvorbehalt für ein Bundesgesetz zur Regelung des Wahlrechts eingeräumt. Im Gegensatz zu einem weitergehenden Gesetzesvorbehalt verhindert ein Regelungsvorbehalt jede Einschränkung der Wahlrechtsgrundsätze ohne zwingenden Grund. Ein solcher Grund kann nur in einem anderen Verfassungsrecht, einem kollidierenden Wahlrechtsgrundsatz oder der Sicherung der mit dem Wahlsystem verfolgten, demokratischen Prinzipien entsprechenden staatspolitischen Zielen liegen. Das gültige Bundeswahlgesetz stammt aus dem Jahr 1953 und wurde zuletzt 1993 umfassend reformiert. Seit 1956 ermöglicht es die Verwendung von Wahlgeräten anstelle von Stimmzetteln. Zu Regelung der Voraussetzungen, die Wahlgeräte erfüllen müssen, um allgemein zur Verwendung bei Wahlen zugelassen werden zu können und Genehmigungen für den Einsatz bei konkreten Wahlen zu erlangen, hat der Gesetzgeber 1975 die Bundeswahlgeräteverordnung erlassen. Nachdem damit ursprünglich nur mechanisch oder elektrisch betriebene Wahlgeräte zulassungs- und verwendungsfähig waren, wurde im Zuge einer Novellierung 1999 auch der Einsatz von Wahlcomputern ermöglicht.

Im Folgenden soll anhand der Regelungen des BWahlG, der BWahlGV und der „Richtlinien für die Bauart von Wahlgeräten“[2] dargestellt werden, welche Voraussetzungen Wahlgeräte und Wahlcomputer nach Meinung des Gesetzgebers erfüllen müssen, um zu Wahlen für den Deutschen Bundestag und das Europaparlament zugelassen zu werden. Die meisten Landesgesetzgeber haben ihrerseits die Zulassung für bundesweite Wahlen als Zulassungsvoraussetzung für Wahlgeräte und Wahlcomputer für Wahlen auf Landes- und kommunaler Ebene in ihre jeweiligen Landeswahlgesetze und Landeswahlgeräteverordnungen aufgenommen. Inhaltlich abweichende technische Voraussetzungen existieren in keinem Bundesland, auf eine gesonderte Behandlung landesrechtlicher Regelungen wird daher verzichtet.

2.3.1 Bundeswahlgesetz

In § 1 Abs. 1 S. 2 wiederholt das BWahlG die in Art. 38 Abs. 1 GG verfassungsrechtlich festgeschriebenen Wahlrechtsgrundsätze der allgemeinen, unmittelbaren, freien, gleichen und geheimen Wahl. Die Ermächtigung zur Verwendung von Wahlgeräten und Wahlcomputern findet sich in § 35 BWahlG.

Zentrale Anforderung an Wahlgeräte und Wahlcomputer ist die Gewährleistung der Geheimhaltung der Stimmabgabe durch die Geräte selbst. Dies verlangt Abs. 2 S. 1 explizit. Auch die konkreten Umstände des Einsatzes im Wahllokal sind nach Abs. 4 so zu gestalten, dass sich daraus keine Rückschlüsse auf das Wahlverhalten ziehen lassen können. Hier sind also sowohl Zulassungs- als auch Einsatzbedingungen gesetzlich festgelegt.

[2] Anlage 1 zu § 2 BWahlGV.

Notwendig für die Verwendung von Wahlgeräten sind weiterhin eine Bauartzulassung sowie eine Verwendungsgenehmigung. Über erstere wird nur auf Antrag des Herstellers durch das Bundesministerium des Innern (BMI) entschieden, letztere kann durch das BMI bei Vorliegen der Bauartzulassung ausgesprochen werden. Sie können jeweils für einzelne Wahlen oder allgemein gelten.

Zur Untersetzung dieser allgemein gehaltenen Regelungen durch konkrete Bestimmungen, Bedingungen und Verfahren hat der Gesetzgeber das BMI in Abs. 3 ermächtigt, eine diesbezügliche Rechtsverordnung zu erlassen. Zu den Rechtsfragen, die von der Rechtsverordnung geregelt werden können, gehören die Voraussetzungen und das Verfahren für die amtliche Bauartzulassung von Wahlgeräten und Wahlcomputern sowie für die Rücknahme und den Widerruf der Zulassung. Weiterhin kann das BMI ein Verfahren für die Prüfung eines Wahlgerätes oder Wahlcomputers auf Übereinstimmung mit der amtlich zugelassenen Bauart und für die öffentliche Erprobung von Wahlgeräten und Wahlcomputern vor ihrer Verwendung bestimmen. Auch das Verfahren für die amtliche Verwendungsgenehmigung sowie deren Rücknahme oder Widerruf kann vom BMI geregelt werden. Und zuletzt kann das BMI Verfahrensvorschriften für die Verwendung von Wahlgeräten und Wahlcomputern erlassen, die sich aus deren technischen Besonderheiten ergeben. Alle diese Regelungsbereiche sind als Kann-Bestimmungen ausgeführt. Gleichwohl lässt sich daraus ablesen, welche Fragen der Gesetzgeber im Zusammenhang mit der Zulassung und Verwendung von Wahlgeräten und Wahlcomputern für regelungsbedürftig hält. Dieser Regelungsermächtigung ist das BMI mit dem Erlass der BWahlGV nachgekommen.

Da es sich bei der Bauartzulassung um ein typisches Verwaltungsverfahren handelt und damit nicht dem „Recht der Wahlen“ mit erheblich eingeschränkter Anfechtungsmöglichkeit unterliegt, finden das Verwaltungsverfahrensgesetz (VwVfG) und die Verwaltungsgerichtsordnung Anwendung. Damit kann ein Hersteller, dessem Antrag auf Bauartzulassung nicht stattgegeben wurde, gegen den Ablehnungsbescheid rechtlich vorgehen. Gleiches gilt für den Umgang mit Rücknahmen und Widerrufen der Bauartzulassung. Hingegen können Gegnerinnen und Gegner von Wahlgeräten und Wahlcomputern nicht gegen eine ergangene Zulassung klagen, weil sie nicht Betroffene im Sinne des VwVfG sind. Demgegenüber handelt es sich bei der Verwendungsentscheidung um eine spezifisch wahlorganisatorische Maßnahme gem. § 49 BWahlG, gegen die jedoch kein spezieller Rechtsbehelf gegeben ist, so dass daraus resultierende Wahlfehler nur in dem nach der Wahl stattfindenden Wahlprüfungsverfahren korrigiert werden können. Mit dieser zeitlichen Verschiebung der Rechtskontrolle auf nach der Wahl soll der reibungslose Ablauf der Wahl sichergestellt werden.

2.3.2 Bundeswahlgeräteverordnung

Bei der Bundeswahlgeräteverordnung handelt es sich gem. § 5 um eine spezialgesetzliche Regelung mit Vorrang vor der BWO für den Einsatz technischer Hilfsmittel bei der Wahlhandlung. Die Vorschriften der BWO, die zur Durchführung des BWahlG dient, greifen also nur, wenn die BWahlGV nicht anderes bestimmt.

Wahlgeräte und Wahlcomputer dürfen gem. § 1 nur bei Wahlen zum Bundestag eingesetzt werden, wenn ihre Bauart zugelassen und ihre Verwendung genehmigt ist. Die Bauartzulassung wird gem. § 2 Abs. 1 vom Bundesministerium des Innern für Wahlgeräte und Wahlcomputer einer bestimmten Bauart auf Antrag des Herstellers erteilt. Durch diese wird die

Eignung von Wahlgeräten und Wahlcomputern einer bestimmten Bauart festgestellt. Die für diese Feststellung notwendige Prüfung wird gem. § 2 Abs. 2 durch die PTB auf Kosten des Antragstellers vorgenommen. Die Richtlinien für die Bauartprüfung sind in Anlage 1 zur BWahlGV festgelegt. Sie geschieht grundsätzlich auf der Basis von Beschreibung, Bauplan, Bedienungsanleitung und einem Muster des Wahlgerätes oder Wahlcomputers. Auf Verlangen der PTB muss der Antragsteller dieser weitere Unterlagen überlassen sowie Einsichtnahme in Entwicklungs- und Herstellungsprozesse gewähren. Der Bauartzulassung folgende Änderungen in der Konstruktion und den technischen Angaben sind gem. § 2 Abs. 3 nur gestattet, wenn die PTB durch eine Nachprüfung nachweist, dass diese keinen Einfluss auf den Vorgang der Abgabe und Zählung der Stimmen besitzen. Eine solche Nachprüfung kann gem. § 2 Abs. 4 auch das Bundesministerium des Innern von der PTB durchführen lassen, wenn die Annahme besteht, dass Änderungen vorgenommen wurden, die Einfluss auf den Vorgang der Abgabe und Zählung der Stimmen besitzen, ohne dass der Hersteller eine solche Nachprüfung oder eine neue Bauartzulassung beantragt hat. Für jedes in Verkehr gebrachte Wahlgerät und jeden Wahlcomputer muss der Hersteller mit einer „Baugleichheitserklärung“ erklären, dass es baugleich mit dem von der PTB geprüften Baumuster ist.

Nach § 3 Abs. 1 kann die Bauartzulassung zurückgenommen werden, wenn sich herausstellt, dass die Voraussetzungen der Bauartzulassung bei ihrer Erteilung nicht vorgelegen haben. Während es sich hierbei um eine Kann-Regelung handelt, erlischt die Bauartzulassung gem. § 3 Abs. 2 automatisch, wenn an Wahlgeräten oder Wahlcomputern oder Teilen von ihnen Änderungen vorgenommen wurden, die Einfluss auf den Vorgang der Abgabe und Zählung der Wählerstimmen besitzen. Die Bauartzulassung kann gem. § 3 Abs. 3 widerrufen werden, wenn die Wahlgeräte- oder Wahlcomputerbauart nicht den Erfordernissen der Durchführung der Wahlen zum Bundestag oder nicht mehr den Rechtsvorschriften für Wahlen zum Bundestag entspricht.

Gem. § 4 Abs. 1 bedarf die Verwendung von Wahlgeräten und Wahlcomputern mit zugelassener Bauart vor jeder Wahl der Genehmigung durch das Bundesministerium des Innern, wobei sie unter Bedingungen erteilt oder mit Auflagen verbunden werden kann.

Auf die Verwendung von Wahlgeräten oder Wahlcomputern in Wahlbezirken muss gem. § 6 in der Wahlbekanntmachung gesondert hingewiesen werden. Die Verwendung beschränkt sich gem. § 7 Abs. 1 auf solche Geräte und Computer, die nach Bestimmung des Wahltages an Hand der Bedienungsanleitungen und Wartungsvorschriften vom Hersteller oder der Gemeinde überprüft worden sind und deren Funktionstüchtigkeit festgestellt worden ist. Bei Wahlcomputern hat die Gemeindebehörde auch für die ordnungsgemäße Verwendung externer Datenträger zu sorgen, wenn diese für die Inbetriebnahme notwendig sind. Notwendig ist außerdem gem. § 7 Abs. 3 eine Einweisung des Wahlvorstandes in die Bedienung der Wahlgeräte und Wahlcomputer.

Der Wahlablauf unter Verwendung von Wahlgeräten und Wahlcomputern ist dabei folgender: Vor Beginn der Stimmabgabe muss der Wahlvorstand unter anderem feststellen, dass sich die Wahlgeräte und Wahlcomputer gem. § 8 Abs. 2 in einem ordnungsgemäßen Zustand befinden, sie dem amtlichen Stimmzettel entsprechend beschriftet sind (gem. § 10 Abs. 1 Nr. 1), sämtliche Zähl- und Speichervorrichtungen für die Stimmabgabe auf Null stehen oder gelöscht sind (Nr. 3) und nicht benötigte Zähl- und Speichervorrichtungen für die Stimmabgabe gesperrt sind (Nr. 4). Danach muss der Wahlvorsteher gem. § 10 Abs. 2 die Wahlgeräte und Wahlcomputer oder dessen Zähl- und Speichervorrichtungen verschließen, wonach diese

bis zum Schluss der Wahlhandlung nicht mehr geöffnet werden dürfen, es sei denn, dass das Gerät oder der Computer zum Zwecke der Fortsetzung der Wahl ohne Gefahr des Bekanntwerdens oder Löschens der bereits abgegebenen Stimmen gemäß Bedienungsanleitung in einen Grundzustand gebracht werden muss.

Die Wahlgeräte und Wahlcomputer müssen gem. § 9 Abs. 1 so aufgestellt werden, dass jede Wählerin und jeder Wähler die Stimme unbeobachtet abgeben können.

Während der Wahl darf ein Wahlgerät oder Wahlcomputer nur nach Freigabe durch ein Mitglied des Wahlvorstandes benutzt werden können. Diese Freigabe darf gem. § 11 Abs. 3 erst erfolgen, wenn die vorherige Wählerin oder der vorherige Wähler die Wahlzelle verlassen haben. Nach § 11 Abs. 4 wird eine Nichtabgabe der Erst- und Zweitstimme als „Nichtwahl“ gewertet und gesondert vermerkt, bei Nichtabgabe einer von beiden Stimmen gilt die nichtabgegebene Stimme als ungültig und wird als solche sofort gezählt. Dafür ist jeweils eine gesonderte Zählliste für die nichtabgegebenen Erst- und Zweitstimmen zu führen. Um nachvollziehen zu können, ob und dass eine Wählerin oder ein Wähler eine oder beide Stimmen nicht abgegeben hat, muss dies von außerhalb der Wahlzelle für den Wahlvorstand überprüfbar sein. Vom Wahlgerät oder Wahlcomputer angezeigte Störungen, die ohne Gefahr eines vorzeitigen Bekanntwerdens oder Löschens der bereits abgegebenen Stimmen behoben werden können, dürfen nach § 11 Abs. 5 gemäß Bedienungsanleitung behoben werden. Bei dadurch nicht behebbaren Störungen kann entweder die Wahl mit einem anderen Wahlgerät oder Wahlcomputer fortgesetzt werden, wenn dies ohne nennenswerte Verzögerung und ohne Gefährdung des Wahlgeheimnisses möglich ist, andernfalls muss die Wahl mit Stimmzetteln fortgesetzt werden. Beides ist in der Wahlniederschrift zu vermerken und das betreffende Wahlgerät oder der betreffende Wahlcomputer ist gegen jede weitere Stimmabgabe zu sperren und die Sperrung, sofern diese rückgängig gemacht werden kann, zu versiegeln.

Nach der Schließung der Wahlhandlung durch die Wahlvorsteherin oder den Wahlvorsteher müssen diese gem. § 12 die Wahlgeräte und Wahlcomputer gegen jede weitere Stimmabgabe sperren und die Sperrung, sofern diese rückgängig gemacht werden kann, versiegeln. Bevor die Stimmen gezählt werden dürfen, muss nach § 13 Abs. 1 eine Zählung der Wählerinnen und Wähler durchgeführt werden. Dies muss zuerst auf der Basis von Wählerinnen- und Wählerverzeichnis und Wahlscheinen geschehen, erst dann sollen die betreffenden Zahlen von den Wahlgeräten und Wahlcomputern abgelesen werden. Bei Abweichungen sind diese in der Wahlniederschrift zu vermerken. Gleiches gilt für das danach nach § 14 vorgenommene Ablesen der Stimmen von Wahlgeräten oder Wahlcomputern, dass gem. Abs. 3 laut erfolgen muss und von deren Richtigkeit sich alle Mitglieder des Wahlvorstandes überzeugen müssen. Auch hier sind Diskrepanzen in der Wahlniederschrift zu vermerken.

Nach der so erfolgten Ermittlung des Wahlergebnisses sind die Wahlgeräte und Wahlcomputer gem. § 15 Abs. 3 zu schließen und zu versiegeln. Diese Sperrung und Versiegelung kann nach § 17 Abs. 3 von der Landeswahlleiterin oder dem Landeswahlleiter erst dann wieder aufgehoben werden, wenn das Wahlergebnis des betreffenden Wahlkreises festgestellt wurde und nur dann, wenn die Zählergebnisse der Wahlgeräte oder Wahlcomputer nicht für ein schwebendes Wahlprüfungsverfahren von Bedeutung sein können. Bis zu diesem Zeitpunkt muss gem. § 16 Abs. 2 auch sichergestellt sein, dass die Wahlgeräte und Wahlcomputer oder deren herausgenommene Stimmenspeicher Unbefugten nicht zugänglich sind.

2.3.3 Richtlinien für die Bauart von Wahlgeräten und Wahlcomputern

Die in Anlage 1 zur BWahlGV festgelegten „Richtlinien für die Bauart von Wahlgeräten“ sind die Grundlage für die von der PTB durchgeführte Prüfung eines Wahlgerätes oder Wahlcomputers. Ihre Erfüllung ist eine notwendige aber keine hinreichende Bedingung für die Erteilung einer Bauartzulassung durch das Bundesministerium des Innern.

Der Inhalt ist auf zwei Bereiche aufgeteilt: Einen allgemeinen Teil A („Gültigkeitsbereich“), in dem allgemeine Anforderungen an Wahlgeräte und Wahlcomputer als solche und ihre Eigenschaften aufgezählt werden, und einen besonderen Teil B („Anforderungen an die Bauart“). Im zweiten Teil werden die konkreten Anforderungen an eine konkrete Bauart eines Wahlgerätes oder Wahlcomputers beschrieben.

Der erste Teil spezifiziert die grundsätzlichen Eigenschaften von Geräten oder Computern, die diese als Wahlgeräte oder Wahlcomputer gem. § 1 BWahlGV qualifizieren. Von ihnen wird dabei verlangt, dass sie die Wahlvorschläge gemäß Stimmzettel darstellen und sowohl die Stimmauswahl und -abgabe im Allgemeinen als auch die Abgabe einer explizit ungültigen Stimme ermöglichen (A. Nr. 1). Sie müssen die Einzelstimmen für Kandidatinnen und Kandidaten, Listen oder die ungültigen Stimmen registrieren (A. Nr. 2), bis zur explizit vorgenommenen Löschung speichern (A. Nr. 5) und zusammenzählen und anzeigen (A. Nr. 4) können. Außerdem müssen sie die Gesamtzahl aller abgegebenen Stimmen speichern und ausgeben können (A. Nr. 3). Weitere Eigenschaften dürfen nur insoweit erfüllt sein, wie sie in unmittelbarem Zusammenhang mit der Wahl stehen.

Der zweite Teil konkretisiert die Eigenschaften und Anforderungen an Wahlgeräte im Hinblick auf ihre Identifizierung (B.1), ihren technischen Aufbau (B.2), ihre Funktionsweise (B.3) und die mitzuliefernden Bedienungsanleitungen (B.4).

Für jedes Wahlgerät und jeden Wahlcomputer, seine Komponenten und die zugehörigen Prüfunterlagen muss die Bauart geeignet identifizierbar sein. So müssen alle Geräte mit Typenschildern ausgestattet sein und für jeden Wahlcomputer muss die installierte Software eindeutig identifizierbar sein.

Der Normgeber hat hier auch explizit den Umfang der Prüfunterlagen definiert, die der Hersteller der PTB zur Verfügung stellen muss. Neben technischen Spezifikationen, Abbildungen und Bedienungsanleitungen sind dies vor allem die vollständigen Konstruktionsunterlagen und Funktionsbeschreibungen, auch jeweils für die Software, die Programmdokumentation nebst Programmentwicklungsdokumentation, der kommentierte Quellcode und das lauffähige Programm selbst.

2.3.4 Technischer Aufbau von Wahlgeräten und Wahlcomputern

Wahlgeräte und Wahlcomputer müssen gemäß B.2.1 in ihrer Konstruktion dem allgemeinen Stand der Technik entsprechen und unter Beachtung der für Systeme mit schwerwiegenden Schadensfolgen bei Fehlverhalten (hohe Kritikalität) anerkannten Regeln der Technik aufgebaut sein.

Das Bundesverfassungsgericht hat in seiner Entscheidung zum Atomgesetz 1978 ausführlich dargelegt, wie der Gesetzgeber die Erkenntnisse und Entwicklungen von Wissenschaft und Technik im Wege einer Normgebung, die damit Schritt hält, rechtlich verbindlich werden

lassen kann. Drei unbestimmte Rechtsbegriffe werden dabei als angemessen[3] betrachtet: die „allgemein anerkannten Regeln der Technik“, der „Stand der Technik“ und der „Stand von Wissenschaft und Technik“.

Dabei stellt die erste Formulierung die geringste rechtliche Anforderung an eine Technik, ein technisches Verfahren oder eine technische Einrichtung. Es genügt, die herrschende Auffassung unter den technischen Praktikern zu ermitteln. Jedoch reicht es nicht, dass sie im Fachschriftum vertreten und der Theorie gebilligt wird, sie muss vielmehr in der Praxis erprobt sein und sich bewährt haben. Der Nachteil dieser Lösung besteht jedoch darin, dass die Rechtsordnung damit stets hinter einer weiterstrebenden technischen Entwicklung herhinkt.

Die zweite Formulierung verlagert den Maßstab für das Erlaubte oder Gebotene an die Front der technischen Entwicklung. Der damit verbundene Nachteil ist die Erschwerung der Feststellung und Beurteilung der maßgeblichen Tatsachen für Behörden und Gerichte, weil es dabei unmittelbar auf das technisch Notwendige, Geeignete, Angemessene und Vermeidbare ankommt. Während die allgemein anerkannten Regeln der Technik außerrechtlich zu beurteilen sind, müssen Behörden und Gerichte für die Ermittlung des Standes der Technik in die Meinungsstreitigkeiten der Techniker eintreten.

Noch weitergehend ist die Formulierung des Standes von Wissenschaft und Technik. Damit erzwingt der Gesetzgeber, dass die neuesten wissenschaftlichen Erkenntnisse zum Maßstab einer Entscheidung gemacht werden und damit, dass die rechtliche Regelung mit der wissenschaftlichen und technischen Entwicklung Schritt hält. Das technisch gegenwärtig Machbare kann demnach keine Grenze der Ansprüche an eine konkrete Technik darstellen.

Die Konstruktion von Wahlgeräten und Wahlcomputern – und dazu zählt bei Wahlcomputern zweifellos auch die Software – muss also grundsätzlich dem neuesten Stand der technischen Entwicklung entsprechen, eingeschränkt möglicherweise durch den Verweis des Normgebers auf den „allgemeinen“ Stand der Technik. Ihr Aufbau muss aus erprobten und bewährten Komponenten und technischen Mechanismen bestehen, wobei der außerrechtliche Maßstab, der bei der Beurteilung an Wahlgeräte und Wahlcomputer angelegt werden soll, durch die Angabe eines spezifischen Systembegriffs konkretisiert wird.

Bei allen Wahlgeräten und Wahlcomputern muss nach B.2.1 eine von unbefugten Dritten vorgenommene Veränderung des technischen Aufbaus erkannt werden können, bei Wahlcomputern zusätzlich auch eine Veränderung der installierten Software.

Wahlgeräte und Wahlcomputer gelten unter anderem dann als funktionssicher, wenn bei Störungen in der Energieversorgung, beim normalen Gebrauch und bei Fehlern in der Bedienung die Funktionsfähigkeit aufrechterhalten und die abgegebenen Stimmen erhalten bleiben (B.2.3). Der Hersteller kann dabei selbst angeben, unter welchen mechanischen, klimatischen und elektromagnetischen Umgebungseinflüssen diese Eigenschaften garantiert werden.

Die Rückwirkungsfreiheit – im Sinne einer Unbeeinflussbarkeit – von Wahlgeräten und Wahlcomputern von nicht zur Bauart gehörenden Komponenten muss nach B.2.4 gegeben sein. Gleiches gilt bei der gleichzeitigen Durchführung mehrerer voneinander unabhängiger Wahlen oder Wahlarten.

[3] Die Alternative wäre eine gesetzliche Fixierung von Standards – z. B. Sicherheitsstandards – durch Aufstellung starrer Regeln, die dann jeweils an die wissenschaftliche und technische Entwicklung angepasst werden müssten und damit – nicht nur durch langwierige Gesetzgebungsverfahren – immer dem jeweiligen Entwicklungsstand hinterherhinken würden.

Elektrisch betriebene Wahlgeräte und Wahlcomputer müssen laut B.2.5 gegen kurzfristige Stromausfälle und Spannungsschwankungen gesichert sein. Bei längeren Stromausfällen müssen sie sich für mindestens 13 Stunden – also die Dauer der Durchführung einer Bundestagswahl – von einer externen Notstromeinheit ohne Auswechslung versorgen lassen können und dafür geeignete Anschlüsse zur Verfügung stellen.

2.3.5 Funktionsweise von Wahlgeräten und Wahlcomputern

Wahlgeräte und Wahlcomputer müssen nach B.3.1 so konstruiert sein, dass sie garantieren, dass eine Wählerin oder ein Wähler nur genau so viele Stimmen abgeben können, wie bei der jeweiligen Wahl möglich sind, wobei dabei die Möglichkeit der Abgabe ungültiger Stimmen gegeben sein muss und die Reihenfolge der Stimmabgabe bei mehreren möglichen Stimmen nicht vom Wahlgerät vorgegeben sein darf.

Die Funktionsfähigkeit von Wahlgeräten und Wahlcomputern muss kontrollierbar sein und bei Wahlcomputern durch eine Funktionsfähigkeitsanzeige unterstützt werden. Funktionsfehler, die während der Durchführung der Wahl auftreten, müssen derart angezeigt werden, dass sie eine Fehlerdiagnose ermöglichen (B.3.2).

Die Anzeige der Wahlmöglichkeiten muss optisch neutral und gut erkennbar sein. Die Zuordnung zwischen dem Wahlvorschlag oder der ungültigen Stimmabgabe und der zugeordneten Bedienvorrichtung muss eindeutig sein, genauso wie die Zuordnung zwischen Bedienvorrichtungen und Zählergebnissen, die auch jeweils gleich numeriert sein müssen (B.3.3).

Für Entgegennahme und Registrierung (Speicherung) der Stimmen und ihre Zählung werden unterschiedliche Anforderungen gestellt. Die Speicherung muss in der Weise mehrfach (redundant) erfolgen, dass mit an Sicherheit grenzender Wahrscheinlichkeit keine abgegebene Stimme verloren geht und somit die Zählung mit hoher Zuverlässigkeit richtig erfolgt. Die Zählung aller abgegebenen Stimmen (pro Wahlvorschlag, als ungültig gekennzeichnete abgegebene Stimmen, Gesamtzahl der Stimmen) muss vollständig, eindeutig und richtig erfolgen und diese dürfen auch nur angezeigt werden. Der Wahlvorstand muss zu jedem Zeitpunkt die Gesamtzahl der abgegebenen Stimmen von außen einsehen können, die anderen Zählergebnisse dürfen hingegen erst nach Schluss der Wahl nach einer besonderen Handlung ablesbar sein. Die Geheimheit der Wahl muss jederzeit gewährleistet sein (B.3.4).

Die vor Beginn der Wahl notwendige Löschung sämtlicher Zähl- und Speicherinhalte für die Stimmenregistrierung muss auf einfache Weise kontrollierbar sein. Wahlgeräte und Wahlcomputer müssen in einen gesicherten Grundzustand gebracht werden können, von dem aus die Geräte so in Betrieb genommen werden können, dass nur eine vom Wahlvorstand bezüglich jeder einzelnen Wählerin und jedes einzelnen Wählers kontrollierbare Abgabe und Speicherung von Stimmen erfolgen kann. Gegen jeden anderen Eingriff müssen Wahlgeräte und Wahlcomputer durch Mehrfachverschluss gesichert sein. Dabei stellt die Verordnung klar, dass damit Schlösser gemeint sind, die unterschiedliche Schließungen besitzen. Nach der Wahl müssen Wahlgeräte und Wahlcomputer gegen Abgabe und Speicherung von Stimmen gesperrt werden können, während die Möglichkeit des Ablesens der Ergebnisse freigegeben werden können muss, ohne dass dabei Ergebnisse geändert oder gelöscht werden können. Die Sperre zur Löschung muss gesondert entriegelt werden (B.3.5).

Die Wählerin oder der Wähler darf ein Wahlgerät oder einen Wahlcomputer erst dann nutzen können, wenn diese der Wahlvorstand zur Stimmabgabe freigegeben hat. Die Geräte müssen sich nach der Registrierung der Stimmabgabe selbsttätig wieder sperren, wobei diese Sperrung sowohl für den Wahlvorstand als auch für die Wählerin oder den Wähler erkennbar sein muss (B.3.6).

Bedienungshandlungen, Fehlgriffe und absichtliche Eingriffe dürfen keine Störungen oder gar Zerstörungen zur Folge haben, es sei denn, sie wurden gewaltsam oder unter Anwendung besonderer Hilfsmittel vorgenommen.

2.3.6 Anforderungen für Wahlcomputer-Software

Die PTB hat für die Software von Wahlcomputern eine spezielle Anforderungsliste (Phy07d) aus den Richtlinien nach Anlage 1 der BWahlGV abgeleitet. Darin werden die in den Richtlinien festgelegten Anforderungen an Wahlgeräte und Wahlcomputer durch Anforderungen an die Software von Wahlcomputern weiter konkretisiert.

Zu den konkretisierten Anforderungen gehört die geforderte Unmöglichkeit jeder Änderung der Funktion der Bedienelemente, also der Zuordnung zwischen einzelnen Tasten und ihren Funktionen, während der Wahl. Die allgemeinen Richtlinien forderten demgegenüber nur, dass die Zuordnung zwischen Bedienelementen und Funktionen eindeutig ist.

Im Gegensatz zu den Richtlinien, nach denen Wahlcomputer die Stimmen sowohl registrieren (speichern) als auch zusammenzählen und beide redundant speichern können müssen, heißt es in der Anforderungsliste der PTB: „Die Registrierung oder Zählung der Stimmen muss mit [...] Redundanz erfolgen."

Während nach den Richtlinien für die Software als Teil der Konstruktion eines Wahlcomputers insgesamt gilt, dass sie dem allgemeinen Stand der Technik entsprechen soll, gilt nach der Anforderungsliste der PTB der Stand der Technik als Maßstab für die Software, für ihre Entwicklung jedoch nur, dass diese unter Beachtung der anerkannten Regeln der Softwareentwicklung und auf der Grundlage eines definierten Vorgehensmodells erfolgen muss.

Weiterhin fordert die PTB, dass eine statische Code-Analyse des Programms keine problematischen Konstrukte sichtbar machen darf, wobei der Term „problematische Konstrukte" ein unbestimmter Rechtsbegriff ist und daher – gemäß der Anforderung, dass die Software dem Stand der Technik entsprechen soll – am neuesten Stand der technischen Entwicklung zu messen ist. Als dem der Programmierung zugrundeliegenden Paradigma wird die strukturierte Programmierung gefordert, wobei gleichzeitig alle Daten gekapselt sein müssen.

2.4 Anforderungen an den Umgang mit Wahlgeräten und Wahlcomputern

Im folgenden Abschnitt sollen die rechtlichen Anforderungen an den Umgang mit Wahlgeräten und Wahlcomputern vor, während und nach einer Wahl dargestellt werden. Hier wird sich auf die im BWahlG, in der BWO und in der BWahlGV kodifizierten Regelungen beschränkt. Auf bisher nicht gesetzlich fixierte Umgangsregeln, die sich vor allem in den letzten Jahren aus der verstärkten öffentlichen Diskussion über Sicherheitsfragen ergeben

haben, wird im dritten Teil der Arbeit im Rahmen der Sicherheits- und Diskursgeschichte eingegangen.

Die Wahl beginnt im weiteren Sinne mit ihrer Bekanntmachung. In dieser müssen die Gemeindebehörden laut § 6 BWahlGV darauf hinweisen, dass und in welchen Wahlbezirken Wahlgeräte und Wahlcomputer zum Einsatz kommen. Dem ist – neben dem Musterstimmzettel – eine Abbildung hinzuzufügen mit der Benutzerschnittstelle der eingesetzten Geräte und der gerätespezifischen Darstellung der Wahlvorschläge.

Vor Beginn des Wahltages sind alle Wahlgeräte und Wahlcomputer, die zur Wahl eingesetzt werden sollen, gemäß § 7 Abs. 1 BWahlGV vom Hersteller oder von der Gemeinde zu überprüfen. Diese Prüfung beschränkt sich auf die Funktionstüchtigkeit der Geräte und richtet sich nach den am Wahltag geltenden gesetzlichen Bestimmungen. Eine weitere Überprüfung kann nach Abs 2 durch die Kreiswahlleiterin, den Kreiswahlleiter oder von diesen Beauftragten durchgeführt werden und beschränkt sich nicht nur auf die eingesetzten Wahlgeräte und Wahlcomputer sondern kann auch eventuell notwendige externe Datenträger umfassen. Abgesehen von dieser möglichen Zusatzprüfung unterliegen die externen Datenträger in der Regel keiner Überprüfung vor einer Wahl. Abs. 3 verpflichtet die Gemeindebehörden zur Einweisung der Wahlvorstände in die Bedienung der Wahlgeräte und Wahlcomputer.

Vor Beginn der Wahlhandlung muss die Gemeindebehörde der Wahlvorsteherin oder dem Wahlvorsteher gemäß § 8 Abs. 1 BWahlGV die benötigten Wahlgeräte oder Wahlcomputer nebst den jeweils dazugehörenden Schlüsseln und dem sonstigen Zubehör übergeben. Ein genauer Zeitpunkt dieser Übergabe ist nicht festgelegt. Für den Aushang im Wahllokal erhalten die Wahlvorstände eine der oben genannten Abbildungen mit der Darstellung der Benutzerschnittstelle sowie eine Anleitung zur Stimmabgabe für die Wahlberechtigten. Zum Gebrauch durch den Wahlvorstand werden diesem zusätzlich Bedienungsanleitungen für die verwendeten Wahlgeräte und Wahlcomputer und eine Baugleichheitserklärung des Herstellers übergeben. Zuletzt erhält der Wahlvorstand Material zum Versiegeln jedes Wahlgerätes, Wahlcomputers und des Zubehörs.

Die Aufstellung der Wahlgeräte und Wahlcomputer im Wahllokal hat nach § 6 Abs. 1 BWahlGV so zu erfolgen, dass jede Wählerin und jeder Wähler unbeobachtet abstimmen kann.

Zur Eröffnung der Wahlhandlung und vor Beginn der Stimmabgabe muss der Wahlvorstand gemäß § 10 Abs. 1 BWahlGV feststellen und in der Wahlniederschrift nach Anlage 2 BWahlGV – oder Anlage 3 für Europawahlen – protokollieren, welche Wahlgeräte und Wahlcomputer zum Einsatz kommen, indem deren Gerätenummern notiert werden, und dass sich die Geräte in einem ordnungsgemäßen Zustand befinden. Auch die Übereinstimmung der gerätespezifischen Darstellung der Wahlvorschläge mit dem amtlichen Stimmzettel muss protokolliert werden. Zuletzt ist zu überprüfen, ob alle Zähl- und Speichervorrichtungen für die Stimmabgabe auf Null gestellt oder gelöscht sind oder, soweit sie nicht benötigt werden, gesperrt sind und ob die Behälter für die Aufnahme von Wahlmarken leer sind. Auch das ist im Protokoll zu vermerken.

Nach der Überprüfung und Protokollierung des Zustandes der eingesetzten Wahlgeräte und Wahlcomputer müssen Wahlvorsteherinnen und Wahlvorsteher die eingesetzten Wahlgeräte oder Wahlcomputer oder deren Zähl- und Speichervorrichtungen laut § 10 Abs. 2 BWahlGV verschließen. Die dabei verwendeten Schlüssel sind getrennt voneinander bis zur Beendigung

der Wahlhandlung von Wahlvorsteherin oder Wahlvorsteher und anderen Mitgliedern des Wahlvorstandes aufzubewahren.

Danach eröffnet der Wahlvorstand die Wahl.

Nachdem sich Wählerinnen und Wähler gegenüber dem Wahlvorstand als wahlberechtigt ausgewiesen haben und im Wählerverzeichnis abgezeichnet wurden, muss ein Mitglied des Wahlvorstandes das Wahlgerät oder den Wahlcomputer gemäß § 11 Abs. 3 BWahlGV zur Stimmabgabe freischalten, wenn die oder der vorherige Wahlberechtigte die Wahlzelle verlassen hat. Erst danach kann die oder der Wahlberechtigte die Wahlzelle betreten und ihre oder seine Stimme oder Stimmen abgeben. Die Stimmabgabe muss dabei vom Wahlvorstand vermerkt werden. Nach Abgabe der Stimme sperrt sich das Wahlgerät oder der Wahlcomputer, wobei die Sperrung durch den Wahlvorstand von außen überprüft werden kann. Bei Nichtabgabe einer oder mehrerer Stimmen muss dies vom Wahlvorstand gesondert gezählt werden (§ 11 Abs.4 BWahlGV). Sollten Funktionsstörungen auftreten, die ohne Gefahr eines vorzeitigen Bekanntwerdens oder Löschens der bereits abgegebenen Stimmen behoben werden kann, ist dies vom Wahlvorstand nach § 11 Abs. 5 BWahlGV gemäß Bedienungsanleitung vorzunehmen. Kann eine solche Gefahr nicht ausgeschlossen werden, kann der Wahlvorstand beschließen, mit einem anderen Wahlgerät oder Wahlcomputer die Wahl fortzusetzen, wenn dies ohne Verzögerung oder Gefährdung des Wahlgeheimnisses möglich ist. Andernfalls muss die Wahl mit Stimmzetteln fortgesetzt werden. In jedem Fall ist jede Störung zu protokollieren.

Nach Schließung der Wahl muss die Wahlvorsteherin oder der Wahlvorsteher laut § 12 BWahlGV jedes Wahlgerät, jeden Wahlcomputer und jeden Stimmenspeicher gegen jede weitere Stimmabgabe sperren. Weiterhin legt die BWahlGV fest, dass die Sperrung zusätzlich versiegelt werden muss, falls sie rückgängig gemacht werden kann. Demgegenüber verlangt Nr. 2.10 der Anlage 2 der BWahlGV die bedingungslose Versiegelung der Sperrung.

Vor der Ermittlung des Wahlergebnisses ist nach § 13 BWahlGV die Zahl der Wählerinnen und Wähler anhand des Wählerverzeichnisses festzustellen. Erst danach dürfen von den Wahlgeräten und Wahlcomputern die Zahlen der abgegebenen Erst- und Zweitstimmen abgelesen werden. Diese Zahlen müssen nun miteinander vergleichen werden. Eventuell auftretende Abweichungen müssen protokolliert und, soweit möglich, erläutert werden. Anschließend sind die Wahlgeräte und Wahlcomputer zur Zählung freizugeben, die Zahlen der für die jeweiligen Bewerberinnen und Bewerber abgegebenen Stimmen sowie die ungültigen Erst- und Zweitstimmen zu protokollieren und laut zu verlesen. Auch dabei müssen eventuell auftretende Diskrepanzen zwischen den einzelnen Werten und Summen in der Wahlniederschrift vermerkt werden.

Nach der Ermittlung des Wahlergebnisses ist jedes Wahlgerät und jeder Wahlcomputer gemäß § 15 Abs. 3 BWahlGV zu verschließen und zu versiegeln. Wenn eine Entsperrung im verschlossenen Zustand nicht möglich ist und die Stimmenspeicher herausnehmbar sind, dann genügt es, die Schlüssel und die Speicher in ein gesondertes Behältnis zu verpacken und dieses zu kennzeichnen und zu versiegeln.

Bis zur Aufhebung der Sperrung und Versiegelung der Wahlgeräte, Wahlcomputer und Stimmenspeicher dürfen diese Unbefugten nicht zugänglich sein. Die Verantwortung dafür tragen nach § 16 BWahlGV die Wahlvorsteherinnen und -vorsteher, die Gemeindebehörden und die Kreiswahlleiterinnen und -wahlleiter.

2.4.1 Probleme und Regelungslücken

Bei der Betrachtung des Regelwerkes zum Umgang mit Wahlgeräten und Wahlcomputern fallen verschiedene nicht gelöste Probleme auf. Die Regelungslücken betreffen dabei vor allem Fragen zur Sicherheit. Eine kurze Übersicht soll dies verdeutlichen. Dabei ist zu beachten, dass die kodifizierten Regeln zwar die rechtliche Basis für den Umgang mit Wahlgeräten und Wahlcomputern darstellt, das BMI – oder für Landtags- oder Kommunalwahlen auch die Innenministerien der Länder – jedoch durch Verwendungsgenehmigungen im Einzelfall Regelveränderungen und -erweiterungen vornehmen können. Diese werden, wie bereits angesprochen, im dritten Teil dieser Arbeit genauer und in ihrem zeitlichen Zusammenhang mit Entwicklungen des Sicherheitsdiskurses betrachtet.

Die rechtlichen Vorschriften in BWahlG und BWahlGV enthalten keine Regelungen zum Umgang mit und zur Lagerung von Wahlgeräten, Wahlcomputern, externen Datenträgern und Speichervorrichtungen zwischen den einzelnen Wahlen. Der Normgeber und die inhaltlich zuarbeitende PTB haben es versäumt, gesetzliche Regelungen für eine sichere Verwahrung der betreffenden Geräte zwischen den Wahlen zu erlassen. Durch das Fehlen einer Überprüfung der technischen Unversehrtheit der Geräte vor Beginn einer Wahl können Wahlvorstände gegenüber Wählerinnen und Wählern die Integrität der Wahlergebnisse, die mit diesen Geräten produziert werden, nicht garantieren. Bei Wahlcomputern kommt erschwerend hinzu, dass die Wahlvorstände gesetzlich nicht verpflichtet sind, die auf den Wahlcomputern laufende Software zu verifizieren.[4] Regelungen, die eine Überprüfung der Zuordnung zwischen den einzelnen Bedienvorrichtungen und den zugeordneten Zähl- und Speichervorrichtungen erzwingen, existieren nicht. Den Wahlberechtigten kann daher nicht einmal garantiert werden, dass ihre Stimmen überhaupt gezählt werden.

Zusammenfassend lässt sich konstatieren, dass die Erfüllung der technischen Anforderungen an Wahlgeräte und Wahlcomputer, die sich aus der derzeit gültigen BWahlGV ergeben, nicht ausreicht, um eine demokratische und manipulationssichere Wahl zu gewährleisten.

[4] Über die technischen Probleme mit der Verifikation der verbauten Hardware und der darauf laufenden Software beschäftigt sich der zweite Teil dieser Arbeit ausführlicher.

3 Sicherheit

Der zweite Teil der Arbeit betrachtet die Anforderungen, die an die Sicherheit demokratischer Wahlen zu stellen sind. Grundlage dieser Sicherheitsanalyse sind die verfassungsrechtlichen und einfachgesetzlichen Vorgaben sowohl an Wahlen im Allgemeinen als auch an Wahltechniken im Besonderen. Dazu werden im ersten Abschnitt die Schutzziele definiert, die bei der Durchführung von Wahlen von Belang sind. Im zweiten Abschnitt wird betrachtet, welche Angriffe oder Angriffsarten auf Wahlen, deren politisches und gesellschaftliches Umfeld und daran Beteiligte durchgeführt werden können. Dies geschieht vor dem Hintergrund der Intentionen und Ziele, die Angreiferinnen und Angreifer verfolgen können. Aus den dabei gewonnenen Informationen wird ein Bedrohungsmodell erstellt, mit dem dann für die verschiedenen Wahltechniken Risikoanalysen durchgeführt werden. Diese beschränken sich dabei in diesem Abschnitt auf die Möglichkeiten zur Entdeckung der beschriebenen Angriffe zum jeweiligen Angriffszeitpunkt und während des Wahlablaufes. Im folgenden Abschnitt, dem dritten, wird die Analyse dann auf die Erkennbarkeit und Nachvollziehbarkeit dieser Angriffe zu einem Zeitpunkt nach der Wahl ausgedehnt. Nach einer kurzen Beschreibung der allgemeinen Anforderungen an Sicherheitsregeln werden im vierten Abschnitt ausgewählte Probleme und Fehler in den derzeitigen Regelwerken aufgezeigt, die beschriebene Angriffe erleichtern oder deren Entdeckung und Verhinderung erschweren. Der letzte Abschnitt wird am Beispiel des Digitalen Wahlstift-Systems eine Einführung in die Common Criteria (CC) geben und dabei das von der Prüfstelle für IT-Sicherheit des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI) dafür ausgearbeitete Schutzprofil (VV07) anhand der in diesem Teil der Arbeit aufgeworfenen Sicherheitsfragen bewerten.

Für die theoretischen Überlegungen zu den Sicherheitsbegriffen, ihren Inhalten und ihren Grenzen, zu Vorgehensweisen bei der Analyse und Bewertung von Sicherheit und Sicherheitsproblemen, -bedrohungen, -risiken und -politiken stützt sich die Arbeit vorwiegend auf die Ausführungen von Anderson (And01) und Schneier (Sch04). Die praktischen Überlegungen zu möglichen Angriffszielen, Angriffen und Typen von Angreiferinnen und Angreifern entstammen entweder konkreten Ereignissen der Vergangenheit, Diskussionen über Sicherheitsfragen im Rahmen universitärer oder außeruniversitärer Veranstaltungen oder mit Mitstudentinnen und Mitstudenten oder eigenen Überlegungen, was ich selbst als möglicher Angreifer beabsichtigen oder durchführen würde.

Bei der Betrachtung und Bewertung der Sicherheit von Techniken oder Verfahren müssen drei Sicherheitsmechanismen unterschieden werden, die gleichwohl nicht streng voneinander getrennt werden können, sich überlappen und aufeinander einwirken: Schutz-, Erkennungs- und Reaktionsmechanismen (Sch04, S. 8, 280f.). Dabei sollen Schutzmechanismen die Sicherheit von Systemen durch die Verhinderung oder Abweisung von Angriffen garantieren. Wenn sie stark genug sind und damit ihre Sicherheitsgarantien tatsächlich einlösen können, bedarf es nicht unbedingt ausgefeilter Erkennungs- und Reaktionsmechanismen. Andererseits müssen diese gerade dann besonders gut funktionieren, wenn die Schutzmechanismen nur schwach oder gar nicht vorhanden sind. In Einzelfällen ist die Erkennbarkeit eines Angriffes, und damit auch eine eventuelle Reaktion darauf, grundsätzlich ausgeschlossen. Ein Beispiel für nicht erkennbare Angriffe ist das Mitlesen von E-Mails, vor allem außerhalb eines eigenen, möglicherweise geschützten, Netzwerkes. In einem solchen Fall müssen die Schutzmechanismen, wie Verschlüsselungsalgorithmen, deren Implementationen oder die Geheim-

haltung von Schlüsseln, in der Lage sein, die Sicherheit allein zu garantieren. Weil nach Schneier (Sch04, S. 9) Schutzmechanismen niemals perfekt sein können, sind Erkennungs- und Reaktionsmechanismen immer notwendig. Und auf Angriffe kann nur dann reagiert werden, wenn sie erkennbar sind und tatsächlich erkannt werden oder wurden.

Von der angesprochenen Sicherheit im Sinne eines Schutzes von Systemen, Daten, Personen und Handlungen vor Ausspähung, Manipulationen und anderen unberechtigten Eingriffen (*security*) ist die Sicherheit im Sinne der Garantierung einer bestimmten Funktionalität und des Schutzes vor Fehlern und Ausfällen (*safety*) zu trennen. „Sicherheit“ ist somit begrifflich mehrfach belegt. Der Fokus dieser Arbeit liegt ganz klar auf ersterem, der *security*. Fragen zur *safety* werden daher nur in einem sehr begrenzten Umfang behandelt.

3.1 Schutzziele bei Wahlen

Die Schutzziele ergeben sich einerseits aus den einschlägigen verfassungsrechtlichen und einfachgesetzlichen Regelungen und andererseits aus immanenten Eigenschaften und systemischen Beschränkungen der eingesetzten nichttechnischen und technischen Systeme und der zur Anwendung kommenden Verfahren.

Zum Schutz des verfassungsrechtlich verankerten Demokratieprinzips muss jede eingesetzte Wahltechnik allen Wahlberechtigten verständlich sein. Wahltechniken, deren Komplexität oder technische Ausgestaltung nur von einigen wenigen Expertinnen und Experten begriffen und nachvollzogen werden können, widersprechen dem Geist der Demokratie im Sinne einer Herrschaft des Volkes fundamental. Außerdem müssen Funktionalität und Funktionssicherheit der Wahltechnik und deren Integrität sowie die Integrität aller abgegebenen Stimmen sichergestellt werden. Alle weiteren Schutzziele, die sich aus dem Demokratieprinzip ergeben, wie ein demokratisches Wahlsystem und Wahlverfahren und die freie Konkurrenz der Ideen, die sich auch in den Zulassungsbedingungen für Kandidaturen äußert, liegen außerhalb des Fokus dieser Arbeit.

Eine Wahltechnik darf zum Schutz des Grundsatzes der Allgemeinheit der Wahl nicht auf technischen oder organisatorischen Voraussetzungen beruhen, die nicht von allen Wahlberechtigten erfüllt werden oder erfüllt werden können. Eine Wahltechnik, die selbst für die Feststellung der Wahlberechtigungen von potentiellen Wählerinnen und Wählern zuständig ist, indem sie diese zum Beispiel anhand ihrer Fingerabdrücke identifizieren soll, würde nach (Bus07) zwischen drei und elf Prozent der Betroffenen von der Wahl ausschließen und demnach einen Verstoß gegen den Grundsatz der allgemeinen Wahl darstellen. Auch eine Wahltechnik, die zur Benutzung von Wahlberechtigten besondere Kenntnisse oder Fähigkeiten verlangt oder schlicht von einem Großteil der Betroffenen in ihrer Funktionsweise nicht verstanden wird, kann nicht verfassungsgemäß sein. Zuletzt verstößt eine Wahltechnik gegen den Grundsatz der Allgemeinheit der Wahl, wenn sie unter Verwendung von Daten wie Geschlecht oder Alterskohorte, die im Zusammenhang mit der Durchführung der Wahlstatistik aufgenommen werden, die abgegebenen Stimmen bestimmter Bevölkerungskreise nicht zählt, also nicht rückwirkungsfrei ist.

Der Schutz der Unmittelbarkeit der Wahl fordert vor allem die Sicherstellung der Integrität der verwendeten Wahltechnik, da jede Manipulation der abgegebenen Stimmen immer auch einen Verstoß gegen den Unmittelbarkeitsgrundsatz darstellt. Dieses Schutzziel folgt auch unmittelbar aus der Strafbarkeit der Wahlfälschung nach § 107a StGB. Auch das Schutzziel

der Funktionssicherheit der Wahltechniken folgt aus dem Unmittelbarkeitsgrundsatz. Andere Schutzziele wie der Ausschluss von Wahlmännern und -frauen unterfallen als wahlsystemspezifisch nicht dem Fokus der Arbeit.

Mit dem Schutz des Wahlgeheimnisses ist, wie bereits gezeigt, unmittelbar auch der Schutz der Wahlfreiheit verbunden. Die Vertraulichkeit der Stimmabgabe gegenüber allen Dritten ist primäres Ziel der geheimen Wahl. Zur Verhinderung von Stimmenkauf gilt das Wahlgeheimnis auch für die Wählerinnen und Wähler selbst. Sie dürfen also nicht in der Lage sein, Dritten gegenüber nachzuweisen, wie sie gewählt oder nicht gewählt haben. Das Verbot, in irgendeiner Form Zwischenergebnisse berechnen zu können, schützt im engeren Sinne das Wahlgeheimnis, weil sonst aus der Differenz direkt aufeinanderfolgender Zwischenergebnisse Wahlentscheidungen rekonstruiert werden können. Im weiteren Sinne schützt dieses Verbot auch die Freiheit der Wahl, indem nachfolgende Wählerinnen und Wähler nicht von Wahlergebnisvorhersagen bei ihren Wahlentscheidungen beeinflusst werden können. Diese Schutzziele folgen auch gleichzeitig aus den Strafnormen der §§ 107c, 108 und 108b StGB (Verletzung des Wahlgeheimnisses, Wählernötigung und Wählerbestechung).

Im Zusammenhang mit Wahltechniken bezieht sich der Schutz der Wahlgleichheit vor allem auf den Schutz der Gleichheit des Zählwertes. Allen Wählerinnen und Wählern muss dabei garantiert werden, dass sie ihre Stimme oder Stimmen abgeben können und dass diese auch gespeichert und gezählt werden. Gleichzeitig muss sichergestellt werden, dass sie nicht mehr als die zulässige Höchstzahl an Stimmen im Laufe einer Wahl abgeben können oder dass mehr als die abgegeben Stimmen gespeichert werden. Die Integrität der abgegeben Stimmen muss gegen alle Versuche, sie zu ändern oder zu löschen, geschützt werden. Auch die Produktion zusätzlicher Stimmen muss ausgeschlossen werden. Alle abgegeben Stimmen müssen entweder als gültige oder als ungültige korrekt gespeichert und gezählt werden und das Ergebnis muss korrekt ermittelt werden. Die durchgehende Verfügbarkeit der Wahltechnik muss während des gesamten Wahlablaufes sichergestellt werden, andernfalls ist zumindest zu garantieren, dass im Fehlerfall weder Stimmen gelöscht oder geändert oder neue Stimmen produziert werden. Wahlsystem und Wahlkreiseinteilung, die auch dem Grundsatz der Wahlgleichheit folgen müssen, liegen als wahltechnikunabhängige Schutzziele nicht im Fokus dieser Arbeit.

Wie bereits ausführlich in (Poh07, S. 28f.) dargelegt, können weder Wahlgeräte noch Wahlcomputer, so wie sie bisher in der BRD zugelassen sind und Verwendung finden, die Öffentlichkeit der Stimmenauszählung sicherstellen. Allenfalls in Verbindung mit einem Voter Verifiable Paper Audits Trail (VVPAT), bei dem ausschließlich die von Wählerinnen und Wählern überprüfbaren Papierbelege zur Ermittlung des Wahlergebnisses herangezogen werden, können diese Geräte zur Erstellung einer – möglicherweise besonders genauen – Wahlergebnisvorhersage dienen.

Zur Sicherstellung des durchgehend amtlichen Charakters einer Wahl muss jede eingesetzte Wahltechnik genauso wie jeder einzelne ihrer Bestandteile sicher und eindeutig identifiziert werden können. Wer immer Zutritt oder Zugang zu oder Zugriff auf diese Wahltechnik haben will, muss sich authentifizieren, ob es sich dabei um Wählerinnen und Wähler, Mitglieder des Wahlvorstandes, Mitarbeiterinnen und Mitarbeiter der Gemeindebehörden oder der Hersteller oder andere berechtigte Personen handelt. Abgesehen von Wählerinnen und Wählern während ihrer Stimmabgabe müssen jedes Handeln und die dabei handelnden Personen nicht

abstreitbar protokolliert werden. In Bezug auf die eingesetzte Wahltechnik schützen diese Anforderungen auch gegen die nach § 108a StGB strafbare Wählertäuschung.

Grundsätzlich die gleichen Anforderungen werden an Wahltechniken gestellt, um sowohl die jederzeitige als auch vor allem die nachträgliche Überprüfbarkeit aller Abläufe vor, während und nach einer Wahl garantieren zu können, die im Zusammenhang mit den Wahltechniken stehen. Dazu zählen also die sichere und eindeutige Identifizierbarkeit aller Bestandteile der eingesetzten Wahltechniken und die Nachprüfbarkeit aller an oder mit den Wahltechniken vorgenommenen Handlungen unter Beachtung der Nichtrekonstruierbarkeit der Wahlentscheidungen einzelner Wählerinnen und Wähler. Die Ermittlung der Wahlergebnisse muss vollständig nachvollziehbar sein. Die Notwendigkeit einer jederzeit möglichen Kontrollierbarkeit fordert darüber hinaus sowohl die Funktionssicherheit der eingesetzten Wahltechniken als auch ihre Rückwirkungsfreiheit. Zuletzt muss jede Wahltechnik zu ihrer Überprüfbarkeit grundsätzlich deterministisch arbeiten. Vorhandene nichtdeterministische Einzelschritte, die zum Schutz des Wahlgeheimnisses notwendig sind, müssen in jedem Fall die Eigenschaft der Atomarität[5] erfüllen.

Die Wahlbehinderung und die Fälschung von Wahlunterlagen, strafbar nach §§ 107 und 107b StGB, sind nicht wahltechnikspezifisch durchführbar. Aus ihnen lassen sich daher keine Schutzziele ableiten, die im Fokus dieser Arbeit liegen. Sie werden daher hier nicht weiter betrachtet.

Die dabei aus den rechtlichen Anforderungen abgeleiteten Schutzziele lassen sich nun den allgemeinen Bereichen *safety* und *security* zuordnen. Zur *safety* gehören dabei die Schutzziele Funktionalität, Funktionssicherheit, Verlässlichkeit, Verfügbarkeit und Verständlichkeit. Unter den Begriff der *security* fallen hingegen die Schutzziele Integrität, Identifizierbarkeit, Authentizität, Verbindlichkeit, Überprüfbarkeit, Rückwirkungsfreiheit, Vertraulichkeit und das Zwischenergebnisverbot.

3.2 Angriffe

Angriffe auf Wahlen sind vielfältig. Sie können vor, während oder nach Wahlen stattfinden. Aus der Sicht derjenigen, die verfassungs- und rechtmäßige Wahlen sicherstellen wollen, sind alle Handlungen, die zu Wahlfehlern führen oder führen können, als Angriffe zu betrachten. Zusätzlich sind Unterlassungen dann als Angriffe zu werten, wenn für die betreffenden Personen eine gesetzliche Handlungspflicht besteht, der sie nicht nachkommen. Angriffe können dabei sowohl fahrlässig als auch vorsätzlich ausgeführt werden. Der Angriffsbegriff muss also, wenn es um den Schutz von Wahlen geht, als sehr umfassend betrachtet werden.

Einerseits lassen sich mögliche Angriffe direkt aus den Regelungen des Strafgesetzbuches ableiten, die selbst bereits die Ergebnisse der Erfahrungen vergangener Angriffe sind. Andererseits speisen sich Angriffe aus den politischen Zielen möglicher Angreiferinnen und Angreifer, zu deren Erreichen die Begehung strafbarer Handlungen nur Mittel zum Zweck ist.

Zur übersichtlichen Darstellung möglicher Angriffe und Angriffsvektoren dienen die von Schneier in (Sch04, S. 318ff.) entwickelten Angriffsbäume, wobei aus Platzgründen die

[5] Die Einzelschritte, gleich ob sie noch weiter unterteilt werden können oder nicht, werden als logische Einheiten betrachtet. Sie können nur entweder erfolgreich verlaufen oder vollständig fehlschlagen.

1. Ziel
   1. Teilziel 1 (Oder)
   2. Teilziel 2

1. Ziel
   1. Teilziel 1 (Und)
   2. Teilziel 2

Abbildung 1: Oder- und Und-Relation für Angriffsbäume

Schriftform nach (Sch04, S. 324ff.) genutzt wird. Sie ermöglichen gleichzeitig eine methodische Herangehensweise an die Beschreibung von Angriffen sowie Sicherheitsberechnungen und -vergleiche. In der Baumdarstellung erscheint das Angriffsziel als Wurzelknoten, in der Listendarstellung als erstes Element der Aufzählung. Mögliche Teilziele und Angriffswege werden jeweils als Kindknoten oder als Unterelemente dargestellt. Angriffsbäume können selbst auch nur einen Teilausschnitt einer komplexen Angriffsbetrachtung enthalten. In diesem Fall sind die Wurzelknoten eines Angriffsbaumes die Blattknoten eines anderen. Entsprechend können Listen Unterelemente anderer Listen sein. Die Kanten zwischen den einzelnen Knoten können in zwei Ausformungen auftreten, entweder als Oder- oder als Und-Relation. Abbildung 1 zeigt die Schreibweisen dieser Relationen in Listendarstellungen. In der Oder-Relation muss mindestens ein beliebiges Teilziel erreicht werden, um das jeweils zugehörige Angriffsziel im Elternknoten zu erreichen ($Z = T_1 \vee T_2 \vee \cdots \vee T_n$). Dementsprechend müssen in einer Und-Relation alle Teilziele errungen werden, um den Angriff auf das jeweilige Oberziel erfolgreich durchzuführen ($Z = T_1 \wedge T_2 \wedge \cdots \wedge T_n$). Mit Hilfe von Metriken und Werten, die einzelnen Teilzielen zugeordnet werden, können Angriffsbäume zur Berechnung von Sicherheitseigenschaften verschiedener Teilbereiche komplexer Systeme verwendet werden. Mögliche Metriken sind dabei vor allem Aufwand, sowohl zeitlich, finanziell oder technisch, erforderliches Wissen auf Seiten der Angreiferinnen und Angreifer, Erfolgs- und Entdeckungswahrscheinlichkeit. Auch die Frage, ob bestimmte Angriffe nur von Innentäterinnen und -tätern ausgeführt werden können, lässt sich mit Hilfe von Angriffbäumen modellieren. So es sich um einfache Kosten handelt, können diese in Und-Relationen einfach als Summe dargestellt werden ($K(Z) = \sum K(T_n)$). Für Oder-Relationen gilt dementsprechend, dass die Kosten zur Erreichung des Angriffszieles dem Minimum der Kosten aller Teilziele entsprechen ($K(Z) = \min(K(T_n))$). Für komplexere Kostenfunktionen müssen die Formeln entsprechend angepasst werden.

Grundlage für die Betrachtung möglicher Angriffe ist immer die Seite der Angreiferinnen und Angreifer. Sie, und nicht die Verteidigerinnen und Verteidiger, entscheiden, an welchen Stellen Angriffe ausgeführt werden. Ihre verschiedenen Kenntnisse, Fähigkeiten und finanziellen Mittel, Zugangsmöglichkeiten, Risikofreudigkeiten und Intentionen determinieren ihre Entscheidung bei der Wahl zwischen verschiedenen möglichen Angriffen (siehe Abbildung 2). Die erste Unterscheidung muss hier also zwischen fahrlässig und vorsätzlich durchgeführten Angriffen vorgenommen werden. Während fahrlässig ausgeführte Angriffe gerade kein originäres Ziel verfolgen, lassen sich für vorsätzlich begangene Angriffe verschiedene Intentionen herauskristallisieren. Der offensichtlichste Angriff verfolgt das Ziel, das Wahlergebnis zu manipulieren. Dies kann entweder zum eigenen Vorteil oder zum Vor- oder Nachteil von Dritten geschehen. Dabei ist der Manipulationsbegriff weit zu verstehen und umfasst alle Einflussnahmen, die zu einem Wahlergebnis führen, das sich von einem sol-

1. Angreiferin oder Angreifer handelt:
   1. fahrlässig (Oder)
   2. vorsätzlich und will:
      1. Wahlentscheidung zu eigenen Gunsten oder zu Gunsten oder Ungunsten Dritter beeinflussen (Oder)
      2. Wählerinnen oder Wähler erpressen (Oder)
      3. die eigene Stimme verkaufen (Oder)
      4. Vertrauen in Wahl, Politik und Demokratie unterminieren (Oder)
      5. Vertrauen in einzelne oder mehrere Parteien unterminieren (Oder)
      6. Vertrauen in einzelne oder mehrere Wahltechniken unterminieren

Abbildung 2: Intentionen von Angreiferinnen und Angreifern

chen unterscheidet, das den Wählerwillen umfassend informierter Wählerinnen und Wähler in einer freien Wahl abbildet. Ein durch solche Manipulation produziertes Wahlergebnis muss notwendig konsistent sein. Ein zweites Angriffsziel liegt in dem Verkauf der eigenen Stimme durch die Wählerin oder den Wähler. Drittens kann das Ziel einer Angreiferin oder eines Angreifers darin bestehen, aus der Kenntnis über die Wahlentscheidungen Anderer Kapital zu schlagen. Die Form des Kapitals kann dabei vielfältig sein und sowohl Geld, Publizität oder andere Vorteile einschließen. Drei weitere Angriffe zielen auf die Unterminierung des öffentlichen Vertrauens in verschiedene „Beteiligte“ an der Wahl. Das Vertrauen in eine oder mehrere spezifische Wahltechniken selbst kann ein mögliches Angriffsziel sein. Zweitens kann die Integrität von an den Wahlen beteiligten Personen oder Parteien angegriffen werden und drittens ist auch das Vertrauen in die Wahl als Mittel der politischen Auseinandersetzung, in die Politik als solche oder gar in die Demokratie als Gesellschaftsform ein potentielles Angriffsziel. Diese sechs verschiedenen Intentionen oder Hauptziele von Angriffen auf Wahlen und Wahltechniken beinhalten selbst wieder mehrere und teilweise gleiche Teilziele. Auf sie soll jetzt im Einzelnen näher eingegangen werden.

3.2.1 Wahlmanipulation

Manipulationen von Wahlergebnissen können zu verschiedenen Zeitpunkten durchgeführt werden, vor, während oder nach der Wahl. Sie lassen sich sinnvoll nach ihrer strafrechtlichen Einordnung unterscheiden. Einige Manipulationen unterfallen dem Wahlstrafrecht, andere dem sonstigen Strafrecht und dritte sind gar nicht strafbewehrt. Zum Wahlstrafrecht gehören die Wahlbehinderung, die Wahlfälschung, die Fälschung von Wahlunterlagen, die Wählernötigung, die Wählertäuschung sowie die Wählerbestechung. Von diesen stehen die Wahlbehinderung und die Fälschung von Wahlunterlagen nicht im Fokus der Arbeit. Auch die dem nicht wahlspezifischen Strafrecht unterfallenden Manipulationsmöglichkeiten durch Nötigung, Bestechung oder Verleumdung sowie die allgemein nicht strafbewehrten Manipulationen werden hier nicht weiter behandelt. Beispiele für nicht strafbewehrte Manipulationen sind die unterschiedlichen Zugangsmöglichkeiten zu Medien oder Partei- oder Kandidaturverbote.

1. Wählertäuschung
   1. bei Wahlen mit Papier, Stift und manueller Auszählung (Oder)
      1. falscher Stimmzettel
   2. bei Wahlen mit Papier und Zählcomputern (Oder)
      1. falscher Stimmzettel (Oder)
      2. falsches computerlesbares Muster
   3. bei gerätebasierten Wahltechniken (Oder)
      1. falsche Beschriftung
   4. wahltechnikunabhängig

Abbildung 3: Wählertäuschung

Wahltechnikspezifische Formen der Wählertäuschung (siehe Abbildung 3), insbesondere solche, deren Ziel eine ungültige Stimmabgabe ist, sind nur sehr schwer mit der Produktion eines konsistenten Wahlergebnisses vereinbar. Bei Wahlen mit Papier wird zwar die Ausgabe falscher Stimmzettel zur Ungültigkeit der abgegebenen Stimme führen, aber gerade diese Form der Manipulation ist dadurch notgedrungen leicht zu entdecken. Gleiches gilt für eine falsche Anordnung oder Beschriftung der Bedienelemente bei gerätebasierten Wahltechniken. Selbst bei Wahlen mit Papierstimmzetteln, die gerätebasiert ausgezählt werden und bei denen nur diese Auszählung ergebnisrelevant ist, fällt eine Manipulation der computerlesbaren Muster für die einzelnen Wahlalternativen mindestens dann auf, wenn das Einscannen der abgegebenen Stimmen im Zuge der Auszählung stattfindet und dabei Stimmzettel und gespeicherte Wahlentscheidung direkt miteinander verglichen werden können. Findet diese Gegenüberstellung nicht statt oder wird die Wahlentscheidung bereits bei der Stimmabgabe eingescannt, ist eine Entdeckung der Manipulation während der Wahl eher unwahrscheinlich. Nur unter diesen Voraussetzungen lässt sich sinnvoll ein konsistentes Wahlergebnis durch Wählertäuschung produzieren. Andere Formen der Täuschung wie eine geschickte Formulierung von Fragen bei Abstimmungen oder die Veröffentlichung falscher Wahldaten werden als wahltechnikunabhängige Manipulationen nicht weiter betrachtet. Gleiches gilt hier für die Täuschung von Wählerinnen und Wählern über bestimmte Eigenheiten des Wahlablaufes. Insbesondere die Anforderung an die Wählenden, im Verlauf der Stimmabgabe bestimmte Handlungen durchzuführen wie die explizite Bestätigung der Stimmabgabe durch Betätigen eines zusätzlichen Hebels oder einer Taste bei der Verwendung von Wahlcomputern, kann zur Täuschung genutzt werden, wie laut (Jon06) in einem Fall in den Niederlanden geschehen. All diesen Manipulationen ist gemein, dass sie besonders leicht durch Innentäterinnen und -täter durchgeführt werden können.

Wählernötigung und Wählerbestechung setzen notwendig eine Verletzung des Wahlgeheimnisses voraus. In beiden Fällen kann dabei das Wahlgeheimnis durch die Wählerin oder den Wähler selbst oder durch die Angreiferin oder den Angreifer gebrochen werden (siehe Abbildung 4). Beim Bruch des eigenen Wahlgeheimnisses kann die Wahlentscheidung entweder nicht beweisbar mündlich übermittelt oder beweisbar fotografisch dokumentiert werden. Weder im Fall der Nötigung noch der Bestechung wird sich die Angreiferin oder der Angreifer jedoch auf die Aussage der Wählerin oder des Wählers verlassen können. An-

dererseits ist die fotografische Dokumentation der eigenen Wahlentscheidung mit der weiten Verbreitung von Mobiltelefonen mit eingebauter Kamera derart einfach geworden, dass diese Art des Angriffes nur schwer verhindert werden kann, wenn die Verwendung solcher Geräte in der Wahlzelle nicht verboten und dieses Verbot tatsächlich durchgesetzt wird. Bisher wird dies gesetzlich nicht verlangt. Während die Wählerbestechung dabei auf der Zusammenarbeit der Angreiferinnen und Angreifer mit den Wählenden basiert und daher von diesen aus Eigeninteresse nicht öffentlich gemacht werden wird, besteht bei der Wählernötigung immer die Gefahr, dass die Opfer den Angriff auffliegen lassen. Das Entdeckungsrisiko ist daher im zweiten Fall bedeutend höher. In beiden Fällen sind jedoch die betroffenen Wahlberechtigten über die Verletzung ihres Wahlgeheimnisses mindestens informiert, wenn sie nicht sogar, wie im Falle der Wählerbestechung beim Bruch des eigenen Wahlgeheimnisses, selbst auch Angreiferinnen oder Angreifer sind.

1. Wahlgeheimnisbruch
    1. eigenes Wahlgeheimnis (Oder)
        1. nicht beweisbar (Oder)
            1. durch Aussage
        2. beweisbar
            1. fotografisch, videografisch
    2. fremdes Wahlgeheimnis
        1. wahltechnikunabhängig (Oder)
            1. durch Inaugenscheinnahme
            2. fotografisch, videografisch
        2. bei gerätebasierten Wahltechniken
            1. mittelbar gerätebezogen (Oder)
                1. thermografisch (Oder)
                2. mittels Kontaktfarbe
            2. Datenleck durch Designfehler (Oder)
                1. mittels Geräuschmessung (Oder)
                2. mittels Van-Eck-Phreaking
            3. vorsätzlich herbeigeführtes Datenleck
                1. mittels Datenübertragung
                2. mittels Datenspeicherung und Zeitstempel

Abbildung 4: Bruch des Wahlgeheimnisses

Ein fremdes Wahlgeheimnis kann entweder wahltechnikunabhängig gebrochen werden oder die Verwendung von Wahlgeräten oder Wahlcomputern voraussetzen. Bei jeder Wahltechnik ist grundsätzlich eine Inaugenscheinnahme der Wahlentscheidung möglich, genauso wie eine Dokumentation auf Foto oder Video. Besonders einfach kann ein solcher Angriff bei der Briefwahl durchgeführt werden (siehe Abschnitt 2.1.6, S. 11). Er kann dort auch systembedingt nicht verhindert werden. Im Falle von Präsenzwahlen ist dies anders. Die gesetzliche Verantwortung der Wahlvorstände umfasst explizit jede Verhinderung des hier beschriebenen Angriffs. Als mittelbar gerätebezogene Angriffe kommen zwei Alternativen in Betracht: der

Bruch des Wahlgeheimnisses durch Thermografie oder durch Verwendung von Kontaktfarbe. Zwar könnte erstere grundsätzlich bei allen Präsenzwahlen zum Einsatz kommen, sinnvoll ist dies jedoch nur bei der Verwendung von Wahlgeräten und Wahlcomputern. Mit Hilfe der Thermografie lässt sich die genaue Position von Händen und Fingern während der Stimmabgabe feststellen, jedoch nur relativ zu einem festen Bezugspunkt. An welcher Stelle die Wählerin oder der Wähler ihre Wahlentscheidung relativ zum Tisch in der Wahlzelle vorgenommen haben, dokumentiert nicht die Entscheidung auf dem Stimmzettel selbst, weil dessen Position in der Wahlzelle zumindest dann unbekannt bleiben muss, wenn seine Temperatur sich nicht oder nur marginal von der Temperatur des Tisches unterscheidet. Dies ist bei gerätebasierten Wahlen anders. Hier sind die Positionen sowohl von Wahlzelle und Wahlgerät oder Wahlcomputer als auch der jeweiligen Bedienelemente bekannt. In diesem Fall ist das Wahlgeheimnis demnach verletzbar. Da die notwendige Thermografietechnik in Form und Größe Ähnlichkeit mit einer normalen Fernsehkamera hat oder diese Ähnlichkeit unschwer hergestellt werden kann, wäre auch die Entdeckungswahrscheinlichkeit während der Wahl eher gering. Auch mit Hilfe von Kontaktfarbe, wie von Schneier in (Sch04, S. 290.) beschrieben, lässt sich das Wahlgeheimnis bei gerätebasierten Wahlen grundsätzlich immer verletzen. Zur Durchführung dieses Angriffs muss eine Angreiferin oder ein Angreifer die Wahlzelle möglichst direkt oder kurz vor der Zielperson betreten und die Farbe auf ein oder mehrere Bedienelemente applizieren. Wenn die Farbe für das bloße Auge unsichtbar ist, ist diese Angriffsvariante nicht leicht zu entdecken. Allerdings ist der Umgang mit den Ergebnissen, die mit Hilfe solcher Farbe gewonnen wurden, nicht trivial. Nur weil eine Wählerin oder ein Wähler diese Farbe nach der Stimmabgabe an den Händen hat, ist die Wahlentscheidung damit nicht zwangsläufig rekonstruierbar. Dennoch ist zumindest ein negativer Beweis möglich: Wer die auf einem bestimmten Bedienelement aufgebrachte Farbe nicht trägt, kann dieses Element auch nicht berührt haben. Somit ist zumindest nachweisbar, dass eine bestimmte Person eine bestimmte Wahlentscheidung nicht getroffen hat.

Zwei Arten von Datenlecks sind zur Verletzung des Wahlgeheimnisses ausnutzbar. Einerseits können Designfehler bei der Konstruktion von Wahlgeräten und Wahlcomputern die Wahlentscheidung nach außen kenntlich machen, andererseits kann ein solches Datenleck auch vorsätzlich eingebaut werden. Für mechanische und elektromechanische Wahlgeräte kommt dabei vor allem die Geräuschmessung infrage, weil die Geräte als große Hohlkörper wie Klangkörper wirken. Die jeweilige Position der einzelnen mechanischen Bauteile kann daher zu unterscheidbaren Klangbildern führen. Obwohl ein solcher Angriff bisher nicht beschrieben wurde, erscheint er vor dem Hintergrund der Möglichkeiten moderner Signalverarbeitung und Mustererkennung nicht ausgeschlossen. Auch mittels Messung der elektromagnetischen Abstrahlung kann, wie Gonggrijp et. al. in (GHB$^+$06, S. 16ff.) für auch in der BRD verwendete Wahlcomputermodelle gezeigt haben, das Wahlgeheimnis verletzt werden. Wie auch für die Thermografie hängt die Erkennbarkeit dieser Angriffe wesentlich davon ab, ob notwendige Messgeräte entdeckt werden können oder nicht. Vorsätzlich eingebaute Mechanismen zum Informationsabfluss umfassen sowohl die direkte Übertragung der jeweiligen Wahlentscheidung aus dem Wahlgerät oder Wahlcomputer heraus an Dritte als auch die Speicherung der Daten zusammen mit einem Zeitstempel zu ihrer nachträglichen Rekonstruktion. Die direkte Datenübertragung nach außen kann dabei sowohl kabelgebunden als auch kabellos erfolgen. Der Einbau der dazu notwendigen Technik muss dabei fast immer entweder bereits beim Hersteller oder während der Lagerung der Geräte zwischen den

1. Wahlfälschung
    1. wahltechnikunabhängig (Oder)
        1. durch Abgabe zusätzlicher Stimmen (Oder)
            1. zusätzliche Abstreichungen in Wählerlisten (Und)
            2. Ausfüllen zusätzlicher Stimmzettel
        2. bei der Übermittlung der Wahlergebnisse (Oder)
        3. bei der Verkündung der Wahlergebnisse
    2. bei papierbasierten Wahltechniken (Oder)
        1. bei manueller Auszählung (Oder)
        2. bei Verwendung von Zählcomputern
    3. bei gerätebasierten Wahltechniken
        1. bei jeder gerätebasierten Wahltechnik (Oder)
            1. Löschen aller Ergebnisse (Und)
            2. „Neuwahl“
        2. bei mechanischen Wahlgeräten (Oder)
        3. bei elektromechanischen Wahlgeräten (Oder)
        4. bei Wahlcomputern

Abbildung 5: Übersicht Wahlfälschung

Wahlen durch Innentäterinnen oder -täter geschehen, weil während einer Wahl, wenn auch Außentäterinnen und -täter Zugriff auf die Geräte haben, die zeitlichen Beschränkungen zu groß sind. Und abgesehen vielleicht von kabelgebundenen Informationsabflüssen, zumindest wenn die Daten nicht über das Stromkabel übertragen werden, sind die einzelnen Angriffe nicht ohne genaue Inspektion der Geräte zu entdecken. Während der Wahl ist daher die Entdeckungswahrscheinlichkeit äußerst gering.

Die umfangreichsten Angriffsszenarien bei der Wahlmanipulation fallen unter den Begriff der Wahlfälschung (siehe Abbildung 5). Wahltechnikunabhängig lassen sich Wahlergebnisse durch die zusätzliche Abgabe von Stimmen fälschen. Dazu müssen Wahlberechtigte, die nicht an Wahlen teilgenommen haben, nachträglich in der Wählerliste abgestrichen und zusätzliche Stimmzettel ausgefüllt werden. Dies kann sowohl in einem Präsenzwahllokal als auch in einem Briefwahlbezirk durchgeführt werden. Die innere Konsistenz des Wahlergebnisses ist zumindest dann gegeben, wenn die Person nicht auf dem jeweils anderen Weg an den Wahlen teilnimmt oder teilgenommen hat oder deren Stimmabgabe aus einem anderen Grund nicht stattgefunden haben kann, etwa weil sie vor der Wahl verstorben ist. Auch bei der Zählung und Übermittlung der Wahlergebnisse können Fälschungen vorgenommen werden, jeweils auf allen Ebenen der Wahlorganisation. Gleiches gilt für die Verkündung der Wahlergebnisse. Beides ist grundsätzlich während der Wahl entdeckbar.

Für papierbasierte Wahltechniken lassen sich die möglichen Angriffe danach trennen, ob die Auszählung manuell oder gerätebasiert erfolgt. Im ersten Fall müssen die Papierstimmzettel selbst manipuliert werden, im zweiten kann der Angriff sowohl auf die Stimmzettel als auch auf die eingesetzte Computertechnik zielen. Bei Wahlen mit Wahlgeräten und Wahlcomputern erweist sich eine Trennung anhand der eingesetzten Technik als sinnvoll. Zusätzlich ist

1. Wahlfälschung bei Papierstimmzetteln und manueller Auszählung
   1. Stimmen löschen (Oder)
      1. Stimmzettel vernichten (Und)
      2. neue Stimmzettel produzieren (Und)
      3. Wählerliste anpassen
   2. Stimmzettel ändern (Oder)
   3. Stimmen neu produzieren (Oder)
      1. Stimmzettel vernichten (Und)
      2. neue Stimmzettel produzieren (Und)
      3. Stimmzettel ausfüllen
   4. Stimmen falsch zählen

Abbildung 6: Wahlfälschung mit Papier und Stift

es grundsätzlich bei allen gerätebasierten Wahlen möglich, die Wahlergebnisse nach Schließung der Wahl vollständig neu zu produzieren. Die Originalergebnisse müssen dazu schlicht gelöscht werden, bevor die „Wahl“ einfach „wiederholt“ wird. Vorteilhaft für eventuelle Angreiferinnen und Angreifer sind hier zwei Tatsachen: Zu diesem Zeitpunkt ist die genaue Anzahl der Wählerinnen und Wähler bekannt, so dass ein Wahlergebnis mit innerer Konsistenz produziert werden kann, und einem einfachen Einbau einer genauen Zeitquelle in die Wahlgeräte und Wahlcomputer stehen die hohen Hürden des Wahlgeheimnisschutzes entgegen. Grundsätzlich nachteilhaft ist der Zeitbedarf für die Fälschung nach Schließung der Wahl, bis das Ergebnis übermittelt werden kann. Dieser Angriff ist nur von Innentäterinnen und -tätern durchführbar und von allen anwesenden Nichtbeteiligten leicht zu entdecken.

Die Produktion konsistenter aber falscher Wahlergebnisse bei papierbasierten Präsenzwahlen mit manueller Auszählung ist weder trivial noch von Außentäterinnen und -tätern durchführbar (siehe Abbildung 6). Zur nachträglichen Vernichtung von Stimmen, die für die „falsche“ Partei abgegeben wurden, können die Stimmzettel nicht einfach nur vernichtet werden, es müssen gleichzeitig genauso viele leere Stimmzettel nachproduziert und die Wählerliste muss an das neue Ergebnis angepasst werden. Wenn die Stimmzettel nicht einfach veränderbar sind, weil sie mit Bleistift ausgefüllt wurden,[6] dann können Wahlergebnisänderungen nur durch Vernichtung von ausgefüllten Stimmzetteln, deren Neuproduktion und erneutes Ausfüllen erfolgen. Abgesehen von der eventuell möglichen Veränderung von Stimmzetteln und einer bewusst fehlerhaften Auszählung sind die anderen Angriffe nicht unauffällig durchführbar. Gleichzeitig ist die Entdeckungswahrscheinlichkeit auch in diesen beiden Fällen dann sehr hoch, wenn die Mitglieder des Wahlvorstandes sich gegenseitig kontrollieren. Findet eine solche gegenseitige Kontrolle hingegen nicht statt, lässt sich die Manipulation, wie unter anderem (HL08) zeigt, ohne Risiko der Entdeckung während der Wahl durchführen.

Wird die Auszählung hingegen gerätebasiert durchgeführt, gibt es weitere Angriffsmöglichkeiten (siehe Abbildung 7). Findet das Einscannen der Stimmen zum Zeitpunkt der

[6] Von solchen Vorkommnissen wird zumindest im Netz auch für die BRD berichtet, wie das Beispiel auf http://forum.golem.de/read.php?22690,1201143,1201143 zeigt.

1. Wahlfälschung bei Papierstimmzetteln und Zählcomputern
   1. Scannen während der Stimmabgabe (Oder)
      1. falsches computerlesbares Muster
   2. Scannen während der Stimmenauszählung (Oder)
      1. Stimmen löschen (Oder)
      2. Stimmzettel ändern (Oder)
      3. Stimmen neu produzieren (Oder)
      4. Stimmen falsch einscannen
   3. Manipulationen des Zählcomputers
      1. Manipulationen der Hardware (Oder)
      2. Manipulationen der Software (Oder)
      3. Manipulationen der Konfiguration

Abbildung 7: Wahlfälschung mit Papier und Geräten

1. Wahlfälschung mit mechanischen Wahlgeräten
   1. Manipulationen der Hardware (Oder)
      1. Zählwerk (Oder)
      2. Verbindung zwischen Bedienelement und Zählwerk
   2. Manipulationen der Konfiguration
      1. falsche Nullsetzung des Zählwerkes

Abbildung 8: Wahlfälschung mit mechanischen Wahlgeräten

Stimmabgabe statt, verfälscht eine Manipulation des computerlesbaren Musters auf dem Stimmzettel das Wahlergebnis. Der Angriff selbst, also die Produktion manipulierter Stimmzettel, muss dann schon vor Beginn der Wahl stattgefunden haben und ist für Innentäterinnen und -täter ungleich einfacher als für andere. Wenn die Stimmen erst zum Zeitpunkt der Auszählung eingescannt werden, lassen sich die gleichen Angriffe wie bei einer manuellen Auszählung durchführen. Da hier die eigentliche Zählung aber vom Computer vorgenommen wird, reicht ein falsches Einscannen für die Verfälschung des Wahlergebnisses. Die Bewertungen von Sicherheit und Entdeckungswahrscheinlichkeit entsprechen denen für die manuelle Auszählung genannten. Zusätzlich lassen sich Scanner und Zählcomputer manipulieren, wobei diese sowohl in Hardware, in Software als auch bei der Konfiguration vorgenommen werden können. Sicherheitsfragen zu Computern, deren Software und Konfiguration werden ausführlicher im Zusammenhang mit Wahlcomputern diskutiert.

Rein mechanische Wahlgeräte haben zwei grundsätzliche Angriffsvektoren (siehe Abbildung 8). Einerseits kann das Gerät selbst manipuliert werden, andererseits auch seine Konfiguration. Manipulationsmöglichkeiten an der Hardware betreffen dabei entweder die mechanische Verbindung zwischen dem Bedienelement und dem Zählwerk oder das Zählwerk selbst. Beide Manipulationen sind nur sehr unwahrscheinlich während einer Wahl durchführbar, so dass als mögliche Angreiferinnen und Angreifer vor allem Innentäterinnen und -täter infrage kommen. Auch lassen sie sich nicht während einer Wahl feststellen. Die

1. Wahlfälschung mit elektromechanischen Wahlgeräten
   1. Manipulationen der Hardware (Oder)
      1. Zählwerk (Oder)
      2. Verbindung zwischen Bedienelement und Auslöser (Oder)
      2. Verbindung zwischen Auslöser und Zählwerk
   2. Manipulationen der Konfiguration
      1. falsche Nullsetzung des Zählwerkes

Abbildung 9: Wahlfälschung mit elektromechanischen Wahlgeräten

Verbindung zwischen Auslöser und Zählwerk eignet sich als Angriffsvektor nur sehr bedingt, weil eine solche Manipulation allein die äußere Konsistenz des Ergebnisses infrage stellt, indem sie zwangsläufig alle manipulierten Entscheidungsmöglichkeiten betrifft und für diese damit das Ergebnis notwendig mit null Stimmen determiniert. Hingegen kann eine Manipulation des Zählwerkes durchaus so vorgenommen werden, dass sowohl innere als auch äußere Konsistenz des Wahlergebnisses sichergestellt wird. Eine solche Manipulation könnte unter anderem eine mechanische Verbindung zwischen verschiedenen Zählwerken beinhalten, durch die in einer bestimmten Stellung des Zählwerkes für die eigentlich gewählte Partei ein anderes Zählwerk weitergeschaltet wird. Während die erste Hardware-Manipulation eher trivial ist, stellt die zweite hohe Anforderungen an die mechanischen Fähigkeiten der Angreiferin oder des Angreifers. Im Zusammenhang mit der Konfiguration der Wahlgeräte vor Beginn der Wahl kann eine Wahlfälschung dadurch geschehen, dass nicht alle Zähler auf Null gesetzt werden. Dabei muss allerdings beachtet werden, dass zur Sicherstellung eines konsistenten Ergebnisses für jede Stimme, die einer Partei zugeschlagen werden soll, das Zählwerk einer anderen Partei um eine Stimme zurückgesetzt werden muss. Unter zwei Bedingungen kann dies technisch unauffällig geschehen. Erstens muss das Zählwerk überlaufen können. Zweitens müssen für die Partei, deren Zählwerk zu ihrem Nachteil manipuliert wurde, mindestens so viele Stimmen abgegeben werden, dass ein Überlauf über die Nullstellung stattfindet, andernfalls wird das Ergebnis offenkundig inkonsistent. Auch hier liegt der Schutz ausschließlich auf der organisatorischen Ebene der gegenseitigen Kontrolle der Mitglieder des jeweiligen Wahlvorstandes.

Grundsätzlich bieten elektromechanische Wahlgeräte die gleichen Manipulationsmöglichkeiten wie rein mechanische. Allerdings existieren dort keine direkten Verbindungen mehr zwischen den Bedienelementen und den Zählwerken. Stattdessen existiert zwischen beiden ein Auslöser, dessen Funktion der Weiterschaltung des Zählwerkes ein sich beim Betätigen einer Taste schließender Stromkreis auslöst. Insofern gibt es auch drei Angriffsvektoren (siehe Abbildung 9): die Verbindung zwischen Taste und Auslöser und zwischen Auslöser und Zählwerk sowie der Auslöser selbst. Im Allgemeinen sind auch diese Angriffe für Innentäterinnen und -täter einfacher durchführbar und während der Wahl schwer zu entdecken. Gleichwohl könnte ein elektromagnetischer Auslöser unter Umständen auch während der Wahl von Wahlberechtigten mit Hilfe von Magneten angegriffen werden. In diesem Fall ist allerdings die Konsistenz des Wahlergebnisses gefährdet. Außerdem könnte das Geräusch des weiterschaltenden Zählwerkes bei gleichzeitigem Fehlen einer von außen erkennbaren

1. Wahlfälschung mit Wahlcomputern
   1. Manipulationen der Hardware (Oder)
      1. CPU (Oder)
      2. Eingabe-/Ausgabesysteme (Oder)
      2. Datenspeicher
   2. Manipulationen der Software (Oder)
      1. Zugelassene Software (Oder)
         1. Fehlerhafte Software (Oder)
         2. Software mit Hintertür
      2. Nichtzugelassene Software
         1. Programmspeicher austauschen (Und)
         2. Wahlcomputersoftware manipulieren oder neu schreiben
   3. Manipulationen der Konfiguration
      1. Konfigurationssoftware (Oder)
         1. Fehlerhafte Software (Oder)
         2. Software mit Hintertür (Oder)
         3. Software manipulieren oder neu schreiben
      2. falsche Konfigurationsdaten

Abbildung 10: Wahlfälschung mit Wahlcomputern

Wahlhandlung Verdacht erregen. Wie auch bei rein mechanischen Wahlgeräten hängt die Sicherstellung der richtigen Nullsetzung des Zählwerkes ausschließlich von organisatorischen Maßnahmen ab.

Die umfangreichsten Möglichkeiten zu Manipulationen bieten jedoch Wahlcomputer (siehe Abbildung 10). Wie bei allen gerätebasierten Wahltechniken lassen sich die Angriffsvektoren in drei Bereiche einteilen: Hardware, Software und Konfiguration. Die höhere Komplexität ihres Aufbaus – die Wahlcomputer von Nedap sind vollwertige Standard-Computer, wenn auch basierend auf Technik aus den achtziger Jahren, wie (GHB$^+$06, S. 5.) zeigen – vergrößert die Liste der angreifbaren Systembestandteile enorm. Auf der Ebene der Hardware lassen sich grundsätzlich alle eingebauten Teile, die an Stimmabgabe und -auszählung beteiligt sind, angreifen. Dazu gehören insbesondere alle Ein- und Ausgabesysteme, die CPU sowie die Speichersubsysteme. Dabei können entweder eingebaute Teile verändert oder neue Teile hinzugefügt werden. Die Veränderung der Ein- und Ausgabesysteme ist zumindest dann am schwersten vor den Wählerinnen und Wählern zu verbergen, wenn jeweils vor der Bestätigung einer Stimmabgabe die getroffene Wahlentscheidung zur Kontrolle ausgegeben wird. Veränderungen an der CPU, unter deren Kontrolle jede Software auf dem Computer läuft, fallen während einer Wahl genauso wenig auf wie Veränderungen am Speicherinterface oder den Speichermodulen. Die enorme Weiterentwicklung der Technik ermöglicht heute den Bau eines vollständig kompatiblen Prozessors auf einer viel kleineren Fläche, die dann, wie (KTC$^+$08) gezeigt haben, Platz für zusätzliche Funktionen im Chipgehäuse lassen. Sogar eine Virtualisierung des 68000 mit Hilfe eines modernen Prozessordesigns ist möglich, solange mechanische, elektrische und Datenkompa-

tibilität zwischen Chipgehäuse und -sockel beachtet werden. Zwar handelt es sich dabei um relativ teure Angriffe, aber der Zeitbedarf für den Austausch und das Entdeckungsrisiko sind gering, während die Wahrscheinlichkeit für eine erfolgreiche Produktion eines falschen aber konsistenten Wahlergebnisses sehr hoch und Veränderungen an der Software unnötig sind. Auch im Umfeld der Speichersubsysteme liegt ein großes Angriffspotential, entweder wird im Wahlcomputer das Speicherinterface manipuliert oder die Hardware im externen Speichermodul. Alle Angriffe setzen unauffällige Zugangsmöglichkeiten zu den Wahlcomputern voraus, so dass eine Ausführbarkeit während der Wahl wenig wahrscheinlich erscheint.

Das zweite große Angriffsziel bei Wahlcomputern ist die Software. Die Software, die während einer Wahl auf dem Wahlcomputer läuft, kann dabei aus zwei Quellen stammen. Entweder handelt es sich um die zugelassene Software oder um eine nicht zugelassene. Erstere kann einerseits fehlerhaft sein oder sie wurde vom Hersteller mit einer Hintertür versehen. Fehlerhafte Software ist alles andere als ungewöhnlich, aber zu Sicherheitsproblemen werden solche Fehler erst, wenn diese für Wahlergebnismanipulationen ausgenutzt werden können. Die Bewertung der Angriffswahrscheinlichkeit hängt hier entscheidend von der Qualität der eingesetzten Software ab, über die mangels Kenntnis in dieser Arbeit keine Aussage getroffen werden kann. Allerdings schätzen (GHB+06, S. 7.) die Softwarequalität eher hoch ein. Vom Hersteller eingebaute Hintertüren stellen grundsätzlich ein schwerwiegenderes Problem dar. Erstens lassen sie sich – Kenntnis vorausgesetzt – leicht ausnutzen, zweitens sind sie selbst bei einer Quellcodeanalyse dann nicht zu entdecken, wenn sie erst während des Kompiliervorganges in die Software eingefügt werden können, und drittens können sie die Produktion eines konsistenten Wahlergebnisses von allen betrachteten Angriffen am ehesten garantieren. Die Installation nicht zugelassener Software, die am Wahltag auf einem Wahlcomputer laufen soll, erfordert entweder längeren Zugriff auf ein Gerät und eine direkte Änderung der installierten Software oder zumindest einen Austausch des originalen Programmspeichers mit einem neuen, auf dem sich die manipulierte Software befindet. In diesem Fall reicht dann auch, wie in (KRG07, S. 15f.) gezeigt wird, eine extrem kurze Zugriffszeit. Dabei kann die nicht zugelassene Software auf drei Arten entstehen: Erstens als komplette Neuerstellung anhand eines ausführlichen Funktionstests ohne Zugriff auf Quell- oder Binärcode, zweitens als Veränderung des gegebenen Binärcodes und drittens auf der Basis des Quellcodes. Die Umsetzung der ersten Möglichkeit setzt relativ langen Zugriff auf einen Wahlcomputer, umfangreiche Testmöglichkeiten und viel Wissen über Wahlablauf und -interna voraus. Für die Manipulation des Binärcodes bedarf es nichtalltäglicher Kenntnisse im Bereich des Reverse Engineerings, allerdings ist der Zeitbedarf, wie von (GHB+06, S. 10ff.) gezeigt, eher gering. Die geringsten Anforderungen an Kenntnisse und Fähigkeiten von Angreiferinnen und Angreifern sowie die aufzuwendende Zeit werden bei Kenntnis des Quellcodes gestellt. Die beschriebenen Angriffe lassen sich preiswert umsetzen und bergen nur wenig Gefahr einer Entdeckung während der Wahl.

Neben Hardware und Software von Wahlcomputern können auch die Konfigurationen und die Konfigurationssoftware Ziele von Angriffen sein. Diese Trennung ist sinnvoll, weil bei den derzeit in der BRD eingesetzten Wahlcomputern die Software zur Konfiguration der Wahl und der Zuordnung zwischen Tasten und Wahlbewerberinnen und -bewerbern auf einem getrennten PC durchgeführt wird, der im Regelfall von der Kommune gestellt werden soll. Hier lassen sich vier Angriffsvektoren identifizieren: Der PC selbst, die Speichermodulanbindung, die Konfigurationssoftware sowie die Konfigurationsdaten. Da die verwendeten

PCs nicht nur exklusiv für die Durchführung von Wahlen eingesetzt werden, sind alle seine Hardware- und Softwaresysteme grundsätzlich zu jedem beliebigen Zeitpunkt zwischen den Wahlen angreifbar, insbesondere, aber nicht ausschließlich, durch Innentäterinnen und -täter. Gleichzeitig gilt es für die Angreiferinnen und Angreifer einige Unwägbarkeiten zu beachten. Erstens kann die Anzahl der PCs in den Kommunen, aus denen für eine Verwendung bei Wahlen ausgewählt werden kann, extrem groß sein. Im schlimmsten Fall müssten alle oder zumindest fast alle davon erfolgreich angegriffen werden. Zweitens ist nicht garantiert, dass die Rechner vor der Wahl nicht vollständig neu aufgesetzt werden. Und drittens besteht immer die Gefahr einer frühzeitigen Entdeckung des Angriffs, vor allem wenn dieser bereits lange vor einer Wahl durchgeführt wird. Hingegen ist eine Manipulation der Speichermodulanbindung mit dem Ziel, die Konfigurationsdaten bei der Übertragung von der Software auf die Speichermodule zu ändern, einfacher und schneller durchführbar, kann aber bei Verwendung von mehr als einem Lese- und Schreibsystem für die Speichermodule leicht auffallen. Für mögliche Manipulationen an der Konfigurationssoftware gilt im Wesentlichen das Gleiche wie für die Wahlcomputersoftware, allerdings könnten die Zugriffsmöglichkeiten für Angreiferinnen und Angreifer einfacher sein, weil die erforderlichen Schutzmechanismen für die PCs, auf denen die Software läuft, weniger hoch sind und die Software selbst keinerlei Tests unterzogen werden muss. Und zuletzt können die Konfigurationsdaten selbst angegriffen werden, je nachdem, wie und wo ein Zugriff auf die Speichermodule zwischen Aufspielen der Daten und Übertragung der Daten in die Wahlcomputer möglich ist. Vor Wählerinnen und Wählern lassen sich alle diese Angriffe leicht verbergen.

3.2.2 Stimmenverkauf und andere Vorteilsgewinnung

Der Stimmenverkauf ist das Gegenstück zum Stimmenkauf. Angreiferinnen und Angreifer sind in diesem Fall die Wahlberechtigten. Wer gewählt werden soll ist aus Sicht der Angreiferin oder des Angreifers egal, solange sie dafür bezahlt werden oder andere Vorteile erhalten. Wie auch beim Stimmenkauf hängt ein erfolgreicher Stimmenverkauf wesentlich von einer erfolgreichen und nichtentdeckten Verletzung des Wahlgeheimnisses ab, in diesem Fall jedoch vorrangig des eigenen. Insofern gilt hier das oben für den Wahlgeheimnisbruch Erläuterte in Bezug auf Einfachheit des Angriffes und geringe Entdeckungsmöglichkeiten während der Wahl bei weiterhin fehlenden Kontrollen auf mitgebrachte Aufzeichnungsgeräte.

Im Gegensatz zur Verletzung eines fremden Wahlgeheimnisses im Zuge von Wählerbestechung und -nötigung soll bei dieser Angriffsvariante die ausgespähte Person gerade nicht über den Angriff informiert oder gar darin involviert sein. Dieser Angriff muss daher nicht nur vor Dritten wie den Mitgliedern des Wahlvorstandes oder anderen anwesenden Personen geheimgehalten werden sondern auch vor den betreffenden Wählerinnen und Wählern. Während aber insbesondere Angriffe zur Wahlmanipulation immer einen größeren Personenkreis betreffen, weil das Ziel im Gewinnen der Wahl liegt, ist die Zahl der Opfer bei dieser Angriffsvariante naturgemäß sehr klein. Insoweit Personen des öffentlichen Lebens Angriffsziele darstellen, lässt sich die verwendete Technik leicht tarnen, weil insbesondere die Anwesenheit von Geräten, die wie Videokameras aussehen, den Erwartungen aller Anwesenden entspricht und damit unauffällig ist. Der Fokus auf einzelne oder einige wenige Zielpersonen lässt dabei Angriffe, die auf vorsätzlich herbeigeführten Datenlecks basieren,

als wenig wahrscheinlich erscheinen. Angriffe, die keine beweiskräftigen Ergebnisse produzieren, lassen sich mit an Sicherheit grenzender Wahrscheinlichkeit ausschließen.

3.2.3 Vertrauensangriffe

Angriffe auf das Vertrauen der Öffentlichkeit in verschiedene „Beteiligte“ an der Wahl setzen immer voraus, dass die expliziten oder impliziten Erwartungen an diese enttäuscht werden. Anhand der drei wesentlichen „Vertrauensobjekte“ (siehe Abbildung 2) sollen die spezifischen Erwartungen aufgezeigt und Methoden zu ihrer Enttäuschung dargestellt werden.

Soll das Vertrauen in bestimmte Wahltechniken unterminiert werden, dann betreffen die Erwartungen vor allem die Schutzziele, wie sie in Abschnitt 3.1 aufgeführt wurden. Für die Bereiche *safety* mit den Schutzzielen Funktionalität, Funktionssicherheit, Verlässlichkeit, Verfügbarkeit und Verständlichkeit und *security* mit Integrität, Identifizierbarkeit, Authentizität, Verbindlichkeit, Überprüfbarkeit, Rückwirkungsfreiheit, Vertraulichkeit und dem Zwischenergebnisverbot lassen sich dabei verschiedene Angriffsszenarien identifizieren. Wahltechniken, bei denen Angreiferinnen und Angreifer dafür gesorgt haben, dass sie am Wahltag nicht wie erwartet funktionieren oder benutzbar sind, verlieren den Rückhalt in der Öffentlichkeit vor allem dann, wenn die Gründe für die Schwierigkeiten unerkannt bleiben. Mögliche Angriffe, wie sie bereits in Abschnitt 3.2.1 für Wahlmanipulationen beschrieben wurden, zielen dabei in diesem Fall nicht auf die Veränderung des Wahlergebnisses sondern auf die Verhinderung eines normalen Wahlablaufes. Insbesondere technische Probleme wie Wackelkontakte, mechanische Unzuverlässigkeiten oder unvorhersehbare Abstürze können als gewollte Ergebnisse von Angriffen das Vertrauen in die Sinnhaftigkeit des Einsatzes bestimmter Wahltechniken schmälern. Unerwartete, kryptische oder unverständliche Fehlermeldungen bei Wahlcomputern oder allgemein nicht nachvollziehbare Verhaltensweisen und „komische“ Geräusche bei gerätebasierten Wahltechniken können weitere Ziele von Angreiferinnen und Angreifern darstellen. Für den Bereich der *security* stellen vor allem offensichtlich inkonsistente Wahlergebnisse, nicht gespeicherte oder gelöschte Stimmen oder die jeweilige Ausgabe der Wahlentscheidung der vorherigen Wählerinnen oder Wähler beim Betreten der Wahlzelle die größten Gefahren für das Vertrauen in die spezifische Wahltechnik und damit bevorzugte Angriffsziele dar. Dabei sind die Anforderungen an die Durchführung der Angriffe unterschiedlich. Angriffe auf die *safety* dürfen nicht oder nur sehr schwer zu entdecken sein, damit die öffentliche Meinung die Probleme direkt als immanent mit der jeweiligen Wahltechnik verbunden sieht und nicht als das Produkt fremder Eingriffe. Solche fremden Eingriffe in die *safety* führen jedoch selbst dann, wenn sie entdeckt aber nicht verhindert werden, zu einem Vertrauensverlust in die erwartete Nichtmanipulierbarkeit der Wahltechnik. Gleiches gilt noch mehr, wenn Angriffe auf Schutzziele aus dem Bereich *security* erfolgreich durchgeführt werden können. Allgemein werden im Wesentlichen ähnliche technische, finanzielle und Wissensanforderungen an die Angreiferinnen und Angreifer gestellt wie bei einer Wahlmanipulation, allerdings mit Ausnahme der fehlenden Notwendigkeit der Beachtung von Konsistenzbedingungen bei der Wahlergebnisproduktion. Auch für die Entdeckungswahrscheinlichkeit muss eine Trennung vorgenommen werden: Die Angriffe sollen unentdeckt bleiben, deren Folgen umso öffentlicher werden.

Ein Angriff auf die Integrität von an den Wahlen beteiligten Personen oder Parteien kann im Prinzip jeden der bisher beschriebenen Angriffsvektoren nutzen, solange dabei ein

inkonsistentes Wahlergebnis produziert oder ein anderer offenkundiger Wahlrechtsverstoß begangen wird. Das Ziel solcher Angriffe liegt dabei darin, die Identifizierbarkeit der eigentlichen Angreiferinnen und Angreifer zu verhindern und statt dessen jeden Verdacht auf die Opfer selbst zu lenken. Ein sinnvolles Angriffsziel ist dabei die Produktion eines Wahlergebnisses mit innerer aber ohne äußere Konsistenz, dessen offensichtliche Nutznießerinnen und Nutznießer die Opfer sind. Beispiele können nicht nachvollziehbar hohe Wahlgewinne der Opfer oder genauso extreme Wahlniederlagen ihrer Gegnerinnen und Gegner sein. Zu den Anforderungen an die Angreiferinnen und Angreifer und Erfolgs- und Entdeckungswahrscheinlichkeiten der Angriffe gilt dabei das bereits Gesagte. Auch die Konstruktion schwerwiegender Verdachtsmomente auf Wählerbestechung ist ein mögliches Ziel von Angriffen, ein sehr einfaches noch dazu. Wenn die Angreiferinnen und Angreifer die Partei des Opfers wählen, ihre Wahlentscheidung dabei beweisbar dokumentieren und danach bei der Partei des Opfers die Auszahlung der versprochenen Bestechungssumme einfordern, ist das Verhalten der betreffenden Partei zu ihrer Forderung irrelevant für die Feststellung, dass von vier Aussagen – 1. das Opfer hat Wählerinnen und Wähler bestochen, 2. die Angreiferinnen und Angreifer haben ihre Stimmen dem Opfer gegeben, 3. sie haben das beweisbar dokumentiert, 4. das Opfer oder dessen Partei hat, je nach tatsächlichem Ablauf, gezahlt oder nicht gezahlt – genau drei (2., 3. und 4.) immer bewiesen werden können. Aus der Sicht von Außenstehenden sprechen damit die Indizien für die Korrektheit auch der ersten Aussage zum Nachteil des Vertrauens in die Opfer.

Das dritte „Vertrauensobjekt“ stellt im Wesentlichen eine Obermenge des zweiten dar. Statt eines Opfers oder einer Partei hat dieser Angriff gleichzeitig verschiedene Opfer oder Parteien zum Ziel, um damit die Erwartungen, es gäbe jeweils auch politische Alternativen zu den Personen, Parteien oder Institutionen, auf die jeder Verdacht weist, zu enttäuschen. Die Komplexität dieses Angriffes liegt dabei nicht so sehr in den möglichen Angriffsvektoren oder in den Anforderungen an die Durchführung und die Durchführenden sondern im erforderlichen räumlichen Umfang und dem personellen Bedarf für einen erfolgreichen Abschluss. Angriffsvarianten können dabei sowohl die Produktion falscher und inkonsistenter Wahlergebnisse sein aber auch die großflächige Manipulation einer eingesetzten Wahltechnik, um deren politische Befürworterinnen und Befürworter bloßzustellen. Die notwendig große räumliche Ausdehnung des Angriffes, die Vielzahl der Einzelziele sowie die große Anzahl an Angreiferinnen und Angreifern führen zu einer signifikant höheren Entdeckungswahrscheinlichkeit als bei allen vorher betrachteten Angriffen.

3.2.4 Analyse der Risiken

Nach der bisherigen Betrachtung der Angriffe lassen sich einige Zwischenergebnisse ableiten.

Angriffe durch Innentäterinnen und -täter stellen die größte Gefahr für Wahlen dar. Die Abgabe zusätzlicher Stimmen, die vorsätzlich fehlerhafte manuelle Auszählung oder Manipulationen beim Einscannen von Stimmen sind leicht auch von Einzelpersonen oder kleinen Gruppen durchführbare Angriffe. Gleiches gilt für Manipulationen bei der Nullsetzung von Zählwerken und der Konfiguration von Wahl- und Zählcomputern. Entweder mit etwas größeren Gruppen oder bei fehlender gegenseitigen Kontrolle im Wahlvorstand lassen sich auch einfach Stimmen löschen oder neu produzieren, sowohl bei papier- als auch bei gerätebasierten Wahltechniken. Nachträgliche Veränderungen von abgegebenen Stimmzet-

teln sind nur bei der Verwendung von nicht dokumentenechten Stiften möglich, in diesem Fall aber einfach und relativ unauffällig durchführbar. Manipulationen an der Software von Wahlcomputern oder der Konfigurationssoftware sind bei vorliegenden technischen Kenntnissen einfach und unauffällig durchführbar, nicht nur aber vor allem für Hersteller und Wartungspersonal. Mit höheren Kosten aber gleich niedrigem Entdeckungsrisiko lässt sich die Hardware von elektromechanischen Wahlgeräten und Wahlcomputern manipulieren. Angriffe auf die Mechanik von Wahlgeräten sind dabei aufgrund der schlechteren Granularität von Wahlergebnismanipulationen unwahrscheinlich. Weiterhin nicht zu erwarten sind eine falsche Übermittlung und Verkündung des Wahlergebnisses.

Im Gegensatz zu Manipulationen, die während der Wahl oder der Stimmenauszählung stattfinden müssen, sind alle anderen technischen Manipulationen grundsätzlich dann von Außentäterinnen und -tätern durchführbar, wenn sie Zugriff auf die Wahlgeräte, Wahlcomputer oder Zählcomputer erlangen können. Für diesen Angreifertypen hängt die Bewertung der Risiken solcher Angriffe allein von diesen Zugriffsmöglichkeiten ab.

Im Wesentlichen angreifertypenunabhängig lassen sich die meisten Angriffe durchführen, deren Ziel oder Teilziel die Verletzung des Wahlgeheimnisses ist. Die für eine beweisbare Dokumentation von Wahlentscheidungen benötigte Technik ist entweder allgemein verfügbar oder relativ leicht zu beschaffen. Gegen eine umfangreiche Wählerbestechung, die im Einzelfall für eine mandatsrelevante Wahlmanipulation notwendig ist, spricht vor allem das große Entdeckungsrisiko.

3.3 Forensik

Allen bisher beschriebenen Angriffen ist gemein, dass sie unter Umständen während einer Wahl unentdeckt bleiben können. Gleichwohl kann es Verdachtsmomente wie inkonsistente Ergebnisse, nachträglich aufgefundene Stimmzettel oder Aussagen von Zeuginnen oder Zeugen geben, die eine Überprüfung von Wahlabläufen und -ergebnissen nach einer Wahl notwendig machen. Eine solche Überprüfung kann für einen festgelegten Prozentsatz aller Wahllokale, Wahlbezirke oder Wahlkreise auch gesetzlich vorgeschrieben sein. Im folgenden Abschnitt sollen nun die Möglichkeiten und Grenzen einer nachträglichen Entdeckung und Aufklärung der beschriebenen Angriffe aufgezeigt werden.

Dem Fokus der Arbeit entsprechend bleiben dabei Methodiken des Vorgehens zur Aufklärung von Manipulationen und anderen Angriffen außen vor. Auch kriminaltechnische Hilfsmittel und die Gewichte eventuell gefundener Indizien, etwa von Fingerabdrücken unbefugter Personen innerhalb von Wahlgeräten oder Wahlcomputern oder Radierspuren auf Stimmzetteln, bleiben unbeachtet.

Manipulationen, die die Daten der abgegebenen Stimmen nicht verändern oder vernichten sondern diese nur falsch bewerten oder auszählen, sind auch nach Ende einer Wahl zu entdecken. Fälschlich als ungültig gewertete und dann nicht gezählte, falsch eingescannte oder manuell falsch gezählte Stimmzettel oder durch fehlerhafte oder manipulierte Zählgeräte oder -computer falsch berechnete Ergebnisse lassen sich nachträglich anhand unveränderter Stimmzettel oder Datensätze erkennen und sind damit korrigierbar.

Manipulationen von Stimmen, die gegenständlich, etwa auf Stimmzetteln, gespeichert sind, im Gegensatz zu elektronisch gespeicherten Daten,[7] lassen sich im Nachhinein zumindest dann erkennen, wenn diese offensichtlich sind oder unvollkommen vorgenommen wurden. Zu den offensichtlichen Manipulationen gehören Stimmzettel, die zur Wählertäuschung falsch beschriftet sind, und denen diese Fehler auch nach der Wahl noch angesehen werden können sowie zusätzlich in Wählerlisten vermerkte Wahlberechtigte, die nachweisbar nicht oder nicht in diesem Wahllokal gewählt haben. Beispiele für unvollkommene Manipulationen sind Veränderungen von mit Bleistift ausgefüllten Stimmzetteln, die etwa anhand von Radierspuren erkannt werden können, Übereinstimmungen im Schriftbild vieler Stimmzettel oder die unvollständige Vernichtung von Stimmzetteln, wie sie im Wahlfälschungsskandal von Dachau[8] zur Erkennung der Manipulationen geführt haben. Auch die Herstellung zusätzlicher Stimmzettel, die als Ersatz für vernichtete Stimmzettel ausgefüllt wurden, kann sich erkennen lassen, wenn Papier oder Druckbild nicht mit amtlichen Stimmzetteln übereinstimmen.

Werden Stimmen nur als Daten gespeichert oder sogar ohne Speicherung nur gezählt, sind Nachweise von Manipulationen schwieriger.

Veränderungen an der Mechanik von Wahlgeräten lassen sich durch Vergleiche mit den Bauplänen unterstützt durch Wahlsimulationen leicht erkennen. Voraussetzung dafür ist, dass die Angreiferinnen und Angreifer keine Möglichkeiten hatten, die Manipulationen zwischen dem Ende der Wahl und dem Beginn der Überprüfung rückgängig zu machen. Fehlkonfigurationen bei der Nullsetzung der Zählwerke, wie sie auf Seite 37 beschrieben wurden, lassen sich nur dann mit absoluter Sicherheit feststellen, wenn bei mindestens einem Wahlvorschlag kein Überlauf aufgetreten ist. Sind bei allen Zählwerken Überläufe aufgetreten und besitzt das Wahlergebnis zumindest eine innere Konsistenz, können allenfalls Indizien für Manipulationen sprechen. Falsche Beschriftungen lassen sich auch hier nur beweisen, wenn sie nicht zwischenzeitlich vernichtet wurden. Aussagen von Wählerinnen und Wählen stellen auch hier nur Indizien dar.

Die Vielfalt der Manipulationsmöglichkeiten bei Wahlcomputern erfordert in jedem Fall einen großen zeitlichen und finanziellen Aufwand bei der Überprüfung, der im Einzelfall den Wert des geprüften Gerätes übersteigen kann. Weder die fehlerfreie Durchführung von Wahlsimulationen (siehe (KRG07, S. 13f.)) noch ein erfolgreicher Vergleich des Binärcodes der Wahlcomputersoftware mit einem nichtmanipulierten Original (siehe (Sie06)) können Manipulationen von Hardware-Komponenten wie CPU oder Mikrocontroller für Ein- und Ausgabeeinheiten oder Speichersubsysteme ausschließen. Alle Bauteile müssen also einzeln überprüft werden. Manipulierte Prozessoren könnten zerstörungsfrei mit Röntgenaufnahmen oder Analysen von Seitenkanälen wie Zeitverhalten, Stromverbrauch oder Abstrahlung oder durch zerstörende Prüfungen entdeckt werden. Selbst das Auslesen der Wahlcomputersoftware aus den Speicherbausteinen garantiert keine Manipulationsfreiheit der Bausteine selbst, wenn dieser – etwa in Abhängigkeit von an bestimmten Anschlüssen angelegten Spannungen – unterscheiden kann, ob er eingebaut in einem Wahlcomputer oder in einem externen Auslese- oder Programmiergerät betrieben wird.

Zusammenfassend lässt sich konstatieren, dass die Entdeckung von Manipulationen bei Überprüfungen nach einer Wahl umso aufwendiger und weniger erfolgversprechend ist, je

[7] Sie dazu die Datendefinition des § 202a Abs. 2 StGB.
[8] Siehe (Wik) mit vielen Nachweisen.

komplexer die eingesetzten technischen Wahlhilfsmittel sind. Technische Komplexität führt, wie auch Schneier in (Sch04, S. xi.) feststellt, zu verringerter *security*.

3.4 Sicherheitsregeln

Zur Erfüllung der vom Gesetzgeber festgeschriebenen Anforderungen an Wahlorganisation und -techniken dienen Regelwerke, die als Rechtsnormen niedergelegt sind. Im Fokus der Arbeit liegen dabei solche Regelungen, die Angriffe erschweren oder undurchführbar machen oder zumindest deren Entdeckung ermöglichen oder wenigstens erleichtern sollen.

Schneier weist in (Sch04, S. 308.) darauf hin, dass Sicherheitsregeln knapp, präzise, verständlich und widerspruchsfrei sein sollten, um nicht weitgehend ignoriert zu werden. Diesen Forderungen können rechtliche Regelwerke nicht oder nur selten gerecht werden, sie sind vielmehr oft aufgebläht, auslegungsbedürftig, unverständlich und widersprüchlich. Wie auch die Schutzziele für Wahlen (siehe Abschnitt 3.1, S. 26) müssten die Sicherheitsregeln daher erst aus den einschlägigen Rechtsnormen und den prinzipbedingten Eigenheiten der verwendeten Wahltechniken abgeleitet werden, damit diese den Schneierschen Anforderungen genügen.

Während Sicherheitsregeln das „Wie“ beschreiben, müssen sie im Rahmen einer umfassenden Sicherheitspolitik von einem „Wer“ und einem „Warum“ begleitet werden. Ersteres legt die Verantwortungsbereiche von beteiligten Personen fest, letzteres erklärt die Gründe für die einzelnen Regelungen. Nicht zuletzt muss festgeschrieben sein, welche Folgen Verstöße gegen die Sicherheitsregeln nach sich ziehen, sowohl für die Wahlen als solche als auch für die Verantwortlichen der Regelbrüche.

An drei Beispielen sollen Defizite, Probleme und Fehler derzeitiger oder fehlender Regelungen beleuchtet werden. Dabei handelt es sich um die Verwendung von Bleistiften für das Ausfüllen von Stimmzetteln, die Erkennung der auf Wahlcomputern verwendeten Software und deren Version sowie den allgemeinen Umgang mit erkannten Wahlmanipulationen.

Nach § 50 Abs. 2 BWO soll in der Wahlzelle ein Schreibstift bereitliegen, über den keine weitergehenden Aussagen gemacht werden. Das Fehlen jeglicher Sicherheitsanforderungen an den verwendeten Stift ermöglicht auch die Verwendung von Bleistiften für das Ausfüllen von Stimmzetteln. Derart ausgefüllte Stimmzettel sind jedoch, wie in Abschnitt 3.2.1, S. 35 beschrieben, nicht gegen nachträgliche Veränderungen geschützt. Auch hat die Verwendung von Bleistiften bei Wahlen keine rechtlichen Konsequenzen, wie ein Urteil des Wahlprüfungsgerichtes beim Hessischen Landtag zur Gültigkeit der Landtagswahl 1999 in (Wah99, S. 2355.) zeigt. Daraus lassen sich für das vorliegende Beispiel vier Folgerungen ableiten. Erstens bedarf es einer Sicherheitsregel, die den ausschließlichen Einsatz von dokumentenechten Stiften für papierbasierte Wahlen verlangt. Diese muss zweitens anhand ihrer Folgen – der Verhinderung nachträglicher Änderungen von ausgefüllten Stimmzetteln – den beteiligten Personen erklärt werden. Die Verantwortung für die Durchsetzung dieser Regelung muss drittens auf die Wahlvorsteherin oder den Wahlvorsteher übertragen werden. Viertens müssen die Rechtsfolgen eines Verstoßes definiert werden, allgemein durch die Notwendigkeit einer Wahlwiederholung und in Bezug auf die Verantwortlichen für den Regelverstoß durch deren Pflicht zur Übernahme der Kosten der Nachwahl.

Regelungen zur Feststellung der auf Wahlcomputern verwendeten Software sind teilweise widersprüchlich oder existieren gar nicht erst. In der Anlage 1 zur BWahlGV wird in B.1 festgelegt, dass die installierte Software eindeutig identifizierbar sein muss. § 10 Abs. 1 BWahlGV, der die Aufgaben des Wahlvorstandes vor Beginn der Stimmabgabe festschreibt, verlangt dies jedoch nicht vom Wahlvorstand. Auch bieten die in Anlage 2 und 3 zur BWahlGV abgedruckten Vorlagen für Wahlniederschriften keine Möglichkeit zur Eintragung der verwendeten Software und der Bestätigung, dass deren Version mit der im Herstellerhandbuch oder auf dem Typenschild abgedruckten übereinstimmt. Gleichwohl behauptet das BMI in (Bun06, 1.3.) auf Anraten der PTB, wie Richter in (Sie06) eingesteht, der Wahlvorstand kontrolliere am Wahltag „die Identifikation [des] Softwareprogramms". Gleichzeitig verlangt B.2.1 der Anlage 1 zur BWahlGV, dass eine Veränderung der installierten Software nicht unbemerkt bleiben darf. Weil eine explizite Authentifizierung der eingesetzten Software, wie sie das BMI in (Bun06, 3.2.) inhaltlich von der Identifizierung der Software trennt, vom Wahlvorstand sowohl mangels Wissen als auch notwendiger Technik nicht durchführbar ist und explizit dem Wortlaut der Regelung widerspäche, bliebe nur, die Norm derart auszulegen, dass solche Veränderungen zumindest der PTB gegenüber nicht unbemerkt bleiben dürfen. Die PTB prüft jedoch nicht jeden Wahlcomputer bei jeder Wahl, womit Veränderungen der Software als solche unbemerkt bleiben könnten. Auch dies ist ein Widerspruch zum Text der Norm und daher rechtlich nicht zulässig. Als Lösung kann also hier nur in Betracht kommen, sowohl Identifizierung als auch Authentifizierung als explizite Aufgaben des Wahlvorstandes festzuschreiben, die Verantwortung der Vorsteherin oder dem Vorsteher zu übertragen und allen Beteiligten Wissen und Technik zur Verfügung zu stellen, damit sie diesen Aufgaben gerecht werden können.

Nicht nur in Bezug auf die beschriebene Verwendung von Bleistiften zum Ausfüllen von Stimmzetteln stellt sich die Frage nach dem Umgang mit erkannten Wahlfehlern. Gerade dann, wenn es zu bewiesenen Wahlmanipulationen kam, widerspricht die zusätzliche Anforderung des Beweises der Mandatsrelevanz dieser Manipulationen jeder effektiven Durchsetzung von Sicherheitsregeln. Dies geschieht tatsächlich auch dann, wenn die Verletzung von Sicherheitsregeln nicht ursächlich für die Durchführbarkeit der jeweiligen Wahlmanipulation war. Liegt ein solcher Fall allerdings vor, ist die Folgenlosigkeit für jeden zukünftigen Versuch der Regeldurchsetzung noch gravierender. Keine der einschlägigen Normen des Wahlstrafrechts ist bei Fahrlässigkeit anwendbar. Selbst schwere Verstöße gegen Sicherheitsregeln zeitigen keine Folgen für die Verantwortlichen, die über einen Ausschluss von der weiteren Mitarbeit an Wahlorganisation und -durchführung hinausgehen. Sollte sich dies in Zukunft nicht ändern, wird die mangelhafte Einhaltung der Sicherheitsregeln weiter Bestand haben und damit die Durchführung von Angriffen auf Wahlen erleichtern oder sogar erst ermöglichen.

3.5 Common Criteria

Um bei der Beschreibung und Bewertung von Sicherheitsanforderungen und -eigenschaften das Rad nicht immer wieder neu erfinden zu müssen, liegt es nahe, die Kriterien, nach denen Computersysteme beschrieben, bewertet und zertifiziert werden sollen, zu standardisieren. Mit dem Ziel der Vereinheitlichung der jeweiligen nationalen und regionalen Standards wurden in den neunziger Jahren des zwanzigsten Jahrhunderts die *Common Criteria for*

Information Technology Security Evaluation – kurz *Common Criteria* oder *CC* – entworfen und 1999 in Version 2.3 als ISO-Standard angenommen. Derzeit ist die Version 3.1[9] aktuell. Beschreibung und Bewertung der CC beziehen sich wesentlich auf (And01, S. 529ff.).

Grundlegendes Prinzip der CC ist die Evaluation eines konkreten Produktes (*TOE – target of evaluation*, auch Evaluationsgegenstand) gegen ein Schutzprofil (*PP – protection profile*) mit einer darin festgelegten Prüftiefe (*EAL – evaluation assurance level*).

Das Schutzprofil selbst soll implementationsunabhängig die einzelnen Sicherheitsanforderungen – jeweils mit Begründung und Prüftiefe – aufführen und dabei die Annahmen an die Umgebung, in der das Produkt eingesetzt werden soll, mit identifizierten Bedrohungen sowie die jeweiligen Schutzziele und -anforderungen für alle Produktkomponenten darstellen. Die Begründung der geforderten Schutzziele soll dabei durch wechselseitige Gegenüberstellung mit den Bedrohungen geschehen. Einerseits soll damit gezeigt werden, wie jeder Bedrohung durch eines oder mehrere Schutzziele begegnet werden kann, andererseits soll nachgewiesen werden, dass jedes aufgeführte Schutzziel vor dem Hintergrund der getroffenen Annahmen an die Umgebung und der Bedrohungen tatsächlich notwendig ist.

Die Liste der Prüftiefen reicht von EAL1 bis EAL7, wobei EAL1 die geringsten Anforderungen stellt und EAL7 die höchsten. Für eine Bewertung und Zertifizierung nach EAL1 reicht es demnach aus, wenn der Evaluationsgegenstand ausschließlich funktional gegen das Schutzprofil getestet wird. EAL3 fordert dann schon eine methodische Testdurchführung und tiefgehende Überprüfung des TOE. Eine Zertifizierung nach EAL7 ist demgegenüber nur erreichbar, wenn der TOE auf einem formal verifizierten Entwurf basiert und die Evaluation gegen das Schutzprofil sowohl methodisch als auch tiefgehend erfolgt.

Wenn das Schutzprofil tatsächlich vollständig implementationsunabhängig ist, kann es für eine Evaluation notwendig sein, dieses an ein bestimmtes TOE anzupassen. Das Ergebnis dieser Anpassung sind produktabhängige Sicherheitsvorgaben (*ST – security target*).

Im Idealfall finden die CC wie folgt Anwendung: Zuerst wird ein Schutzprofil erstellt. Die kann und sollte durch die Kundin oder den Kunden geschehen. Dieses Schutzprofil selbst wird einer Evaluation unterzogen. In Anpassung an einen bestimmten Evaluationsgegenstand werden aus dem Schutzprofil Sicherheitsvorgaben abgeleitet, die auch wieder evaluiert werden. Zuletzt findet die Evaluation des konkreten Produkts gegen die Sicherheitsvorgaben statt, die bei Erfolg zu einer Zertifizierung führt. Am Ende sollte dann eine Liste der Schutzprofile nebst den abgeleiteten Sicherheitsvorgaben und den evaluierten Produkten stehen.

Gleichwohl sind die CC nicht ohne strukturelle Defizite. Beschreibung und Bewertung von Sicherheitseigenschaften beschränken sich ausschließlich auf die technische Seite der betrachteten Systeme, während Fragen zu Sicherheitsverfahren vollständig außen vor bleiben. Es existieren keine Regelungen zur Methodik bei der Durchführung von Evaluationen. Ob die gewählte Methodik im Einzelfall sinnvoll oder überhaupt anwendbar ist oder nicht, hat keinen Einfluss auf die Gültigkeit der ausgestellten Zertifizierung. Reevaluationen von Produkten, aus welchen Gründen diese auch immer notwendig sein mögen, werden von der CC als außerhalb ihres Fokus erklärt. Insbesondere müssen Zertifizierungen keine Gültigkeitsbeschränkungen besitzen.

Das größte Manko der CC ist jedoch, dass sie nicht fordert, dass die im Schutzprofil getroffenen Annahmen an die Umgebung mit der Realität übereinstimmen müssen. Im engeren

[9] Für den Standard siehe http://www.commoncriteriaportal.org (Stand: 11.06.2008).

Sinne werden Produkte damit nur gegen die im Schutzprofil beschriebene Welt evaluiert, die ausgestellten Zertifizierungen können daher abhängig von der Größe der Diskrepanz zwischen getroffenen Annahmen und Realität tatsächlich wertlos sein, wie es beim Digitalen Wahlstift-System der Fall ist.

Das Digitale Wahlstift-System besteht aus einem Digitalstift, in dem eine Kugelschreibermine, eine Kamera, ein Prozessor, ein Datenspeicher, eine Ein- und Ausgabeeinheit und eine Batterie integriert sind, dem digitalen Papier, auf dem die Stimmzettel gedruckt sind, einer Dockingstation an einem Rechner zur Datenübertragung zwischen Stift und Computer sowie der erforderlichen Wahlsoftware auf dem Rechner. Die Hamburger Bürgerschaft beschloss am 26.04.2006 die flächendeckende Einführung des Digitalen Wahlstift-Systems zur Bürgerschaftswahl Anfang 2008. Am 28.02.2007 veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein von der Prüfstelle für IT-Sicherheit des DFKI erstelltes CC-Schutzprofil für ein solches System ((VV07)). Dem Schutzprofil liegen die CC in Version 2.3 zugrunde, die Prüftiefe beschränkt sich – von zwei Erweiterungen abgesehen – auf EAL3. Das Schutzprofil wurde am 14.03.2007 vom BSI zertifiziert ((Bun07a)).

Die von der Autorin und dem Autor getroffenen Annahmen über die Einsatzumgebung des Evaluationsgegenstandes stellen sich teilweise als verkürzt und teilweise als falsch dar. Dies soll beispielhaft anhand der von ihnen beschriebenen „Generellen Sicherheitserwartungen an den EVG“ ((VV07, S. 13.)) und der „EVG-Sicherheitsumgebung“ ((VV07, S. 17ff.)) gezeigt werden.

Die aufgeführten Wahlrechtsgrundsätze des Art. 38 Abs. 1 GG stellen nur eine Teilmenge der verfassungs- und wahlrechtlichen Regelungen dar, denen Wahltechniken genügen müssen. Insbesondere fehlen die Grundsätze der Öffentlichkeit nach Art. 20 Abs. 1 GG und der Überprüfbarkeit nach Art. 41 GG.[10]

Das Vorgehen, die Wahlrechtsgrundsätze ausgewählten Sicherheitserwartungen zuzuordnen, ist vor dem Primat des Rechts vor der eingesetzten Technik verfehlt. Richtig und notwendig wäre hier eine formale Ableitung der Anforderungen an *safety* und *security* aus den einschlägigen Rechtsnormen, wie in Abschnitt 3.1 gezeigt. Erst danach können die Sicherheitserwartungen sinnvoll klassifiziert und zusammengefasst werden. Damit würden auch inhaltliche Fehler vermieden wie die Nichtbeachtung des Grundsatzes der unmittelbaren Wahl unter 3. und der falsche Verweis auf die Wahlgleichheit unter 4., wo statt dessen auf den Grundsatz der Wahlfreiheit zu verweisen wäre.

Grundsätzlich verfehlt sind jedoch die folgenden Annahmen über die an der Wahl beteiligten Personenkreise. So wird in (VV07, S. 13.) angenommen, der Wahlvorstand sei vertrauenswürdig und würde den Evaluationsgegenstand nicht absichtlich manipulieren. Diese Annahme ist abwegig, wie etwa am Beispiel des Wahlfälschungsskandals von Dachau auf Seite 44 gezeigt wurde. In (VV07, S. 19.) wird sie jedoch noch erweitert und einerseits personell auf Administratorinnen und Administratoren ausgedehnt und andererseits inhaltlich um den Ausschluss von Sorglosigkeit und Nachlässigkeit erweitert. Allein Wählerinnen und Wähler werden als mögliche Angreiferinnen und Angreifer angenommen und die Wahlkabinen werden neben dem Transport der Daten nach Wahlende zur Wahlzentrale als einzig mögliche Angriffsorte betrachtet. A priori davon auszugehen, dass bestimmte Angriffe nicht stattfinden oder bestimmte Angreifertypen nicht auftreten können, vereinfacht die Entwick-

[10] Siehe die ausführliche Behandlung der Thematik in Teil 2.

lung sicherer Systeme, wie Schneier in (Sch04, S. 212.) zeigt, ungemein. Solche Systeme sind dann zwar als sicher definiert, erweisen sich jedoch zwangsläufig in einer Realität, die sich nicht an die getroffenen Annahmen hält, als inhärent unsicher und damit grundsätzlich angreifbar.

3.6 Zwischenfazit

Zusammenfassend lassen sich folgende Zwischenergebnisse herleiten.

Grundlagen einer sinnvollen und umfassenden Analyse der Anforderungen an *safety* und *security* von Wahlgeräten und Wahlcomputern sind eine ausführliche Darstellung der rechtlichen Bedingungen von und Anforderungen an Wahlen und deren Durchführung, eine darauf aufbauende fundierte Ableitung der Schutzziele aus diesen Anforderungen sowie eine unvoreingenommene Betrachtung potentieller Angreifertypen, möglicher Angriffe und deren Erfolgsaussichten sowie eventuelle Gegenmaßnahmen. Kontraproduktiv sind fehlendes Wissen über die rechtlichen Rahmenbedingungen von Wahlen sowie pauschale und ungerechtfertigte Ausschlüsse von möglichen Angriffen und Angreifertypen.

Soll die Analyse darüber hinaus als Grundlage für eine Überprüfung der Zulassungs- und Verwendungsfähigkeit konkreter Wahlhilfsmittel, Wahlgeräte oder Wahlcomputer dienen, muss sie in einer stärker formalisierten Form erfolgen, als in dieser Arbeit gewählt wurde. Unter der Voraussetzung, dass die Übereinstimmung zwischen Realität und getroffenen Annahmen beweiskräftig nachgewiesen wird, sind CC-Schutzprofile dafür grundsätzlich geeignete Formen.

4 Technik-, Sicherheits- und Diskursgeschichte

Der abschließende Teil der Arbeit vermittelt anhand der Geschichte der Wahlgeräte und Wahlcomputer und ihres Einsatzes bei Wahlen in der BRD einen Überblick über die dabei aufgetretenen Probleme in den Bereichen *safety* und *security* sowie die darauf folgenden Reaktionen der Verantwortlichen in der Politik, bei den Herstellern, bei den Prüferinnen und Prüfern sowie in den Wahlorganen einerseits sowie der Presse und Öffentlichkeit andererseits. Dabei sollen insbesondere diejenigen Ereignisse und Reaktionen eingehender betrachtet werden, die bereits im zweiten Teil Gegenstand der eher theoretischen Betrachtung der Sicherheitsproblematik waren.

Während die Wahlgesetze zum ersten und zweiten Deutschen Bundestag keine Regelungen über mögliche Alternativen zur Urnen- oder Briefwahl enthielten, erlaubte das erste Bundeswahlgesetz[11] in § 35 Absatz 3 dem Bundesministerium des Innern, „anstelle von Stimmzetteln amtlich zugelassene Stimmenzählgeräte“ zur Verwendung bei Wahlen zuzulassen. In keiner der drei Lesungen im Bundestag wurde über diese Änderung gegenüber den beiden vorherigen Wahlgesetzen und ihre Folgen debattiert. Auch die Anforderungen an die „Stimmenzählgeräte“ für eine amtliche Zulassung wurden nicht geregelt.

Die erste öffentliche Vorstellung einer dieser „Wahlmaschinen“, wie sie *Die Zeit* in (Zei60) nannte, fand Anfang November 1960 in Oberhausen statt. Das vorgestellte mechanische Wahlgerät „System Darmstadt“ (siehe Abbildung 11)[12] besaß zu diesem Zeitpunkt noch keine Zulassung, die älteste nachweisbare stammt von 1969.[13]

Verwendung fanden die Wahlgeräte erstmalig am 17. September 1961 zur Bundestagswahl, nachdem das BMI kurzfristig eine entsprechende Verordnung erlassen hatte.[14] Das „Haus der Geschichte“ in Bonn besitzt die Kopie einer Bekanntmachung des Wahlamtes der Stadt Darmstadt (Mag61), in der den Wahlberechtigten unter anderem mitgeteilt wurde:

> „Die Bedienung des Stimmenzählgerätes ist ebenso einfach wie die Bedienung eines Automaten. Das Gerät arbeitet einwandfrei.“

Auf Sicherheitsfragen wurde dabei nicht eingegangen. Stattdessen besaß das Wahlgerät eine Eigenschaft, die es nach heutigen Maßstäben nicht mehr zulassungsfähig machen würde: Es klingelte. Das Wahlamt schrieb dazu:

> „Es ertönt ein Klingelzeichen, die Erststimme ist abgegeben.“

Diese Funktionalität wurde mit der Begründung des Wahlgeheimnisschutzes später entfernt, wobei allerdings nach Aussage von Groß nicht mehr nachvollziehbar ist, zu welchem Zeitpunkt dies geschah.

In der Beantwortung einer Schriftlichen Anfrage durch das BMI vor dem Bundestag (Deu73) wurden die Landeswahlleitungen zu ihren Erfahrungen bei der Bundestagswahl

[11] Bundeswahlgesetz vom 7. Mai 1956 (BGBl. I S. 383).

[12] Die Informationen zu allen Wahlgeräten wurden von Johann Groß, dem derzeitigen Distributor aller mechanischen und elektromechanischen Wahlgeräte in der BRD, und vom „Haus der Geschichte“ in Bonn zur Verfügung gestellt.

[13] Entscheidung des BMI vom 14.08.1969 - V I 5 - 121 115/3.

[14] Verordnung über die Verwendung von Stimmenzählgeräten bei Wahlen zum Deutschen Bundestag vom 24. August 1961 (BGBl. I S. 1618).

„System Darmstadt“ Das Gerät besteht aus einem etwa tischhohen Gehäuse mit einem Aufbau, auf dem die zehn Wahlalternativen (maximal neun verschiedene Wahlvorschläge und die Stimmenthaltung) abgedruckt sind und sich jeweils darunter ein „Stimmschlitz“ befindet. In diese können „Wählmarken“ gesteckt werden, die ein rein mechanisches Zählwerk mit elf Zählern (zehn Wahlalternativen und ein Summenzähler) auslösen. Die Wählmarken werden dann in Beuteln in einer eingebauten Wahlurne aufgefangen, jeweils ein Beutel für jeden Stimmschlitz. Für wahlstatistische Erhebungen können verschiedenfarbige Wählmarken verwendet werden. Das Wahlergebnis ist damit also grundsätzlich unabhängig von der Anzeige der Zählwerke überprüfbar.

„System Darmstadt T“ Anstelle von Stimmschlitzen für die Aufnahme von Wählmarken besitzt dieses Gerät Tasten („T“) für die Stimmabgabe. Durch Drücken der Taste fließt Strom durch eine Spule, die elektromagnetisch ein Zählwerk auslöst. Der gegenüber rein mechanischen Geräten eingesparte Platz erlaubt die Unterstützung von bis zu fünfzehn verschiedenen Wahlvorschlägen. Zusätzlich gibt es eine Taste für die Stimmenthaltung.

Abbildung 11: Mechanische Wahlgeräte „System Darmstadt“

1973 mit der Aussage zitiert, der Zeitgewinn bei der Verwendung von Wahlgeräten sei „relativ unbedeutend“ und die Geräte seien extrem störanfällig. So seien in Nordrhein-Westfalen von 86 eingesetzten Wahlgeräten bei der Wahl 11 ausgefallen. Das BMI sah aufgrund dieser „zurückhaltende[n] Beurteilung“ keine Veranlassung, die Anschaffung dieser Geräte zu fördern.

Gleichwohl wurde durch das BMI zwei Jahre später eine neue und erweiterte Bundeswahlgeräteverordnung erlassen.[15] Sie ersetzte die Verordnung von 1961, der auch sprachlich anzumerken ist, dass sie kurzfristig zur Bundestagswahl geschrieben wurde, um bereits existierenden Wahlgeräten einen Einsatz zu ermöglichen. Die neue Verordnung enthielt erstmals auch Richtlinien für die Bauart von Wahlgeräten. Die Störanfälligkeit der Wahlgeräte blieb dennoch bestehen, wie die Bundesregierung in (Bun77) – drei von 236 eingesetzte Geräte fielen aus – zugeben musste. Jedoch seien in keinem Fall Stimmen verloren gegangen. Anders war dies bei der Bundestagswahl 1980, wie aus (Wah81, Anlage 10) ersichtlich ist.

Im Wahlkreis 247 (Sankt Wendel, Saarland) wichen die Zahlen der abgegebenen Erststimmen um 51 und der Zweitstimmen um 29 von den Zahlen der eingetragenen Wählerinnen und Wähler ab, ohne dass die verantwortlichen lokalen Wahlorgane in den Wahlniederschriften dazu Stellung nahmen. Der siegreiche Bewerber der CDU erhielt in diesem Wahlkreis nach dem amtlichen Endergebnis nur 331 Stimmen mehr als sein SPD-Kontrahent (72.384 zu 72.053), die CDU gewann bei den Zweitstimmen mit nur 279 Stimmen Vorsprung vor der SPD (70.293 zu 70.014). Wenn die FDP nur 131 Zweitstimmen mehr in diesem Wahlkreis bekommen hätte, wäre ihr ein zusätzliches Bundestagsmandat zugekommen – auf Kosten der CDU. Während in allen anderen bekannten Fällen von Wahlfehlern bei der Verwendung

[15] Bundeswahlgeräteverordnung vom 3. September 1975 (BGBl. I S. 2459).

„Schematus“ Ein rein mechanisches Wahlgerät mit zehn „Zugfächern“ an der Frontseite, neun für Wahlvorschläge und eines für die Stimmenthaltung. Die Betätigung der Zugfächer löst mechanische Zählwerke aus, jeweils eines für jedes Zugfach und eines für die Summe der abgegebenen Stimmen.

„Schematus E“ Trotz des gleichen Namens handelt es sich um ein völlig neuentwickeltes Wahlgerät, das elektronisch („E“) arbeitet. Auch hier gibt es jedoch ausschließlich mechanische Zählwerke. Unterstützt werden neben der Stimmenthaltung bis zu fünfzehn Wahlvorschläge.

„Schematus EU“ Das „EU“ steht für „Elektronik Umbau“. Es handelt sich also um Umbauten rein mechanischer Wahlgeräte, bei denen die Gehäuseöffnungen für die Zugfächer in der Front verschlossen wurden und statt dessen Tasten auf dem Gerät installiert wurden, mit denen die mechanischen Zählwerke elektromagnetisch ausgelöst werden können. Die Zählwerke selbst wurden dabei nicht verändert, weshalb also auch hier nur neun Wahlvorschläge neben der Stimmenthaltung unterstützt werden.

Abbildung 12: Mechanische Wahlgeräte „Schematus“

von Wahlgeräten oder Wahlcomputern die Diskrepanzen im niedrigen einstelligen Bereich lagen, war die Fehlerzahl hier in mindestens drei Wahllokalen signifikant höher: Die Anzahl der Fehler bei den Zweitstimmen erreichte mehr als 20% der für eine Mandatsrelevanz zugunsten der FDP notwendigen Stimmen und immer noch mehr als 10% in Bezug auf die SPD. Dennoch haben weder die zuständigen Landes- und Bundeswahlorgane noch der Wahlprüfungsausschuss des Bundestages darin ein Problem gesehen. Stattdessen wies letzterer den Einspruch „als offensichtlich unbegründet“ zurück. Dieses Beispiel zeigt, dass die Personen, die hier die betreffende Entscheidung gefällt haben, die grundsätzliche Problematik der Manipulierbarkeit von Wahlgeräten vollständig ignoriert haben. Ihre Äußerungen lassen zudem vermuten, dass hier schlicht nicht sein konnte, was nicht sein durfte. Dies zeigt sich auch daran, dass keine zwei Jahre später die Bundesregierung in (Bun83) entgegen den Tatsachen behaupten konnte, für die Diskrepanz bei den Wahlstimmen sei das technische Versagen „eines Stimmenzählgerätes“ verantwortlich und gleichzeitig zugeben musste, dass es im gleichen Wahlkreis bei der Bundestagswahl 1983 wieder kein konsistentes Wahlergebnis gab.

In Reaktion auf die Verwendung von Wahlgeräten bei der Bundestagswahl 1990 wurde der erste Einspruch gegen die Wahl eingelegt, dessen Begründung explizit auf der Nichtüberprüfbarkeit von mit Wahlgeräten erzeugten Wahlergebnissen beruht. Wie zu erwarten war, wurde dieser Einspruch vom Wahlprüfungsausschuss des Bundestages, wie (Wah91, Anlage 16) zeigt, „als offensichtlich unbegründet“ zurückgewiesen. Auch ein Antrag auf Erlass einer einstweiligen Verfügung gegen die Verwendung von Wahlgeräten anstelle von Stimmzetteln bei der Kommunalwahl in Hessen 1993, der auch auf dem Argument der fehlenden Kontrollierbarkeit und wahlrechtlichen Nachvollziehbarkeit der Wahl bei der Ver-

wendung von Wahlgeräten basierte, wurde abgewiesen, wenn auch (Sta93) dafür nur formale Gründe anführt.[16]

4.1 Übergang zu Wahlcomputern

Wie schon bei der ersten Verordnung zu Wahlgeräten von 1961 stand auch 1999 ein bereits produziertes Gerät Modell für die Ausformulierung neuer rechtlicher Regelungen insbesondere zu den technischen Anforderungen für eine Bauartzulassung. Diesmal war es jedoch ein Wahlcomputer – ein Nedap ESD1 (siehe Abbildung 13)[17] –, juristisch als „rechnergesteuertes Wahlgerät“ klassifiziert, der gleichzeitig technische Grundlage für die Novellierung der BWahlGV und erster zugelassener Wahlcomputer nach deren neuen Fassung war. Dass der für die technische Prüfung zur Bauartzulassung Verantwortliche diese Koinzidenz in (Sie06) im Nachhinein als das Ergebnis mangelnder Kreativität der Beteiligten und im Übrigen für unproblematisch erklären wird, ist dann selbst bezeichnend für den unkritischen Umgang mit dem Thema Sicherheit. Zumindest kam die Bauartzulassung dann pünktlich zur Europawahl in Köln am 13. Juni 1999, um einen Wahlcomputereinsatz zu ermöglichen. Auch bei den Kommunalwahlen am 12. September 1999 wurden Wahlcomputer eingesetzt, wie (CW:99) berichtete. Sicherheitsfragen wurden auch hier nicht angesprochen, allerdings wurden andere Sicherheitsvorkommnisse aufgezählt, über die sonst eher selten berichtet wird:

> „Auch in anderen Gemeinden ist es ein offenes Geheimnis, daß Wahlhelfer betrunken amtierten, Wahllokale verspätet öffneten oder zu früh schlossen, daß Wahlzettel am nächsten Tag unter Schultischen auftauchten und Auszählungen wiederholt werden mußten.“

Auswirkungen auf die in breiter Öffentlichkeit vertretene Annahme, Mitglieder von Wahlvorständen seien als Sicherheitsrisiken grundsätzlich auszuschließen, hatte dieses Eingeständnis allerdings genauso wenig wie der im März 2002 aufgedeckte Wahlfälschungsskandal von Dachau, auf den schon in Abschnitt 3.3 auf Seite 44 hingewiesen wurde. In diesem Fall wurden zumindest zwei Stadträte der CSU, bei denen es sich aufgrund ihrer Zutritts- und Zugangsmöglichkeiten unzweifelhaft um Innentäter handelte, auch strafrechtlich belangt. Einer der beiden hatte vor der Presse erklärt, bereits seit 1984 Wahlfälschungen begangen zu haben.

Die Anzahl der Städte und Gemeinden, die Wahlcomputer verwendeten, stieg nach (Inn02) zur Bundestagswahl 2002 auf 29. Die Aussage, es sei bei den bisherigen Wahlen zu „keinen nennenswerten Problemen bei der Stimmabgabe“ gekommen, ist bezeichnend für die von den Verantwortlichen an den Tag gelegte Ignoranz gegenüber Sicherheitsfragen, blieb aber presseöffentlich unkommentiert. Das Mantra lautete und lautet vielmehr, dass Wahlcomputer, wie (Bun02) ausführte, „auf Grund ihrer sicheren und einfachen Handhabung das Verfahren für Wähler und Wahlvorstand“ erleichtern. Gleichzeitig wurden und werden hier die beiden unterschiedlichen Sicherheitsbegriffe *safety* und *security* vermischt. Wenn allgemein über „Sicherheit“ gesprochen oder geschrieben wurde, dann sollte damit, wie dies etwa

[16] Zur Begründung der Abweisung diente das in Abschnitt 2.3.1 auf Seite 15 beschriebene Rechtskonstrukt, ausführlicher dazu: (Poh07, S. 12).

[17] Die Beschreibung der Wahlcomputer folgt hier (Bun06) und (GHB+06).

„Nedap ESDx“ Bei den in der BRD zugelassenen Wahlcomputern handelt es sich entweder um Modelle ESD1 oder ESD2 mit weiteren Unterteilungen nach Hardware- und Software-Version. Sie bestehen aus dem eigentlichen Wahlcomputer und einer per Kabel verbundenen Bedieneinheit für den Wahlvorstand. Der eigentliche Wahlcomputer besteht aus einem großen Tastenfeld mit 1116 Tasten, auf dem Wahlzettel befestigt werden können, und einem kleinen Display zur Information von Wählerinnen und Wählern. Auf der Rückseite befindet sich ein Drucker, ein Steckplatz für das Stimmenspeichermodul und das Computermodul. Dessen Hardware besteht aus einem Motorola 68000 als Prozessor, 16 Kilobyte Arbeitsspeicher, 256 Kilobyte Programmspeicher, 8 Kilobyte Speicher für Protokolldaten und zwei seriellen und einem parallelen Anschluss. Vor der Wahl werden auf dem Stimmenspeichermodul die Konfigurationsdaten gespeichert. Dazu muss das Modul mit Hilfe eines Standard-PCs, der Software IWS und einer externen Programmiereinheit beschrieben werden. Während der Wahl werden auf dem Modul, dann eingesteckt in den Wahlcomputer, die Daten der abgegebenen Stimmen gespeichert und danach wieder am PC ausgelesen und verarbeitet. Der Wahlcomputer besitzt ein Gesamtgewicht von etwa 28 Kilogramm.

Abbildung 13: Wahlcomputer des Herstellers Nedap

auch (Sch03) zeigt, zumindest immer der Eindruck erweckt werden, es gehe um *security*. Gleichwohl zeigt der Nachtrag „Die Automaten haben eine vierfache Sicherung“, dass die vermeintliche *security* hier mit einem Argument aus dem Bereich *safety* begründet wird – die „vierfache Sicherung“ meint hier nichts anderes als die in Abschnitt 2.3.5 auf Seite 20 zitierte Anforderung der redundanten Stimmenspeicherung. Auch der deutsche Distributor der Nedap-Wahlcomputer und Hersteller der zugehörigen Wahl- und Geräteanwendungssoftware, Herbert Schulze Geiping von HSG Wahlsysteme, trug seinen Anteil zu dieser Vermischung bei und ließ sich in (Win04) damit zitieren, dass Wählen per Knopfdruck sicher sei, weil „jede Gemeinde halte mindestens ein Ersatzgerät parat, es gebe eine Hotline, und im Ernstfall sorge seine Firma in Windeseile für weitere Ersatzgeräte“, obwohl keine dieser Maßnahmen auch nur entfernt etwas mit *security* zu tun haben. Auch das Wahlgeheimnis musste für eine solche Verwirrung herhalten. Es sei „ohnehin gewahrt“, weil die Wahlcomputer versiegelt in die Wahllokale gebracht und dort von den Wahlvorständen mit einem Schlüssel freigeschaltet würden. Dass diese Maßnahmen nur ganz entfernt den Schutzbereich des Wahlgeheimnisses tangieren und nicht etwa deren fundamentale Schutzmaßnahmen darstellen, wurde offensichtlich entweder nicht verstanden oder bewusst falsch dargestellt. Selbst wenn Aspekte der *security* tatsächlich kritisch angesprochen wurden wie in (Moh04), erscheint der falsche Verweis auf einen „dreimonatigen Härtetest“, den die PTB angeblich durchführen würde, zumindest als gleichzeitige rhetorische Verharmlosung.

Obwohl bereits nach den schwerwiegenden Problemen mit Wahlgeräten und Wahlcomputern bei der US-Präsidentenwahl 2000 erste Ansätze einer öffentlichen Diskussion über die Sicherheit dieser technischen Wahlhilfsmittel aufkamen, fand das Thema erst im Vorgriff auf die US-Wahl 2004 einen breiteren Niederschlag in der Presse. Zwar hatte die c’t schon 2000 in (Sti00) einen kurzen Überblick über die Sicherheitsprobleme und sogar ihre Vorge-

schichte gegeben, aber erst 2004 in (Sie04) wird dieses Thema auch in technischen Details behandelt. Angesprochen wurden dabei etwa unterschiedliche Manipulationsmöglichkeiten, Probleme bei der Durchsetzung von Sicherheitsregelwerken und die grundsätzliche Nichtbeweisbarkeit der Manipulationsfreiheit von Software. Die Wahldurchführung in den USA war dann erwartungsgemäß auch wieder von extremen Ungereimtheiten überschattet, was selbst die heimische Politik nicht mehr unkommentiert lassen konnte. Nur leider waren auch diesmal nicht alle Behauptungen zutreffend. Das Innenministerium Rheinland-Pfalz erklärte etwa in (Min04):

> „Softwarefehler hätten die in Rheinland-Pfalz genutzten Wahlgeräte demgegenüber nicht aufgewiesen. Ihre Software sei vor der Verwendung in Rheinland-Pfalz von der [PTB] in Berlin eingehend geprüft worden. Nach Expertenmeinung würden die Prüfverfahren der [PTB] für Wahlgeräte als die strengsten Prüfverfahren der Welt im Bezug auf Wahlmaschinen gelten."

Zusammengefasst: Weil die PTB keine Softwarefehler gefunden habe, existierten auch keine. Eine offenkundig falsche Schlussfolgerung! Und dass die PTB nicht wirklich qualifiziert für die Prüfung der Wahlcomputer ist, zeigt sich auch an den in (Poh07, S. 27) aufgeführten Beispielen. Stark verkürzt – und in dieser verkürzten Form daher falsch – war auch die Begründung, warum die Wahlcomputer in Rheinland-Pfalz vor „Hackerangriffen" geschützt sein sollten:

> „Sie arbeiten autonom. Dies gewährleistet einen genügenden Schutz der Stimmen von ihrer Abgabe am Wahlgerät bis zu ihrer Erfassung in der Wahlniederschrift seitens des Wahlvorstandes vor Manipulationen."

Nur weil ein konkreter Angriffsvektor konstruktionsbedingt ausgeschlossen werden konnte, wurden nicht nur alle Angriffe eines bestimmten Personenkreises sondern alle Angriffe überhaupt pauschal ausgeschlossen. Dieser Fehlschluss ist schon derart eklatant, dass er nur schwer mit der Unwissenheit der Autorinnen oder Autoren dieser Pressemitteilung erklärt werden kann. Das Innenministerium war jedoch noch einen Schritt weiter gegangen und nutzte eine verfälscht wiedergegebene Problembeschreibung, um dafür eine passende Lösung zu präsentieren. Das Fehlen eines VVPAT bei bestimmten Wahlcomputern in den USA wurde so schlicht und falsch in den Mangel einer Druckmöglichkeit von Wahlergebnissen im Allgemeinen übersetzt und dann geschlussfolgert:

> „Die in Rheinland-Pfalz eingesetzten Wahlgeräte sind mit Papierdruckern ausgestattet. Ihre Ausdrucke weisen die Zahlen der an den Wahlgeräten abgegebenen Stimmen aus. Diese Papierausdrucke sind den Wahlniederschriften hinzuzufügen. An den Wahlgeräten werden die Zahlen der dort abgegebenen Stimmen auch angezeigt."

Hier muss gefolgert werden, dass entweder eine sinnvolle Sicherheitsbetrachtung gar nicht stattfand oder sie zugunsten einer Verharmlosung der Gefahren beim Einsatz von Wahlcomputern einfach ignoriert wurde.

4.2 Die Bundestagswahl 2005

Dennoch konnte auch das Insistieren der politisch Verantwortlichen auf der Sicherheit der Wahlcomputer die öffentliche Diskussion vor der Bundestagswahl nicht mehr zum Schweigen bringen. Auch wenn selbst hier *safety* und *security* teilweise vermischt wurden, warf etwa (Kle05) durchaus die richtigen Fragen auf. So wurde kritisiert, dass ausschließlich Baumusterprüfungen durchgeführt werden, bei allen an die Kommunen ausgelieferten Exemplare jedoch auf die Baugleichheitserklärung des Herstellers vertraut werde. Auch fehlende Nachprüfungen wurden bemängelt, während sie für viele andere technische Geräte regelmäßig durchzuführen seien. Von den Gefahren für die Sicherheit von Wahlen wurden explizit die fehlende Überprüfbarkeit auf Manipulationsfreiheit bei Wahlcomputern, die Einfachheit von Hardwaremanipulationen sowie der fehlende Schutz während der Lagerung in den Kommunen angeführt.

Dass einem Hersteller nicht uneingeschränkt Vertrauen entgegengebracht werden sollte, wenn es um die Bewertung von Sicherheitseigenschaften geht, zeigte auch die Zitierung von Schulze Geiping in (Sie05), der behauptete, VVPAT sei „Blödsinn“, denn damit baue man sich doch nur eine zusätzliche Fehlerquelle und eine zusätzliche Prüfstrecke ein. Diese „zusätzliche Prüfstrecke“, die die Nachvollziehbarkeit von Wahlen bei der Verwendung von Wahlgeräten und Wahlcomputern überhaupt erst ermöglichen würde, soll also nach Meinung des Herstellers unbedingt verhindert werden. Dennoch erhielt dieser indirekt Unterstützung durch das BMI, das sich laut (Zie05) „zum Schutz des Firmen-Know-hows des Herstellers“ erst einmal grundsätzlich weigerte, die Prüfberichte der PTB zu den eingesetzten Wahlcomputern zu veröffentlichen. Der Anfragende, Ulrich Wiesner, nahm die Gelegenheit wahr und kündigte für den Fall von Wahlcomputereinsätzen bei der kurz bevorstehenden Bundestagswahl eine Wahlanfechtung an mit der Begründung, der Einsatz von Wahlcomputern verstoße gegen das Öffentlichkeitsprinzip und das Transparenzgebot.

Der dann am 6. November 2005 eingelegte Einspruch (Wie05) gegen die Bundestagswahl enthielt als Begründung eine Konkretisierung der benannten Vorwürfe. Kernpunkte der Begründung, die im Fokus dieser Arbeit liegen, waren die fehlende Möglichkeit zur eindeutigen Identifizierbarkeit der eingesetzten Wahlcomputersoftware, ein nicht dem Stand der Technik entsprechender Manipulationsschutz der Software sowie die fehlende Überprüfbarkeit des Wahlergebnisses bei der Verwendung von Wahlcomputern. Die Identifizierung der Software würde dabei nach Ansicht des Einsprechenden ihre Authentifizierung mit umfassen, mithin die Identität der Software gegenüber etwa den Wahlvorständen nicht nur behauptet sondern bewiesen werden müsse. Diesen Schluss, den Politik und PTB rechtsirrig nicht teilen, wie schon in 3.4 auf Seite 46 gezeigt, zog Wiesner dabei vor allem aus dem Wortlaut der Richtlinien für die Bauart von Wahlgeräten, die in B.1 eine „*eindeutige* Identifikation der installierten Software“ fordert.

Während die „Initiative Nachrichtenaufklärung“ noch für 2005 Wahlcomputer als eines der am meisten vernachlässigten Themen in Presse und Öffentlichkeit aufführte, bildete die Wahlanfechtung Wiesners gleichzeitig den Ausgangspunkt einer sich entwickelnden gesellschaftlichen Debatte. Wo (Ste06) die kritische Rezeption des Themas noch ausschließlich in der Netzöffentlichkeit angesiedelt sah, wurden die dort angesprochenen Sicherheitsfragen mit dem Wahleinspruch zu allgemein medienöffentlichen Fragen.

Anfang Mai 2006 gab das BMI dann gegenüber dem Wahlprüfungsausschuss des Bundestages eine Stellungnahme (Bun06) zu den Wahleinsprüchen wegen der Verwendung von Wahlcomputern ab. Neben einer Erläuterung von Aufbau und Funktionsweise von Wahlcomputern sowie der Bauartprüfung durch die PTB wurden die Begründungen der Wahleinsprüche inhaltlich zurückgewiesen. Ein kurzer Überblick über die Zurückweisungsgründe zeigt die Fehler und Falschannahmen auf, denen das BMI sowie die PTB, die inhaltlich zuarbeitete, dabei unterlagen. Auf die unzulässige Trennung zwischen Identifizierung und Authentifizierung der Software in technischer Hinsicht wurde unter Verweis auf die einschlägige rechtliche Regelung bereits eingegangen.

> „Um das bestehende Softwareprogramm modifizieren zu können, müsste der Quellcode verfügbar sein."

Diese Aussage ist falsch, wie der Blick in die Geschichte zeigt. Der Compiler – und damit implizit die Trennung von Quellcode und Binärcode – wurde erst in den 1950er Jahren entwickelt, wie (Aue06) zum 100. Geburtstag von Grace Murray Hopper, der Erfinderin, in Erinnerung rief.

> „Welche [...] Listen am Wahltag die Nummern 7 und 8 haben werden, ist bis einige Wochen vor der Wahl in der Regel nicht bekannt. [...] Manipulationen müssten also in der Regel ‚blind' erfolgen und würden sich dann auf alle Wahlen in gleicher Art und Weise auswirken."

Diese Aussage kann im Einzelfall die Realität korrekt widerspiegeln, in ihrer Allgemeinheit ist sie jedoch falsch, wie § 30 Absatz 3 BWahlG festlegt. Danach richtet sich die Reihenfolge der Listen grundsätzlich nach der Zahl der Zweitstimmen, die die betreffenden Parteien bei der letzten Bundestagswahl erreicht haben. In den Landeswahlgesetzen existieren ähnlich lautende Regelungen. Damit ist bereits nach Verkündung des amtlichen Endergebnisses die Reihenfolge der Listen für die jeweils nächste Wahl bekannt.

> „Zum anderen dient die öffentliche Wahlhandlung der Kontrollierbarkeit der Wahlhandlung. Die Öffentlichkeit soll überwachen können, dass nur Wähler, die vom Wahlvorstand daraufhin kontrolliert worden sind, ob sie tatsächlich im Wählerverzeichnis eingetragen waren, einen (einzigen) Stimmzettel einwerfen."

Auch hier irrte das BMI. Die Öffentlichkeit der Wahlhandlung, die auch die Auszählung mit einschließt, dient mitnichten nur der Kontrolle der Wählerinnen und Wähler. Stattdessen dient sie zumindest auch, wie in (Poh07, S. 25f.) nachgewiesen, der Kontrolle der Wahlvorstände und damit dem Schutz gegen Manipulationen durch diese.

Diese Falschaussagen werfen ein schlechtes Licht sowohl auf das BMI als auch auf die PTB – entweder auf deren Sachkenntnis oder auf deren Vertrauswürdigkeit. Obwohl die Fehler offenkundig waren und sind, wurden sie vom Distributor HSG Wahlsysteme und von der „Anwendergemeinschaft Elektronischer Wahlgeräte" in (HSG06a) teilweise wörtlich wiederholt. Außerdem wurde die Behauptung aufgestellt, die Wahlcomputer würden nach ihrer Versiegelung in den Wahlämtern nur noch „besonders geschützt" aufbewahrt. Ob diese Aussage zutreffend war, wurde später widerlegt, wie noch zu zeigen sein wird.

Auch andere politisch Verantwortliche hielten sich nicht immer an die Wahrheit. In der Beantwortung (Inn06) einer Kleinen Anfrage im Hessischen Landtag behauptete das Innenministerium wahrheitswidrig, dass „bei einem jahrzehntelangen Einsatz von Wahlgeräten in der Bundesrepublik Deutschland Unregelmäßigkeiten bei der Wahlhandlung oder der Ergebnisermittlung noch nicht aufgetreten“ sind. Die Ereignisse in Sankt Wendel 1980 sprechen eine andere Sprache.

Nachdem sich die PTB fast ein Jahr lang geweigert hatte, Prüfberichte für Wahlcomputer zu veröffentlichen, änderte sie im August 2006 mit Zustimmung des Herstellers ihre Meinung und veröffentlichte den Prüfbericht für einen Wahlcomputer „ESD1“ (Phy04) vom 12. Mai 2004. Die daraus ablesbare fehlende Sachkunde wurde schon in (Poh07, S. 27) kritisch gewürdigt. Fragwürdig ist an diesem Bericht insbesondere, dass die Prüfung der Wahlcomputersoftware in weniger als einem Tag durchgeführt wurde. Dieser Fakt wurde bisher jedoch öffentlich nicht problematisiert.

4.3 „Nedap-Hack“

Anfang Oktober 2006 demonstrierte die Initiative „Wij vertrouwen stemcomputers niet“ im holländischen Fernsehen die Manipulierbarkeit eines Nedap-Wahlcomputers „ESD3B“. Dabei tauschte sie in weniger als fünf Minuten die Hardwaremodule mit der Wahlcomputersoftware aus und ersetzte diese erst durch Bausteine mit einer manipulierten Version der Originalsoftware und dann durch ein Schachprogramm. Der dazugehörige Bericht (GHB+06) erläutert ausführlich den technischen Aufbau und die zu verschiedenen Angriffen durchgeführten Schritte. Unter anderem stellte sich heraus, dass die Wahlauswertungssoftware mit Hilfe des Passwortes „GEHEIM“ in einen Administrationsmodus versetzt werden konnte, in dem ein Speichermodul erzeugt werden kann, das im Wahlcomputer den Servicemodus freischaltet, dass mit Hilfe von Van-Eck-Phreaking das Wahlgeheimnis gebrochen werden konnte und dass die Versiegelung der Geräte in der vorgenommenen Form untauglich für einen Schutz vor Manipulationen war.

Diese Demonstrationen zogen gleichzeitig große mediale Aufmerksamkeit und scharfe Reaktionen von Hersteller und Distributor, die nicht immer der Wahrheit treu blieben, nach sich. So behauptete Schulze Geiping in (HSG06b), die Wahlcomputer würden „immer in einer ‚geschützten Umgebung‘ gelagert, vorbereitet und betrieben“, obwohl zu diesem Zeitpunkt längst Gegenteiliges bekannt war. Groenendaal versuchte sich in (Gro06) gar an einem Pamphlet, das allerdings inhaltlich nichts zur Diskussion beitrug. Zu der entdeckten Hintertür äußerten sich beide nicht. Und selbst die PTB konnte nicht schweigen und versprach in (Phy06), den Bericht zu berücksichtigen. Ausführlich und kritisch wurde in (Sie06) der verantwortliche Fachbereichsleiter für die Prüfung von Wahlgeräten und Wahlcomputern befragt.

So begründete Richter die Aussage, Wahlcomputer seien „hinreichend manipulationssicher“ mit dem Verweis darauf, dass es keine Erkenntnisse über Manipulationsversuche an Wahlcomputern in der BRD gäbe, obwohl Aussage und Begründung nichts miteinander zu tun haben. Zur „geschützten Aufbewahrung“ zwischen den Wahlen musste Richter immerhin zugeben, dass es dafür an keiner Stelle rechtliche oder andere Regelungen gebe. Wie er dann aber schlussfolgerte, dies wäre eine Selbstverständlichkeit, blieb mehr als unklar. Das Fehlen von Sicherheitsregeln hilft nicht gerade bei deren Durchsetzung. Auch die Aussage,

für eine Manipulation sei der Zugriff auf den Quellcode nötig, wollte Richter plötzlich nicht mehr einschränkungslos vertreten. Dass die Aussage von vornherein unrichtig war, schien er entweder nicht zu wissen oder zu ignorieren. Auch seine Auslegung der Anforderung, dass Veränderungen „der installierten Software durch unbefugte Dritte nicht unbemerkt bleiben“ dürften, als Anforderung an „das Gesamtsystem der Maßnahmen“ war und ist falsch und widerspricht dem Wortlaut der entsprechenden Regelung im BWahlGV. Und obwohl er zumindest zugeben musste, dass das System „keinen absoluten Schutz gegen Insider-Angriffe“ biete, zeugt seine Beschreibung, wer als Insider zu gelten habe, von der grundsätzlichen Unkenntnis der Definition von „Insider“. So solle nach seiner Meinung nur als Insider gelten, wer „die inneren Datenstrukturen“ der Software kenne. Mitglieder der Wahlvorstände und Mitarbeiterinnen und Mitarbeiter der Kommunen, die ebenso legal Zugang zu den Wahlcomputern erlangen können, hat er wohl schlicht vergessen. Zum Abschluss gab er dann zwar Nachbesserungsbedarf in vielen Bereichen zu, allerdings sind seitdem keine großen Reformbemühungen erkennbar geworden.

Eine praktische Auswirkung hatte die Demonstration der Manipulierbarkeit von Wahlcomputern allerdings dann doch noch ganz kurzfristig: Zum ersten Mal im Vorfeld einer Wahl wurden Mitte Oktober 2006 in Cottbus die tatsächlich eingesetzten Wahlcomputer überprüft und sich nicht nur auf die Baugleichheitserklärung verlassen. Wie (Kle06) berichtete, seien alle „eingesetzten Speicherbausteine bitgenau ausgelesen und mit dem Original der Software“ verglichen worden. Anschließend seien die Wahlcomputer amtlich versiegelt worden. Leider wurden die dabei entstandenen Kosten nicht genannt. Auch hat die Sonderprüfung, wie (Cha06) nachgewiesen hat, nicht dazu geführt, dass die Sicherheit der Wahl tatsächlich garantiert werden konnte. So wurden etwa einfach zu manipulierende Versiegelungsmechanismen benutzt, die Wahlcomputer zeitweilig unbeaufsichtigt gelassen oder die Identität der Software nicht geprüft. Die Situation hat sich in Bezug auf die Sicherheitsregeln und deren Einhaltung auch bis heute offensichtlich zumindest nicht überall geändert, wie noch zu zeigen sein wird.

Wie auch Cottbus in (Hie06) versuchte die Stadt Langen in einer Pressemitteilung (Sor06), Befürchtungen um die Manipulierbarkeit von Wahlcomputern entgegenzutreten. Dabei verstieg sie sich allerdings in die folgende Behauptung:

> „Denn es gebe keine Möglichkeit, von außen auf die Wahlmaschinen zuzugreifen. ‚Und das meint der Begriff ‚hacken‘ ja.‘ Für einen solchen Eingriff müssten die Geräte mit einem Netz verbunden sein, was sie aber nicht sind.“

Dies zeigt deutlich, dass die Verantwortlichen auch zu diesem Zeitpunkt die tatsächliche Problemlage noch nicht erkannt hatten.

Hamburg ging einen etwas anderen Weg, der zumindest grundsätzlich sinnvoller ist, als überkommenen Systemen nur deshalb zu vertrauen, weil vorgesetzte Stellen deren Vertrauswürdigkeit mantraartig wiederholen. Die in Hamburg Ende Oktober 2006 vom Senat getroffene und in (Beh06) veröffentlichte Entscheidung, zu den Wahlen 2008 das bereits in Abschnitt 3.5 auf Seite 48 angesprochene Digitale Wahlstift-System einzuführen, wurde mit der Nachweisbarkeit der Sicherheit des Systems anhand eines CC-Schutzprofiles begründet. Dieses sei auch schon vom BSI geprüft und zertifiziert worden. Diese Art eines streng formalisierten Prüfverfahrens wäre grundsätzlich anderen Verfahren vorzuziehen, wenn die Verantwortlichen dabei nicht, wie bereits gezeigt, schwerwiegende Fehler bei der

Beschreibung der Sicherheitsumgebung sowie bei der Übersetzung der rechtlichen in technische Anforderungen begangen hätten. Insofern muss der Verweis auf dieses Schutzprofil und dessen Zertifizierung sowie auf die später erfolgte Zertifizierung des einzusetzenden Wahlstift-Systems anhand der Anforderungen aus dem Schutzprofil sich hier zulässig mit der ärztlichen Verschreibung eines Placebos vergleichen lassen: Es kann ein Mehr an Sicherheit schaffen, insoweit es potentielle Angreiferinnen und Angreifer subjektiv von Angriffen abhalten könnte, aber deren Angriffsdurchführung wird effektiv nicht unterbunden, vielleicht nicht einmal erschwert.

Ende November 2006 entschied dann der Wahlprüfungsausschuss des Bundestages über die eingelegten Wahleinsprüche gegen die Bundestagswahl 2005 und legte dem Bundestag eine entsprechende Beschlussempfehlung (Wah06) zu der angesprochenen Wahlanfechtung von Wiesner vor. Es lässt sich feststellen, dass der Ausschuss ausschließlich den Argumentationen des BMI und der PTB folgte, auch dort, wo sie offenkundig falsch waren. Dazu zählten etwa die Behauptungen, es bedürfe eines Zugriffs auf den Quellcode als Voraussetzung für eine Manipulation der Software, mit der fehlenden Netzanbindung seien die Wahlcomputer „von externen Beeinflussungen während der Wahl weitgehend geschützt“[18], die Software würde „vor der Verwendung zweimal kontrolliert“ und eine Softwaremanipulation sei mangels Wissen über die Reihenfolge der Kandidaturen unmöglich. Alle Einwürfe und Argumente des Einsprechenden, die die Aussagen von BMI und PTB widerlegen, wurden schlicht ignoriert. Auf die gleichlautende Entscheidung des Bundestages am 14.12.2006 in dieser Sache folgte im Februar 2007 die Einreichung einer Wahlprüfungsbeschwerde (Wie07a) vor dem Bundesverfassungsgericht durch Wiesner.

In Bezug auf die *security* hob Wiesner dabei folgende Punkte hervor: Die Überprüfung des mit Nedap-Wahlcomputern ermittelten Wahlergebnisses sei nicht möglich, weil die gespeicherten Stimmen bereits das Ergebnis einer Informationsverarbeitung sind und es demnach keine geräteunabhängige Dokumentation der Wahlentscheidungen gibt. Die Übereinstimmung der gespeicherten Stimmen mit der ursprünglichen Wahlentscheidung hänge damit ausschließlich von der Fehler- und Manipulationsfreiheit der eingesetzten Software ab. Die Software könne, so führte Wiesner weiter aus, jedoch nicht sicher identifiziert werden, weil die genutzten Prüfsummen dies nicht erlauben. Eine manipulierte Software könne unschwer die gleiche Prüfsumme ausgeben wie die echte. Auch würden die Nedap-Wahlcomputer keine Schutzmechanismen gegen die Ausführung herstellerfremden Codes bieten. Insgesamt handelte es sich bei der Begründung der Wahlprüfungsbeschwerde um eine Erweiterung und Präzisierung der bereits im Einspruchsverfahren vor dem Bundestag vorgetragenen Argumente.

Von den drei dazu dem Bundesverfassungsgericht eingereichten Stellungnahmen – von der PTB, vom Chaos Computer Club (CCC) und vom BMI – ist nur die vom CCC in (KRG07) veröffentlichte. Auf die beiden anderen Stellungnahmen kann daher nur in dem Umfang eingegangen werden, wie sie in Wiesners Entgegnung (Wie07b) an das Bundesverfassungsgericht zitiert wurden. Kurz vor der Veröffentlichung der Stellungnahme des CCC beantwortete die Bundesregierung eine Kleine Anfrage der Linksfraktion in (Bun07b). Auch darin finden sich wieder falsche Tatsachenbehauptungen. So erklärte die Bundesregierung, es bestehe die

[18] Eine noch weitergehende Behauptung stellte kurz darauf Schulze Geiping in (Sch06) auf. Danach seien die Wahlcomputer sicher, weil sie in kein Netz eingebunden sind.

Möglichkeit, „jederzeit einen Vergleich der eingesetzten Geräte einschließlich Software mit dem geprüften Baumuster vornehmen zu können“, was vor dem Hintergrund der fehlenden technischen Möglichkeiten der Wahlvorstände und ihres nicht vorhandenen Wissens absurd erscheint. Auch die Falschbehauptung der sicheren Aufbewahrung der Wahlcomputer durch die Gemeindebehörden wurde wider besseren Wissens wiederholt. Als Argument für die Manipulationssicherheit der Wahlcomputer allerdings völlig untauglich war jedoch folgende Behauptung:

> „Außerdem ist die Fälschung der Wahl strafbewehrt, was gegenüber Manipulationen bei einer Wahl präventiv wirkt.“

Das Gegenteil ist richtig: Der Gesetzgeber hat Wahlfälschungen gerade deshalb pönalisiert, weil sie vorgekommen sind und weiter vorkommen. Dies soll vergolten werden.[19] Zwei weitere Falschaussagen seien hier beispielhaft wiedergegeben: Eine Abstimmung mit einem Hersteller habe es bei der Änderung der BWahlGV 1999 nicht gegeben. Und für die Nedap-Wahlcomputer würde sich eine Protokollierung von Wartungszugriffen erübrigen, da diese wartungsfrei seien. Beide Aussagen wurden im Rahmen von Wiesners Entgegnung widerlegt, der erstens Aussagen der PTB über die Zusammenarbeit mit dem Hersteller während der BWahlGV-Novellierung vorlegen konnte und zweitens auf die Softwareupdates verwies, die Zugriffe erforderten.

Keine zwei Wochen nach der Antwort der Bundesregierung widerlegte eine Wahlbeobachtung eines Bürgerentscheids in Neuss, Nordrhein-Westfalen, die unter (Asm07) protokolliert wurde, unter anderem eines der zentralen Argumente für die Sicherheit von Wahlcomputern – die vermeintlich sichere Aufbewahrung. Der Wahlcomputer, der in dem beobachteten Wahllokal in einer Schule zum Einsatz kam, soll in den vier Tagen vor der Wahl im Büro des schuleigenen Hausmeisters untergebracht gewesenen sein. Auch die Versiegelung wurde als lächerlich beschrieben: Eine Kordel um die Griffe des Wahlcomputers, die mit einem „simplen weissen Papiersiegel“[20] gesichert gewesen sei. Und weiter:

> „Das Siegel trug den Schriftzug ‚Dienstsiegel der Stadt Neuss‘ und bot zwar ein Unterschriften-Feld, welches jedoch leer war. [...] Von der Wahllokalleitern Freirichs wurde das nicht unterschrieben Siegel nicht etwa beanstandet; Auch durften wir es nicht mitnehmen. Das Siegel wurde von Frau Freirichs kurzerhand im nachhinein – nachdem es gebrochen war – noch unterschrieben.“[21]

Eine sichere – und im Übrigen rechtskonforme – Verwendung von Wahlcomputern bei Wahlen sähe anders aus. Nicht in dieser extremen Form aber auch ohne Kontrolle der vom Wahlcomputer angezeigten Prüfsummen verlief der Entscheid in einem anderen Wahllokal, von dem (Feh07) berichtete. Trotzdem konnte die Landesregierung von Nordrhein-Westfalen in (Lan07), der Beantwortung einer Kleinen Anfrage behaupten, dass „dem Innenministerium konkrete Wahlfehler oder besondere Probleme hinsichtlich des Einsatzes von Stimmenzählgeräten bei bisherigen Wahlen nicht berichtet oder sonst bekannt geworden“ seien.

[19] Erstes Ziel des Strafrechtes ist nicht die Prävention sondern die Vergeltung, wie § 46 Absatz 1 Satz 1 StGB festlegt.
[20] Schreibfehler wie im Original.
[21] Schreibfehler wie im Original.

Als die Stellungnahme des CCC am 30. Mai 2007 veröffentlicht wurde, waren die zuvor beschriebenen Ereignisse im Wesentlichen bekannt und viele Argumente bereits ausgetauscht. Der Stellungnahme kommt darum eher der Charakter einer strukturierten Situations-, Technik- und Sicherheitsanalyse zu. Neben den an den Adressaten, das Bundesverfassungsgericht, angepassten Wortwahl und Erläuterungsweise enthielt sie allerdings auch Erwiderungen auf zwischenzeitlich vorgeschlagene oder gar eingeführte zusätzliche Schutzmaßnahmen. Dazu gehörte die Vorstellung einer zumindest grundsätzlich zur Erkennung von Testwahlen, also der Simulation einer Wahl unter kontrollierten Bedingungen zum Nachweis der Manipulationsfreiheit der Wahlcomputer, geeigneten manipulierten Software. Auch ausführliche Beschreibungen von möglichen Angriffen auf die Wahlauswertungssoftware IWS oder den Prozessor waren Teil der Stellungnahme, die durch den Nachweis und die Erläuterung einer aufgefundenen Hintertür ergänzt wurde. Als zwei wichtige Ergebnisse der Analyse wurden angegeben:

> „Der Computersicherheitsforschung ist bis heute kein System bekannt, mit dem ein unbemerkter Austausch von Software oder Hardware in einem Computersystem, dass sich in der Hand eines Angreifers befand, erkannt werden kann, ohne eine individuelle Einzelanalyse mit Mitteln der Computerforensik vorzunehmen."

Daraus wurde geschlussfolgert, dass mit den derzeitigen Regelungen in der BWahlGV keine existierenden Wahlcomputer zulassungsfähig sein können. Und zweitens:

> „Bisherige aufgedeckte Fälle von Wahlfälschungen sind ausschließlich durch Innentäter durchgeführt worden, die Zugang zu den Wahlmitteln hatten."

Daher wurde die von BMI und PTB wiederholt getätigte Behauptung, Angriffe durch Innentäterinnen und Innentäter seien unwahrscheinlich, von den Autorinnen und Autoren verworfen.

Anhand der Zitierungen in Wiesners Entgegnung (Wie07b) sollen kurz die Stellungnahmen von BMI und PTB an das Bundesverfassungsgericht in Bezug auf Sicherheitsfragen gewürdigt werden. Das BMI habe nach Wiesner „vollinhaltlich" auf die Stellungnahme vom 3. Mai 2006 an den Wahlprüfungsausschuss des Bundestages verwiesen und insofern offensichtlich selbst von den bereits widerlegten Behauptungen keinen Abstand genommen. Auch die PTB widerrief in ihrer Stellungnahme keine ihrer früher getätigten Behauptungen. Weiterhin habe sie die Sicherheit der Wahl durch organisatorische Maßnahmen und Lagerung der Wahlcomputer in geschützten Umgebungen als geschützt angesehen und die Gefahr durch Innentäterinnen und Innentäter marginalisiert. Ihre Begründung für einen Ausschluss der Gefahr durch Insider stütze sie wesentlich auf durchgeführte Audits beim Hersteller, auf das „langjährig bewährte Prinzip der Baumusterprüfung" und die wirtschaftlichen Interessen der Herstellers an baugleichen Nachbauten der zugelassenen Wahlcomputer. Wiesner wies der PTB in seiner Erwiderung nach, dass deren Verweise auf einschlägige technische Normen und Standards, mit denen sie die besonders sorgfältige Prüfung der Wahlcomputer habe nachweisen wollen, jeder Grundlage entbehrten. Die eine zitierte Norm regelt Anforderungen an die *safety*, die andere, ITSEC – ein Vorläufer der CC –, definiert formale Prozesse zur Festlegung von Sicherheitsanforderungen und deren Überprüfung, von denen

Wiesner zeigen konnte, dass sie im Rahmen der von der PTB durchgeführten Prüfung keine Anwendung gefunden haben konnten. Bei der Zitierung dieser Normen gegenüber dem Bundesverfassungsgericht durch die PTB könnte es sich daher durchaus um den Versuch einer Täuschung des Gerichts gehandelt haben. Dies erscheint auch vor dem Hintergrund nicht ausgeschlossen, dass Richter, der verantwortliche Fachbereichsleiter bei der PTB, auch vor dem Verwaltungsgericht Braunschweig am 17.10.2007 falsch aussagte. Dort behauptete er laut (Sie07d) also auch noch nach dem Beweis des Gegenteils durch die Sicherheitsanalyse des CCC, dass in der Bundesrepublik lediglich drei Personen nachvollziehen könnten, wie die elektronische Erfassung, Speicherung und Zählung von Stimmen an den Nedap-Wahlcomputern funktioniert, dabei hatte er selbst bereits in (Sie06) zugeben müssen:

> „Inzwischen ist durch die Bekanntgabe und Veröffentlichung vieler Informationen die Frage, wer ist jetzt Insider, allerdings nicht mehr ganz so klar."

Das ist schon entlarvend.

Nicht nur die Wahlprüfungsbeschwerde zwang den PTB-Verantwortlichen, Farbe zu bekennen. In (KR07) wurden zusammengefasst die bereits im „Nedap-Hack" und in der Stellungnahme an das Bundesverfassungsgericht aufgezeigten Angriffsvarianten vorgestellt. Auch wurden die bisherigen Reaktionen und Aussagen von BMI und PTB dokumentiert und widerlegt. Auf diese Veröffentlichung in einer renommierten deutschen Zeitschrift reagierte Richter und verfasste für die folgende Ausgabe eine Erwiderung (Ric07). Dabei stellte er Argumente von Kurz und Rieger falsch dar und „widerlegte" diese dann. So unterstellte er, es sei behauptet worden, „die Wahlgeräte allein [seien] technisch zu sichern" und lehnte diese Annahme dann ab. Diese Behauptung wäre tatsächlich falsch, wurde so jedoch auch nicht aufgestellt. Vielmehr verwiesen Kurz und Rieger zutreffend auf die Richtlinie für die Bauart von Wahlgeräten, die etwa in B.1 für Wahlcomputer eine „*eindeutige* Identifikation der installierten Software" fordert und dabei tatsächlich verlangt, dass diese Anforderung von den Wahlcomputern selbst technisch zu erfüllen sei und nicht nur durch organisatorische Maßnahmen. Dies konnte Richter auch deshalb nicht unbekannt sein, weil diese Anforderung tatsächlich im Wortlaut in jeder ausführlichen kritischen Stellungnahme oder Sicherheitsanalyse explizit aufgeführt war. Damit ließe sich auch erklären, warum Richter es unterließ, in seiner Darstellung der Sicherheitsanforderungen an Wahlcomputer auf die Anforderung zur sicheren Identifizierbarkeit einzugehen: Diese werden von den derzeit zugelassenen Nedap-Wahlcomputern schlicht nicht erfüllt. Die von ihm später angesprochenen Prüfsummen, die tatsächlich nicht in der Lage sind, eine sichere Identifizierung zu gewährleisten, sollen damit plötzlich auch nicht mehr dem Nachweis der „Authentizität der Geräte" dienen. Damit widersprach er direkt der von ihm mit ausgearbeiteten Stellungnahme des BMI an den Wahlprüfungsausschuss des Bundestages, in dem noch behauptet wurde, es werde „unter anderem kontrolliert, ob das Wahlgerät und sein Softwareprogramm sich korrekt identifizieren." Beide Formulierungen, die der *sicheren* und die der *korrekten* Identifizierung, verweisen im wesentlichen auf die gleiche Anforderung: Die Identifizierung des Wahlcomputers muss durch diesen bewiesen werden, er muss sich also authentifizieren.

Ein zweiter Fauxpas unterlief Richter, als er die Gefahr durch Innentäterinnen und Innentäter dadurch zu negieren versuchte, dass er auf die Annahme verwies, „dass Wahlämter und Wahlvorstände, die Wahlgeräte einsetzen, genauso zuverlässig sind wie jene, die traditionelle Wahlen durchführen." Offensichtlich in der Hoffnung, dass nun die Leserinnen

und Leser dies dergestalt auslegen würden, dass Wahlvorstände niemals Innentäterinnen und Innentäter sein könnten, endete hier seine Ausführung. Diese Auslegung, die hier hervorgerufen werden sollte, entspricht jedoch nicht den Tatsachen, wie etwa in (Poh07, S. 25f.) ausführlich nachgewiesen wurde. Auch sonst versuchte Richter, mit unklaren Formulierungen und falschen Schlüssen die Bedrohungen herunterzuspielen. So verglich er Manipulationen an der Hardware von Wahlcomputern, mit denen Wahlergebnisse gefälscht werden können, mit Angriffen auf das Wahlgeheimnis durch „das Anbringen einer Minikamera in traditionellen Wahllokalen“, um daraus den Schluss zu ziehen, dass beiden mit organisatorischen Sicherheitsmaßnahmen begegnet werden könne. Wie ausführlich in Abschnitt 3.2 gezeigt, sind diese beiden in Bezug auf Angreifertypen, Bedrohungspotential und Erkennungsmöglichkeit jedoch extrem unterschiedlich und damit nicht vergleichbar, insbesondere nicht betreffend ihrer nachträglichen Nachweisbarkeit. Richters weitere Ausführungen stellen im Wesentlichen eine Wiederholung bereits widerlegter Behauptungen dar, wie sie etwa schon in (Bun06), (Wah06) oder der Stellungnahme der PTB an das Bundesverfassungsgericht aufgestellt wurden.

Ende Oktober stellte der CCC zwei Angriffe (Cha07) auf das in Hamburg anvisierte Digitale Wahlstift-System vor. Einerseits zeigte der Club einen manipulierten Wahlstift, der als Trojanisches Pferd dienen sollte. Andererseits wies er nach, dass eine Veränderung des digitalen Papiers, das die Grundlage für den einlesbaren Stimmzettel darstellt, möglich sei, ohne dass die Manipulation den Wählerinnen und Wählern oder den Wahlvorständen auffallen müsse, da letzteren die digitalen Stimmdaten vom System nur dann zur separaten Auswertung vorgelegt werden, wenn sie sich nicht eindeutig zuordnen lassen. Da gleichzeitig nach dem zitierten Hamburger Wahlgesetz auch nicht die Stimmabgabe auf Papier sondern die elektronischen Daten für das Wahlergebnis relevant sind und so auch der Sinn jeder Wahlprüfung ausgehebelt wird, stellten diese Manipulationen eine große Gefahr für die Durchführung der Wahlen dar. Letztendlich wurde das Digitale Wahlstift-System, wie (Sie07c) berichtete, erst einmal nicht eingeführt, zumindest nicht zur Hamburger Wahl 2008.

Bereits zwei Wochen früher, am 2. November 2007, hatte das BMI Nedap-Wahlcomputern in vier neuen Hard- und Softwarekonfigurationen eine Bauartzulassung erteilt, wie (Sie07b). Die dieser Zulassung zugrundeliegenden Prüfprotokolle veröffentlichte die PTB dann im Januar 2008 mit Einverständnis des Herstellers ((Phy07a), (Phy07b) (Phy07c), (Phy07e)). Auch eine überarbeitete Bedienungsanleitung (HSG07a) sowie ein Muster des Wahlgeräte-Begleitscheines (HSG07b) wurden der Öffentlichkeit zur Verfügung gestellt. Grundtenor aller vorliegenden Dokumente ist, dass die Sicherheit von Wahlcomputern nur garantiert werden könne, wenn zusätzliche Maßnahmen durchgeführt werden. Die PTB stellte daher die Erfüllung der Anforderungen der BWahlGV an die Manipulationssicherheit und damit die positive Bewertung der Sicherheitseigenschaften der Nedap-Wahlcomputer immer unter die Bedingung, dass die Kommunen für eine Lagerung in geschützten Umgebungen sorgen und die ordnungsgemäße Versiegelung der Wahlcomputer und deren Bauteile von den Verantwortlichen kontrolliert wird. Die Versiegelung der Bauteile und des Gehäuses im aufgeklappten Zustand geschehe nach der Bedienungsanleitung auch nicht mehr mit einfachen Papiersiegeln sondern mit solchen, an denen Manipulationen tatsachlich erkannt werden könne. Deren Kontrolle sowie die der amtlichen Versiegelung des Gehäuses im tragbaren Zustand wird jetzt auch in der Bedienungsanleitung ausführlich erläutert und als vorgeschrieben vorausgesetzt.

Trotz dieser Fortschritte stellte der CCC mit Hilfe einer hessischen Wählerin beim Staatsgerichtshof des Landes Hessen einen Antrag auf Erlass einer einstweiligen Verfügung gegen den Einsatz von Wahlcomputern bei der dortigen Landtagswahl und berichtete in (Cha08b) darüber. Auch dieser Antrag wurde aus formalen Gründen abgelehnt und die Antragstellerin auf das nach der Wahl mögliche Wahlprüfungsverfahren verwiesen. Eine in diesem Zusammenhang von Christoph Bieber in einem Interview in (Hau08) geäußerte Behauptung zeigt das grundsätzliche Unverständnis über die Probleme mit Wahlcomputern auf. Er meinte, Papierwahlen seien viel einfacher zu fälschen und wollte dies an einem Beispiel zeigen:

> „Das konnte man gut bei der Wahl des Hamburger SPD-Spitzenkandidaten sehen. Da verschwinden einfach Säckeweise Wahlzettel."

Dabei ist genau das jedoch der große Unterschied zwischen Wahlcomputern und anderen Wahltechniken. Wenn Wahlen, wie Bieber richtig sagte, nur „hinreichend fälschungssicher" sein müssen, dann kann dies nur rechtmäßig sein, wenn Fälschungen in jedem Fall erkannt werden können. Und dies kann bei Wahlcomputern verhindert werden.

Die Sorge, dass Sicherheitsregeln nicht eingehalten werden würden und damit die Sicherheit der Wahl nicht garantiert werden könnte, war nicht unbegründet, wie der CCC in (Cha08c) nach der Wahl konstatieren musste. So seien in der Gemeinde Niedernhausen die Wahlcomputer in der Nacht vor der Wahl in den Privatwohnungen von Parteimitgliedern gelagert worden, was von Mitarbeitern des Ordnungsamtes als „gängige Praxis" bezeichnet worden sei. Auch sonst sei die „geschützte Umgebung" nicht immer gegeben gewesen und Wahlbeobachter in zwei Wahllokalen „für längere Zeit alleine mit den bereits ausgelieferten Wahlcomputern [gewesen], bevor der Wahlvorstand eintraf". Außerdem wurde von massiven Behinderungen der Wahlbeobachtung in verschiedenen Gemeinden berichtet. Zusammenfassend lässt sich feststellen, dass die Sicherheitsregeln nicht eingehalten wurden, weder die schon lange gültigen noch die neu formulierten, und die Verantwortlichen das auch wussten und daher versuchten, die Wahlbeobachtung wenn nicht zu verhindern so doch zu erschweren. Ähnliche Ergebnisse ergab die Wahlbeobachtung in Bayern am 2. März 2008, von denen (Cha08a) berichtete. Hier wurden allerdings keine Wahl- sondern Zählcomputer eingesetzt. Auf den Stimmzetteln waren dafür Barcodes abgedruckt, die jeweils eineindeutig den möglichen Wahlvorschlägen zugeordnet sein sollten, was aber zumindest in einer Gemeinde nicht der Fall war. Dort war zwei Wahlvorschlägen der gleiche Barcode zugeordnet, was erst im Laufe der Auszählung auffiel. Die Auszählung der Stimmzettel erfolgt dann durch Einscannen der Barcodes neben den von den Wählerinnen und Wählern markierten Wahlvorschlägen und eine computergestützte Auswerte- und Zählsoftware. Die Software soll in Bayern zugelassen worden sein, ohne dass sie sich einer formalen Prüfung unterziehen musste. Ein Teil der dafür notwendigen Computer wurde von Mitgliedern der Wahlvorstände und gar von amtierenden Stadträten mitgebracht. Zumindest wurde von nicht ganz so aggressiven Ausfällen von Wahlvorständen gegenüber den Teilnehmenden an der Wahlbeobachtung berichtet wie in Hessen.

4.4 Zwischenstand

Die Publikationen von immer neuen Sicherheitsproblemen und möglichen Angriffen sowie die verstärkte Öffentlichkeitsarbeit zeitigten jedoch auch Ergebnisse. Zwar verweiger-

te die Stadtverordnetenversammlung von Wittenberge einem Antrag auf einen dauerhaften Verzicht auf Wahlcomputer aus Sicherheitsgründen, namentlich wegen der fehlenden Nachprüfbarkeit, eine Mehrheit, aber zumindest wurde die Verwendung von Wahlcomputern mindestens bis zur Entscheidung des Bundesverfassungsgerichts über die anhängige Wahlprüfungsbeschwerde ausgesetzt, wie (Sie07a) berichtete. Die Niederlande, wo vormals ausschließlich mit Wahlcomputern gewählt wurde, ging noch einen Schritt weiter. Laut (Wil08) wurde beschlossen, künftig Wahlen zumindest solange ohne Wahlcomputer durchzuführen, wie diese keine geeignete Alternative zu Wahlen mit Stimmzetteln darstellen würden.

Auch die PTB hatte mit ihren zunehmend unhaltbar gewordenen Positionen Schwierigkeiten, Unterstützerinnen und Unterstützer zu gewinnen. Im Mai 2008 empfahl der Wissenschaftsrat in (Wis08), dass der PTB die Zuständigkeit für die Prüfung von Wahlgeräten und Wahlcomputern genommen werden solle, weil diese „dem wissenschaftlichen Profil der Einrichtung widersprechen“ würde.

5 Zusammenfassung und Ausblick

Zusammenfassend lässt sich konstatieren, dass die technischen Anforderungen an Wahlgeräte und Wahlcomputer, die sich aus der derzeit gültigen Bundeswahlgeräteverordnung ergeben, den verfassungsrechtlichen und einfachgesetzlichen Anforderungen an Wahlen und deren Durchführung nicht entsprechen. Selbst die Erfüllung der technischen Anforderungen durch konkrete Wahlgeräte- oder Wahlcomputertypen kann also die Durchführung demokratischer und manipulationssicherer Wahlen nicht gewährleisten.

Formalisierte Vorgehensweisen bei der Beschreibung und Bewertung von Sicherheitsanforderungen und -eigenschaften, wie sie grundsätzlich die Common Criteria zur Verfügung stellen, sind informalen Abbildungen aus der Sprache eines Anwendungsgebietes in die Sprache der Technik vorzuziehen. Dafür sind fundierte Kenntnisse sowohl in dem betreffenden Anwendungsgebiet als auch über die immanenten Eigenschaften und Beschränkungen der technischen Systeme, die Verwendung finden sollen, unabdingbar. Auch strukturelle Defizite des gewählten Verfahrens, wie sie etwa auch die Common Criteria aufweisen, müssen bekannt sein. Liegen solche Kenntnisse nicht vor, oder werden die Defizite nicht beachtet und durch zusätzliche Maßnahmen kompensiert, wie es sowohl der Physikalisch-Technischen Bundesanstalt als auch dem Bundesamt für Sicherheit in der Informationstechnik vorzuwerfen ist, müssen die derart produzierten Anforderungskataloge, Evaluierungsverfahren oder Zertifizierungen als im Wesentlichen wertlos betrachtet werden.

Die größte Bedrohung für Wahlen im Allgemeinen und Wahlen unter Verwendung von Wahlgeräten und Wahlcomputern im Besonderen stellen Innentäterinnen und Innentäter dar. Die Ignoranz dieser Tatsache durch die Verantwortlichen in Politik, bei den Herstellern von Wahlgeräten und Wahlcomputern, bei den Prüfungsstellen und bei den Wahlorganen findet ihren Niederschlag im Fehlen sinnvoller Sicherheitsregeln zum Umgang mit dieser Bedrohung sowie einer mangelnden Durchsetzung der bestehenden Regularien. Aus technischer Sicht liegen die größten Gefahren in den vielzähligen Möglichkeiten zur Manipulation von Hard- und Software von Wahlcomputern, die ihrerseits in vielen Fällen nicht oder nur unter großem finanziellen und zeitlichen Aufwand nachweisbar sein können.

Der kurze Überblick über die Geschichte der Verwendung von Wahlgeräten und Wahlcomputern bei Wahlen in der Bundesrepublik Deutschland und über den darüber entstandenen Diskurs zu Fragen der Sicherheit dieser technischen Wahlhilfsmittel macht deutlich, dass die Mehrzahl der politisch und technisch Verantwortlichen kritik-, beratungs- und lernresistent ist. Abgesehen von der, jedoch zur Erreichung des angestrebten Zieles untauglichen, Verschärfung der Sicherheitsmaßnahmen in Bezug auf die Kontrolle der Versiegelungen der Wahlgeräte und Wahlcomputer fast ein Jahr nach der Veröffentlichung der ersten erfolgversprechenden Angriffsmöglichkeiten wurden keine Konsequenzen gezogen. Entgegen Ankündigungen wurde keine Überarbeitung der einschlägigen rechtlichen Regelungen zu Wahlgeräten und Wahlcomputern oder der technischen Anforderungen an diese vorgenommen. Stattdessen übten sich die Verantwortlichen in Verharmlosung

Es ist zu hoffen, dass das Bundesverfassungsgericht auch diesmal seiner Aufgabe als Korrektiv rechts- und verfassungswidrigen Handelns des Staates und seiner Organe nachkommen wird. Die Grundlage dafür scheint mit der in dieser Arbeit vorgestellten Begründung der eingelegten Wahlprüfungsbeschwerde und der zustimmenden Stellungnahme des Chaos Computer Clubs gelegt.

Abbildungsverzeichnis

1 Oder- und Und-Relation für Angriffsbäume 29
2 Intentionen von Angreiferinnen und Angreifern 30
3 Wählertäuschung 31
4 Bruch des Wahlgeheimnisses 32
5 Übersicht Wahlfälschung 34
6 Wahlfälschung mit Papier und Stift 35
7 Wahlfälschung mit Papier und Geräten 36
8 Wahlfälschung mit mechanischen Wahlgeräten 36
9 Wahlfälschung mit elektromechanischen Wahlgeräten 37
10 Wahlfälschung mit Wahlcomputern 38
11 Mechanische Wahlgeräte „System Darmstadt“ 51
12 Mechanische Wahlgeräte „Schematus“ 52
13 Wahlcomputer des Herstellers Nedap 54

Literatur

[And01] Anderson, Ross:
Security Engineering.
Wiley Computer Publishing, 2001

[Asm07] Asmuth, Paul:
Wahlbeobachtungen, 13.05.2007. –
http://paulasmuth.de/?/blog/show/000011, Stand: 13.01.2008

[Aue06] Auel, Kersten:
Der Admiralin.
In: *iX – Magazin für professionelle Informationstechnik* (2006), Nr. 12, S. 119

[Beh06] Behörde für Inneres Hamburg:
Pressemitteilung: Bürgerschaft und Bezirksversammlungen werden 2008 digital gewählt, 31.10.2006. –
http://fhh.hamburg.de/stadt/Aktuell/pressemeldungen/2006/oktober/31/2006-10-31-bfi-pm-wahl-digitalerstift.html, Stand: 13.01.2008

[Bun77] Bundesregierung:
Bericht über den Einsatz von Wahlgeräten bei der Wahl zum 8. Deutschen Bundestag am 3. Oktober 1976, 07.02.1977. –
Drucksache 8/94

[Bun83] Bundesregierung:
Das endgültige Ergebnis der Wahl zum 10. Deutschen Bundestag, 25.03.1983. –
Bulletin der Bundesregierung Nr. 29, S. 251

[Bun02] Bundeswahlleiter:
Pressekonferenz „Bundestagswahl 2002“, 27.08.2002. –
http://www.wahlsysteme.de/Presseberichte/Statementm, Stand: 11.01.2008

[Bun06] Bundesministerium des Innern:
Stellungnahme zu den Wahleinsprüchen 76/05, 108/05, 145/05, 03.05.2006. –
http://www.ulrichwiesner.de/stellungnahme_BMI.html

[Bun07a] Bundesamt für Sicherheit in der Informationstechnik:
Zertifizierungsreport zum Schutzprofil Digitales Wahlstift-System.
Version 1.0.1, 14.03.2007

[Bun07b] Bundesregierung:
Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte et. al., 02.05.2007. –
Drucksache 16/5194

[Bus07] Busch, Christoph ; Fraunhofer IGD / Hochschule Darmstadt (Hrsg.):
Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften.

Fraunhofer IGD / Hochschule Darmstadt, 2007. –
Deutscher Bundestag, Innenausschuss, Ausschussdrucksache 16(4)192 A

[Cha06] Chaos Computer Club:
Pressemitteilung: Bericht der CCC-Wahlbeobachtergruppe von der Oberbürgermeisterwahl in Cottbus, 24.10.2006. –
http://www.ccc.de/updates/2006/bericht-ob-wahl-cottbus, Stand: 11.01.2008

[Cha07] Chaos Computer Club:
Pressemitteilung: Chaos Computer Club hackt Basistechnologie des Hamburger Wahlstifts, 25.10.2007. –
http://www.ccc.de/updates/2007/wahlstift-hack?language=de, Stand: 13.01.2008

[Cha08a] Chaos Computer Club:
Pressemitteilung: Chaos Computer Club: Wie erwartet erhebliche Probleme bei bayerischer Computer-Stimmenzählung, 05.03.2008. –
http://www.ccc.de/updates/2008/strichcode-bayern?language=de, Stand: 30.07.2008

[Cha08b] Chaos Computer Club:
Pressemitteilung: Chaos Computer Club geht juristisch gegen Wahlcomputer in Hessen vor, 07.01.2008. –
http://www.ccc.de/updates/2008/wahlcomputer-hessen?language=de, Stand: 09.01.2008

[Cha08c] Chaos Computer Club:
Pressemitteilung: Schwerwiegende Wahlcomputer-Probleme bei der Hessenwahl – Wahleinsprüche und Nachwahlen erwartet, 27.01.2008. –
http://www.ccc.de/updates/2008/wahlbeobachtungen-hessen?language=de, Stand: 28.01.2008

[CW:99] Die Kölner stimmten per Wahlcomputer ab.
In: *Computerwoche* 37 (1999). –
http://www.computerwoche.de/heftarchiv/1999/37/1088646/, Stand: 14.01.2008

[Deu73] Deutscher Bundestag:
Stenographisches Protokoll über die 55. Sitzung vom 5. Oktober 1973, 05.10.1973. –
S. 3202

[Feh07] Fehndrich, Martin:
Wahlbeobachtung: Abstimmung mit Wahlcomputern in Neuss, 18.05.2007. –
http://www.wahlrecht.de/news/2007/14.htm, Stand: 13.01.2008

[GHB+06] Gonggrijp, Rop ; Hengeveld, Willem-Jan ; Bogk, Andreas ; Engling, Dirk ; Mehnert, Hannes ; Rieger, Frank ; Scheffers, Pascal ; Wels, Barry ; Stiftung „Wij vertrouwen stemcomputers niet“ (Hrsg.):
Nedap/Groenendaal ES3B voting computer – a security analysis.

Stiftung „Wij vertrouwen stemcomputers niet“, 06.10.2006. –
http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/
Es3b-en.pdf

[Gro06] Groenendaal, Jan:
Das ‚Abhören‘ von Wahlgeräten und die Wahrung des Wahlgeheimnisses, Oktober 2006. –
http://www.wahlsysteme.de/Wahlnachrichten/2006_Abhoeren_
von_Wahlgeraeten.pdf, Stand: 09.01.2008

[Hau08] Hauck, Mirjam:
„Papierwahlen kann ich viel einfacher fälschen“.
In: *Süddeutsche Zeitung* (24.01.2008). –
http://www.sueddeutsche.de/computer/artikel/653/154255/, Stand: 28.01.2008

[Hie06] Hiekel, Sabine:
Pressemitteilung: Cottbuser Wahlgeräte sind sicher, 14.10.2006. –
http://www.wahlsysteme.de/Presseberichte/PM_KWL_vom_
141006.pdf, Stand: 09.01.2008

[HL08] Hölzlwimmer, Stephan ; Lang, Nicole:
Wahlbetrug im Wallfahrtsort: SPDler fälscht 113 Stimmzettel.
In: *Passauer Neue Presse* (29.03.2008). –
http://www.pnp.de/nachrichten/artikel.php?cid=29-
19450223&Ressort=pol&BNR=0, Stand: 30.07.2008

[HSG06a] HSG Wahlsysteme:
Presseinformation zur Anwendertagung am 31.05.2006 in Dortmund, 31.05.2006. –
http://www.wahlsysteme.de/Wahlnachrichten/2006_Presseinfo
_Anwendergemeinschaft.pdf, Stand: 09.01.2008

[HSG06b] HSG Wahlsysteme:
Statement zu der Nachricht „Bürgerinitiative in den Niederlanden hackt Nedap Wahlmaschine“, Oktober 2006. –
http://www.wahlsysteme.de/Wahlnachrichten/
2006_Niederlaender_hacken_Wahlgeraet01.pdf,
Stand: 09.01.2008

[HSG07a] HSG Wahlsysteme:
Bedienungsanleitung Wahlgerät ESD1und ESD2, 28.09.2007. –
http://www.wahlrecht.de/doku/doku/20070928
_bedienungsanleitung.pdf, Stand: 29.07.2008

[HSG07b] HSG Wahlsysteme:
Muster: Wahlgeräte Begleitschein, 29.09.2007. –
http://www.wahlrecht.de/doku/doku/20071213_muster
_wahlgeraete-begleitschein.pdf, Stand: 29.07.2008

[Inn02] Innenministerium Nordrhein-Westfalen:
Pressemitteilung: NRW Spitzenreiter: In 16 Kommunen wird elektronisch gewählt – Innenminister Behrens: Wahl per Knopfdruck Verfahren der Zukunft, 04.09.2002. –
http://www.im.nrw.de/pe/pm2001/pm2001/news_833.htm, Stand: 13.01.2008

[Inn06] Innenministerium Hessen:
Kleine Anfrage des Abg. Rentsch (FDP) vom 05.04.2006 betreffend Wahlmaschinen in Hessen und Antwort des Ministers des Innern und für Sport, 06.06.2006. –
Drucksache 16/5473

[Jon06] Jongerius, Stephan:
Raadslid Landerd is stuk minder populair in schaduwverkiezing.
In: *Brabants Dagblad* (13.08.2006). –
http://web.archive.org/web/20060813174629/http://www.brabantsdagblad.nl/brabant/article247185.ece, Stand: 30.07.2008

[Kle05] Klein, Jakob:
Bitte keine Kreuze machen!
In: *Frankfurter Allgemeine Sonntagszeitung* 33 (21.08.2005), S. 58

[Kle06] Kleinz, Torsten:
Wahlcomputer in Cottbus geprüft und versiegelt.
In: *heise online* (14.10.2006). –
http://www.heise.de/newsticker/meldung/79480, Stand: 09.01.2008

[KR07] Kurz, Constanze ; Rieger, Frank:
NEDAP-Wahlcomputer – Manipulationsmethoden an Hard- und Software.
In: *Informatik Spektrum* 30 (2007), Oktober, Nr. 5, S. 313

[KRG07] Kurz, Constanze ; Rieger, Frank ; Gonggrijp, Rop:
Beschreibung und Auswertung der Untersuchungen an NEDAP-Wahlcomputern, 30.05.2007. –
http://www.ccc.de/press/releases/2007/20070609/nedapReport54.pdf

[KTC+08] King, Samuel T. ; Tucek, Joseph ; Cozzie, Anthony ; Grier, Chris ; Jiang, Weihang ; Zhou, Yuanyuan:
Designing and Implementing Malicious Hardware.
In: *Proceedings of the First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2008

[Lan07] Landesregierung Nordrhein-Westfalen:
Antwort auf die Kleine Anfrage 1719 des Abgeordneten Horst Becker, 18.07.2007. –

Drucksache 14/4723

[Mag61] Magistrat der Stadt Darmstadt:
Bekanntmachung über die Verwendung von Stimmenzählgeräten zur Bundestagswahl 1961, 08.09.1961

[Min04] Ministerium des Innern Rheinland-Pfalz:
Pressemitteilung: Bruch: In Rheinland-Pfalz eingesetzte elektronische Wahlgeräte sind sicher, 30.12.2004. –
http://www.wahlsysteme.de/Wahlnachrichten/2005_Studie_RP.pdf, Stand: 09.01.2004

[Moh04] Mohr, Heinz-Peter:
Knopfdruck ersetzt das Kreuzchen.
In: *Marler Zeitung* (06.03.2004)

[Phy04] Physikalisch-Technische Bundesanstalt:
Prüfbericht – Baumusterprüfung eines Wahlgerätes Nedap ESD1, 12.05.2004. –
http://www.wahlrecht.de/doku/doku/PB-ESD1-SW03.08-BTW.pdf

[Phy06] Physikalisch-Technische Bundesanstalt:
Pressemitteilung: Wahlgeräte in der Kritik, 09.10.2006. –
http://www.ptb.de/de/aktuelles/archiv/presseinfos/pi2006/pitext/pi061009.htm, Stand: 09.01.2008

[Phy07a] Physikalisch-Technische Bundesanstalt:
Prüfbericht – Baumusterprüfung eines Wahlgerätes Nedap ESD1 mit Steuerungsprogramm SSD1, 11.10.2007. –
http://www.wahlrecht.de/doku/doku/20071011_ptb-8.51-pb-003.07.pdf

[Phy07b] Physikalisch-Technische Bundesanstalt:
Prüfbericht – Baumusterprüfung eines Wahlgerätes Nedap ESD1 mit Steuerungsprogramm SSD1, 11.10.2007. –
http://www.wahlrecht.de/doku/doku/20071011_ptb-8.51-pb-006.07.pdf

[Phy07c] Physikalisch-Technische Bundesanstalt:
Prüfbericht – Baumusterprüfung eines Wahlgerätes Nedap ESD2 mit Steuerungsprogramm SSD1, 11.10.2007. –
http://www.wahlrecht.de/doku/doku/20071011_ptb-8.51-pb-001.06.pdf

[Phy07d] Physikalisch-Technische Bundesanstalt:
Anforderungen an die Software von Wahlgeräten, Version 2, 12.10.2007. –
http://ib.ptb.de/8/85/851/ANF-WAHLGERAETE-ALLG-DT_V2.PDF

[Phy07e] Physikalisch-Technische Bundesanstalt:
Prüfbericht – Baumusterprüfung eines Wahlgerätes Nedap ESD2 mit Steuerungsprogramm SSD1, 24.10.2007. –
http://www.wahlrecht.de/doku/doku/20071024_ptb-8.51-pb-004.06.pdf

[Poh07] Pohle, Jörg:
Wahlrecht und Wahlcomputer – Zu Genehmigung und Einsatz von Wahlcomputern aus rechtlicher Sicht.
2007

[Ric07] Richter, Dieter:
Wahlgeräte in Deutschland: Eine Erwiderung.
In: *Informatik Spektrum* 30 (2007), Dezember, Nr. 6, S. 440

[Sch03] Schneider, Ingo:
Koblenz wählt bald per Knopfdruck.
In: *Rhein-Zeitung* (03.12.2003). –
http://rhein-zeitung.de/03/12/03/b/lok/00000794.html,
Stand: 11.01.2008

[Sch04] Schneier, Bruce:
Secrets and lies: digital security in a networked world.
Wiley Computer Publishing, 2004

[Sch06] Schelp, Stefan:
Bad Oeynhausener wählen den Landrat per Knopfdruck.
In: *Neue Westfälische Zeitung* (2./3. Dezember 2006). –
http://www.wahlsysteme.de/Presseberichte/
2006_Landrat_Bad_Oeynhausen.pdf,
Stand: 11.01.2008

[Sie04] Sietmann, Richard:
E-Voting - ein Spiel mit dem Feuer.
In: *c't – magazin für computer technik* 23 (2004), S. 100

[Sie05] Sietmann, Richard:
Dreimal drücken - fertig?
In: *c't – magazin für computer technik* 19 (2005), S. 54

[Sie06] Sietmann, Richard:
„Eine neue Situation".
In: *c't – magazin für computer technik* 24 (2006), S. 72

[Sie07a] Sietmann, Richard:
Wittenberge bleibt vorerst bei Papierstimmzetteln.
In: *heise online* (01.05.2007). –
http://www.heise.de/newsticker/meldung/107274,
Stand: 30.07.2008

[Sie07b] Sietmann, Richard:
Innenministerium erteilt „verbesserten" Wahlcomputern Zulassung.
In: *heise online* (02.11.2007). –
http://www.heise.de/newsticker/meldung/98369,
Stand: 11.01.2008

[Sie07c] Sietmann, Richard:
Aus für den digitalen Wahlstift.
In: *heise online* (16.11.2007). –
http://www.heise.de/newsticker/meldung/99089,
Stand: 11.01.2008

[Sie07d] Sietmann, Richard:
Wahlcomputer und die Grenzen der Informationsfreiheit.
In: *heise online* (18.10.2007). –
http://www.heise.de/newsticker/meldung/97566,
Stand: 11.01.2008

[Sor06] Sorger, Roland:
Pressemitteilung: Wahlgeräte: Hacker und andere Manipulationen ausgeschlossen, 26.10.2006. –
http://www.wahlen-langen.de/c284/m185/d575/default.html, Stand: 13.01.2008

[Sta93] Staatsgerichtshof des Landes Hessen:
Beschluss P.St. 1161 e.V., 04.03.1993

[Ste06] Stein, Holger ; Initiative Nachrichtenaufklärung (Hrsg.):
Bedenklicher Einsatz von Wahlmaschinen.
Initiative Nachrichtenaufklärung, 14.02.2006. –
http://www.nachrichtenaufklaerung.de/top.php?year=2005&
title=QmVkZW5rbGljaGVyIEVpbnNhdHogdm9uIFdhaG
xtYXNjaGluZW4=, Stand: 13.01.2008

[Sti00] Stieler, Wolfgang:
Die Differenz-Maschine.
In: *c't – magazin für computer technik* 25 (2000), S. 35

[VV07] Volkamer, Melanie ; Vogt, Roland ; Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH, Prüfstelle für IT-Sicherheit (Hrsg.):
Common Criteria Schutzprofile – Digitales Wahlstift-System.
Version 1.0.1.
Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH, Prüfstelle für IT-Sicherheit, 28.02.2007. –
http://www.bsi.de/zertifiz/zert/reporte/PP0031b.pdf

[Wah81] Wahlprüfungsausschuss des Deutschen Bundestages:
Beschlußempfehlung und Bericht zu den gegen die Gültigkeit der Wahl zum 9. Deutschen Bundestag eingegangenen Wahleinsprüchen, 08.04.1981. –
Drucksache 9/316

[Wah91] Wahlprüfungsausschuss des Deutschen Bundestages:
Beschlußempfehlung und Bericht zu den gegen die Gültigkeit der Wahl zum 12. Deutschen Bundestag eingegangenen Wahleinsprüchen, 30.07.1991. –

Drucksache 12/1002

[Wah99] Wahlprüfungsgericht beim Hessischen Landtag:
Urteil zur Gültigkeit der Landtagswahl 1999, 1999. –
Staatsanzeiger für das Land Hessen 30/1999, S. 2350

[Wah06] Wahlprüfungsausschuss des Deutschen Bundestages:
Dritte Beschlussempfehlung des Wahlprüfungsausschusses zu 44 gegen die Gültigkeit der Wahl zum 16. Deutschen Bundestag eingegangenen Wahleinsprüchen, 30.11.2006. –
Drucksache 16/3600

[Wie05] Wiesner, Ulrich:
Wahleinspruch WP 145/05, 06.11.2005. –
http://www.ulrichwiesner.de/wp/WP145_05a.pdf

[Wie07a] Wiesner, Ulrich:
Wahlprüfungsbeschwerde 2 BvC 3/07, 12.02.2007. –
http://www.ulrichwiesner.de/wp/070212
_wahlpruefbeschwerde.pdf

[Wie07b] Wiesner, Ulrich:
Entgegnung zu den Stellungnahmen von BMI, PTB und CCC, 30.07.2007. –
http://www.ulrichwiesner.de/wp/070730JBB.pdf

[Wik] Wikipedia:
Wahlfälschungsskandal von Dachau. –
http://de.wikipedia.org/w/index.php?title=
Wahlfälschungsskandal_von_Dachau&oldid=46120638; Stand: 14.06.2008

[Wil08] Wilkens, Andreas:
Niederlande verzichten auf Wahlcomputer.
In: *heise online* (19.05.2008). –
http://www.heise.de/newsticker/meldung/108050,
Stand: 30.07.2008

[Win04] Winter, Marie-Anne:
Tasten tippen statt Kreuzchen machen.
In: *teltarif.de* (10.05.2004). –
http://www.teltarif.de/arch/2004/kw20/s13681.html,
Stand: 13.01.2008

[Wis08] Wissenschaftsrat:
Stellungnahme zur Physikalisch-Technischen Bundesanstalt (PTB), Braunschweig und Berlin, Mai 2008. –
http://www.wissenschaftsrat.de/texte/8477-08.pdf,
Stand: 30.07.2008

[Zei60] Die Wahlmaschine.
In: *Die Zeit* 46 (1960), S. 7. –
http://www.zeit.de/1960/46/Die-Wahlmaschine,
Stand: 14.02.2008

[Zie05] Ziegler, Peter-Michael:
Innenministerium hält Prüfberichte von elektronischen Wahlmaschinen unter Verschluss.
In: *heise online* (16.09.2005). –
http://www.heise.de/newsticker/meldung/64013,
Stand: 11.01.2008