**Rainer W. Gerling**

# Hackerangriff auf die Wahlfreiheit

*Politische Wahlen finden bei uns nach wie vor auf Papier statt. Eigentlich erstaunlich in Zeiten, in denen wir uns im Internet informieren und einkaufen, die Heizung daheim per App steuern und sogar der Personalausweis eine Online-Funktion hat. Wäre es nicht viel einfacher und bequemer, am heimischen PC oder via Smartphone die Bundestagsabgeordneten zu voten?*
*Lieber nicht. Auch ohne Internetwahlen drohen viele Manipulationsmöglichkeiten auf elektronischem Wege.*

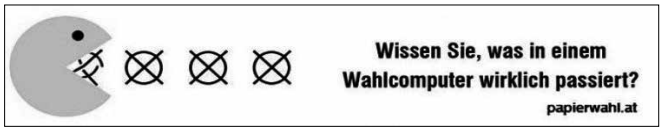


Um es gleich vorwegzunehmen: Politische Wahlen im Internet wird es in absehbarer Zeit zumindest in Deutschland nicht geben. Und das ist gut so. Sicher wäre das Wählen im Internet einfach und komfortabel, vielleicht würden sogar mehr Bürger online ihre Stimme abgeben – trotzdem mag man sich einen Wahlvorgang komplett im Internet für politische Wahlen lieber nicht vorstellen. Ein Angriff auf die Computer der Wähler könnte von jedem Ort der Welt vorgenommen werden, Manipulationen von den verschiedensten Seiten wären Tür und Tor geöffnet. *Ronald L. Rivest* hat dafür ein treffendes Bild geprägt: Im Jahr 2016 beantwortete er in einem Vortrag die Frage nach den Best Practices für eine Internetwahl mit der Gegenfrage nach den Best Practices für das Spielen auf einer verkehrsreichen Straße.[1]

Wahlen müssen geheim, frei und sicher sein. Geheim heißt, dass niemand mitbekommt, wie eine Wählerin oder ein Wähler abstimmt. Damit eine Wahl wirklich frei ist, dürfen Wähler auch keinen Beleg für eine konkrete Stimmabgabe erhalten. Ein Handyfoto aus der Wahlkabine, um die eigene Stimmabgabe zu dokumentieren, ist keine gute Idee. Es muss sichergestellt werden, dass eine Stimme für eine bestimmte Kandidatin oder einen bestimmten Kandidaten nicht erpresst oder gekauft werden kann. Sicher bedeutet, dass die Stimmen unmanipuliert ausgezählt werden können. Und da kommen schon bei Wahlmaschinen, wie sie in den USA weitverbreitet sind, gewisse Zweifel auf.

## Die Stimmabgabe auf Papier findet nur noch in 18 US-Bundesstaaten statt

In den Vereinigten Staaten setzen nur noch 18 der 50 Staaten auf eine ausschließlich papierbasierte Stimmabgabe. Zehn Staaten verwenden zumindest teilweise Wahlmaschinen ohne Kontrollausdrucke auf Papier (zum potenziellen manuellen Nachzählen). Bei diesen Geräten ist eine nachträgliche Kontrolle der digitalen Stimmauszählung kaum möglich. Und selbst wenn die Wähler zur Kontrolle einen Papierbeleg erhalten, den sie in eine Wahlurne legen – für Laien ist dann auch weiterhin nicht nachvollziehbar, ob die Maschine die identische Stimmabgabe speichert.




*Wir danken papierwahl.at für die Druckgenehmigung.*

Grundsätzlich ist Misstrauen gegenüber Wahlmaschinen angebracht: So gab es in der Vergangenheit Probleme mit der Software der Geräte. Im Jahr 2008 wurde etwa bekannt, dass Wahlcomputer der Firma *Premier Election Solutions* beim Zusammenführen von Ergebnissen mehrerer Wahlcomputer einen Teil der Stimmen „vergaßen". Da ein erneuter Zulassungsprozess Jahre dauert, veröffentlichte die Firma einen *Workaround* in Form einer geänderten Bedienungsanleitung. Die Fehlbedienung wird nicht technisch verhindert, vielmehr wird dem Anwender nur gezeigt, wie er sie vermeidet. So werden Fehler nicht ausgeschlossen.

Auch die Sicherheitssysteme von Wahlmaschinen sind äußerst zweifelhaft. Der Experte *Jeremy Epstein* schreibt in seinem Blog-Beitrag *Decertifying the worst voting machine in the US* des *Princeton Center for Information Technology Policy* über unglaubliche Sicherheitslücken bei Wahlcomputern.[2] So wird beispielsweise für die WEP-Verschlüsselung im WLAN der Code „abcde" verwendet. Dieser Schlüssel ist *fest verdrahtet* und nicht änderbar. Einige Systeme haben seit 2004 keine Sicherheits-Patches erhalten. USB-Ports und andere physische Zugänge sind nicht immer abgesichert. Wer ein USB-Gerät in einen ungesicherten USB-Port stecken kann, kann wahrscheinlich Manipulationen vornehmen. *Bruce Schneier,* ein international anerkannter US-amerikanischer IT-Sicherheitsexperte, berichtete, Wahlcomputer hätten die Default-Passworte „abcde" oder „admin" gehabt.[3] Da Wahlcomputer durchaus auch WLAN zur Kommunikation benutzen, ist ein Einbruch selbst aus einiger Distanz denkbar.

## Manipulierte Software bringt den Wahlcomputer zum Schachspielen

Im Jahr 2007 demonstrierten niederländische und deutsche Hacker, dass man einem *Nedap*-Wahlcomputer durch Verändern der Software das Schachspielen beibringen kann.[4] Damit zeigten sie, dass beliebige Veränderungen der Software unbefugt möglich sind. Es ist sicher ein großer Aufwand, Wahlmaschinen zu hacken. Aber die im Erfolgsfall großen Auswirkungen rechtfertigen aus Sicht des Angreifers durchaus den Aufwand. Dazu kommt: Während etwa Unternehmen ein starkes eigenes Interesse daran haben, dass ihre Computersysteme sicher sind, und Sicherheitssysteme wie eine Firewall haben, um sich gegen Angriffe von außen zu schützen, ist bei Wahlmaschinen auch der Betreiber ein möglicher Angreifer. So kann der Betreiber, ohne sich verdächtig zu machen, flächendeckend Updates in die Wahlmaschinen einbringen. Eine Überprüfung durch Wählerinnen und Wähler oder auch Wahlhelfer vor Ort ist nicht möglich. Das Gerät auch vor potenziellen Manipulationen durch den Betreiber zu schützen, ist eine weit größere Herausforderung.

Wahlcomputer technisch komplett abzuschotten, ist keine Option, da zumindest die aktuellen Stimmzettel vor der Wahl eingespielt werden müssen. Dies geschieht in der Regel durch das Einstecken von Speicherkarten, die häufig auf Windows-Rechnern beschrieben werden. Die gleichen Speicherkarten dienen auch dem Update der Software: Ist eine Datei mit einem be-

stimmten Namen vorhanden, sieht das Gerät den Inhalt der Datei als Software-Update an und installiert sie. Jeder, der kurze Zeit Zugriff auf die Wahlmaschine hat, kann eine Speicherkarte einschieben und beliebige Software einspielen.

Die Sicherheit von Wahlmaschinen gilt mit Recht als zweifelhaft. Trotzdem sind flächendeckende Manipulationen eher unwahrscheinlich. Wenn Wahlcomputer gehackt werden, ist davon auszugehen, dass nicht pauschal alle Modelle davon betroffen sind, sondern nur einige. Auch bei normalen Computern erleben wir, dass ein Hack eines Windows-Rechners nicht unbedingt auf einem Apple- oder Linux-Rechner funktioniert. In den Vereinigten Staaten sind immerhin 53 unterschiedliche Wahlgeräte von 17 Herstellern im Einsatz.

Zudem gibt es bis jetzt keine Beweise für die Manipulation von Wahlcomputern. Eine Gruppe, zu der auch der Leiter des *Center for Computer Security and Society* der *University of Michigan, J. Alex Halderman,* gehört, hat zwar behauptet, dass *Hillary Clinton* in Wisconsin in Stimmbezirken mit Wahlcomputern etwa sieben Prozent weniger Stimmen erhielt als in Stimmbezirken mit Papierstimmzetteln.[5] Die Unterschiede lassen sich jedoch auch durch systematische Fehler oder durch zufällige Korrelationen zwischen dem Typus der Wahlmaschine und demografischen Faktoren erklären. Man kann also nur spekulieren, ob die Präsidentschaftswahlen in den USA manipuliert wurden. Ein fader Beigeschmack und ein ungutes Gefühl bleiben.

Auch in Deutschland wurden in der Vergangenheit bei verschiedenen Wahlen bereits Wahlcomputer verwendet. Zwei Beschwerden (2 BvC 3/07, 2 BvC 4/07) gegen „den Einsatz von rechnergesteuerten Wahlgeräten" führten dazu, dass 2009 die Bundeswahlgeräteverordnung vom Bundesverfassungsgericht für verfassungswidrig erklärt wurde, „weil sie nicht sicherstellt, dass nur solche Wahlgeräte zugelassen und verwendet werden, die den verfassungsrechtlichen Voraussetzungen des Grundsatzes der Öffentlichkeit genügen". Voraussetzung sei, „dass die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können". Dies ist bei den derzeitigen Wahlcomputern nicht gewährleistet. So kamen seither in Deutschland keine Wahlcomputer mehr zum Einsatz.

Bleibt die Frage, welche Gründe überhaupt für die Geräte sprechen. Der einzige Vorteil ist, dass sie das Auszählen vereinfachen, schneller und billiger machen. Für die Wählerin oder den Wähler wird der Wahlvorgang dadurch nicht erleichtert. Wahlcomputer können lediglich ungültige Stimmzettel technisch verhindern. Eine ungültige Stimme abzugeben, kann aber auch eine bewusste Wahlentscheidung sein.

Es gibt also viele gute Gründe, die klassischen papierenen Stimmzettel bei politischen Wahlen beizubehalten. Nur wenn wir unser Kreuz mit einem normalen Stift auf normales Papier machen können, ist sichergestellt, dass die Auszählung zeitnah und öffentlich – unter Wahrung des Mehraugenprinzips – erfolgt. Auch während der Stimmabgabe ist das Mehraugenprinzip zur Beobachtung der Wahl sichergestellt.

Allerdings sind Wahlmaschinen wohl nicht dauerhaft aus deutschen Wahllokalen verbannt. Hersteller und Kommunen, die aufs Geld schauen, werden versuchen, wieder elektronische Systeme für die Stimmabgabe und -auszählung einzuführen. Wenn Wahlmaschinen eingesetzt werden, darf dies nicht geschehen mit dem Argument: „Vertrau uns, wir machen das schon richtig." Und das „wir" kann dabei sowohl den Hersteller der Wahlmaschinen als auch den Staat meinen. Die Grundeinstellung muss sein: „Es werden Pannen geschehen, wir müssen sie feststellen und korrigieren." Die Möglichkeiten zu einem Audit müssen in die elektronischen Wahlverfahren eingebaut sein, und ein Audit der Wahlergebnisse muss zwingend durchgeführt werden.

Bei der Bundestagswahl 2017 wird es keine manipulierten Wahlmaschinen geben, aber damit ist die Gefahr digitaler Manipulationen keineswegs gebannt: So müssen die Wahlergebnisse aus den Wahllokalen eingesammelt werden, was über digitale Netze geschieht. Der Bundeswahlleiter *Dieter Sarreither* rechnet mit Hackerangriffen und hat deshalb vorsorglich das verwendete Verwaltungsnetz besonders sichern lassen.[6] Notfalls kann auf Telefon- und Faxkommunikation zurückgegriffen werden. In den Niederlanden wurde bei der Wahl am 15. März 2017 mit der Hand ausgezählt, da die sonst verwendete Software als anfällig für Hacks gilt. Kuriere brachten die Ergebnisse aus den Wahllokalen in die regionalen Wahlbüros. Erst dort wurden dann Computer eingesetzt.[7]

Die Wahlen selbst können bei uns also als sicher gelten, aber es ist zu befürchten, dass Hacker versuchen, im Vorfeld Einfluss auf das Ergebnis zu nehmen. In den USA war das offensichtlich der Fall: Am 6. Januar 2017 veröffentlichten CIA, FBI und NSA einen gemeinsamen Bericht, dass russische Dienste die Präsidentschaftswahlen in den USA beeinflusst hätten.[8] Demnach wurde das Computernetz des *Democratic National Committee* im Juli 2015 gehackt. Bis Mai 2016 wurden im großen Stil Dokumente gestohlen. Später wurden diese Dokumente unter dem (möglicherweise russischen) Pseudonym *Guccifer 2.0* von *DC Leaks* und *Wikileaks* veröffentlicht. Da mit diesen Dokumenten im Wesentlichen die Demokraten und ihre Kandidatin Hillary Clinton diskreditiert werden sollten, kann dies als – zumindest versuchte – Wahlbeeinflussung gesehen werden. Die russische Regierung weist diesen Verdacht weit von sich. Öffentlich verfügbare Beweise, dass russische Dienste hinter den Vorgängen stecken, gibt es nicht.

### Digitale Verbrecher hinterlassen Spuren, handfeste Beweise gibt es kaum

Aber es gibt mehr oder weniger starke Hinweise. Solche Indizien für digitale Vergehen lassen sich natürlich nicht so leicht dingfest machen wie Beweismittel in der realen Welt: Bei einem klassischen Tatort findet die Polizei Fingerabdrücke, Fasern und DNA-Spuren, die sie letztendlich einer oder mehreren Personen zuordnen kann. An einem digitalen Tatort finden Ermittler Schadsoftware und in der Analyse der Kommunikation etwa IP- oder E-Mail-Adressen. Diese Bits und Bytes jemandem zuzuordnen, ist jedoch wesentlich schwieriger als bei klassischen Indizien.

So suchen digitale Forensiker in der Schadsoftware beispielsweise nach russischen oder chinesischen Textfragmenten. Sie sind kein Beweis, da genauso gut Hacker aus einem anderen Land eine falsche Fährte gelegt haben können. Wenn der Fo-

rensiker Glück hat, ist die Schadsoftware eine Optimierung oder Weiterentwicklung einer bekannten Schadsoftware, von der man weiß, dass etwa russische oder chinesische staatliche Stellen sie schon lange einsetzen. Dann gibt es bereits zwei Indizien. Die ausspionierten Daten werden bei einem Server abgeliefert. Der steht irgendwo in Europa oder Amerika bei einem Provider. Hierzu mieten die Angreifer einfach Rechner bei Dienstleistern und melden Domains an. Wenn der Domainname jedoch über eine E-Mail-Adresse registriert wurde, die schon länger russischen oder chinesischen staatlichen Stellen zugeordnet werden konnte, hat man einen weiteren Hinweis in der Hand. Auch kann den Ermittlern etwa die spezielle Technik der Datenübertragung bereits länger bekannt sein, und sie können sie mit älteren Vorfällen vergleichen. Die genauen technischen Details dieser Analysen sind jedoch ein gut gehütetes Betriebsgeheimnis der ermittelnden Geheimdienste.

Ein weiteres Indiz kann die Interessenlage sein: Bei einem Angriff auf die IT-Infrastruktur des *Uigurischen Weltkongresses* ist die Wahrscheinlichkeit hoch, dass es sich um chinesische staatliche Stellen handelt, da der Uigurische Weltkongress zu den sogenannten *Fünf Giften,* den Hauptbedrohungen des chinesischen Staates, gehört. Wenn dagegen – wie am 23. Dezember 2016 – in der Westukraine ein großer Stromausfall für Probleme sorgt, der auf einen Cyberangriff zurückgeht, dann ist es höchst unwahrscheinlich, dass chinesische staatliche Stellen die Urheber waren. Hier spricht eher einiges für einen russischen Ursprung.

Umfangreiches gesammeltes Wissen bei Sicherheitsfirmen und -behörden vermag in der Gesamtschau ein plausibles Bild zu ergeben. Die endgültigen Erkenntnisse werden veröffentlicht, sie sind aber von außen nicht ohne Weiteres nachvollziehbar. Und klar ist auch: Ein plausibles Bild ist noch lange kein gerichtsfester Beweis. Parallel zu den Fällen in den Vereinigten Staaten stellt sich die Frage, ob die Bundestagswahl ähnlich gefährdet ist wie die US-amerikanische Präsidentschaftswahl. Zumindest gab es in den vergangenen 24 Monaten bereits mehrere Hackerangriffe auf deutsche Parteien und Regierungsstrukturen.

### Angreifer könnten versuchen, vor der Bundestagswahl die öffentliche Meinung zu manipulieren

Im Frühjahr 2015 brachen Hacker in das *Parlakom*-Netz des Deutschen Bundestags ein und kopierten etwa 16 Gigabyte Daten. Deutsche Sicherheitsbehörden gehen davon aus, dass dafür eine staatsnahe russische Hackergruppe verantwortlich war, die unter anderem unter dem Namen *APT28* bekannt ist. Diese Gruppe ist seit etwa 2004 aktiv. APT28 wird auch der Angriff auf den französischen Fernsehsender *TV5 Monde* im April 2015 zugeschrieben, wie *Hans-Georg Maaßen,* Präsident des Bundesamts für Verfassungsschutz, in einer Podiumsdiskussion während der IT-Sicherheitstagung 2015 der Max-Planck-Gesellschaft sagte. Die Attacke gilt übrigens als *False-Flag-Operation,* da es ein wohl gefälschtes Bekennerschreiben einer bis dahin unbekannten islamischen Gruppe namens *Cyber Caliphate* gab.

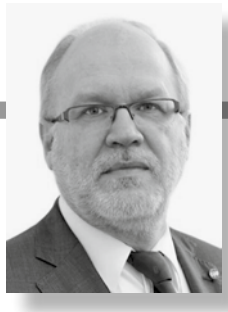
Das Sicherheitsunternehmen *Trend Micro* berichtete im Mai 2016, dass die Gruppe APT28 einen Angriff gegen die CDU gestartet habe.[9] Dazu wurde ein nachgebauter CDU-Webmail-Server in Litauen betrieben, um dann mit Phishing-E-Mails Benutzerkonten und Passwörter abzugreifen.

Im August 2016 schickte ein *Heinrich Krammer* eine E-Mail, die vermeintlich aus dem Nato-Hauptquartier kam (E-Mail-Adresse endet auf *@hq.nato.int)*. Die E-Mail versprach Hintergrundinformationen unter anderem über den Militärputsch in der Türkei. Wer auf den Link in der Mail klickte, installierte eine Schadsoftware auf seinem Rechner. Adressaten der E-Mail waren *Sahra Wagenknecht* und die Bundesgeschäftsstelle der Linken sowie die Junge Union und die CDU im Saarland. Auch hier vermuten Sicherheitskreise die Gruppe APT28 als Urheber.[10]

Im November 2016 veröffentlichte Wikileaks 90 Gigabyte Daten (2420 Dokumente) aus dem NSA-Untersuchungsausschuss des Deutschen Bundestages. Diese Daten scheinen nicht aus dem Bundestags-Hack vom Frühjahr 2015 zu stammen. Die Parallelen zum Vorgehen der Hacker in den USA sind auffällig. Insofern muss damit gerechnet werden, dass in der heißen Phase des Wahlkampfs in Deutschland Informationen aus diesen Hacks auf Wikileaks oder vergleichbaren Plattformen auftauchen.

Das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* beschäftigt sich als die deutsche nationale Cyber-Sicherheitsbehörde intensiv mit dem Thema. BSI-Präsident *Arne Schönbohm* warnte im Herbst 2016 die Parteien persönlich vor Ausspähung durch staatliche Hacker.[11] Der Verdacht, der dabei im Raum steht: Vor der Bundestagswahl könnten Angreifer versuchen, die öffentliche Meinung zu manipulieren. Im Fokus stehen auch automatisierte Meinungsplatzierungen im Internet oder in sozialen Netzen. Im März 2017 warnte das BSI die politischen Parteien in Deutschland nochmals deutlich vor zu erwartenden Cyberangriffen während des Wahlkampfs.[12]

Anfang Februar 2017 gab es Medienberichte, wonach deutsche Geheimdienste keine Beweise für gezielte russische Desinformation gefunden haben. Trotzdem nennt der 50-seitige Bericht laut Recherchen von NDR, WDR und Süddeutscher Zeitung die Be-



**Rainer W. Gerling**

Prof. Dr. **Rainer W. Gerling** ist IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft sowie Honorarprofessor für das Fachgebiet IT-Sicherheit an der Fakultät für Informatik und Mathematik der Hochschule München. Dort ist der habilitierte Physiker für die Zusatzausbildung „Betrieblicher Datenschutz“ im Fachbereich Informatik verantwortlich.

richterstattung russischer Propagandamedien wie der deutschsprachigen Ausgabe von *Russia Today* oder *Sputnik News* geradezu „feindselig“.[13] Wo ist die Grenze zwischen überspitzter Berichterstattung und Desinformation?

Dass Staaten versuchen, durch Desinformation, Propaganda, Fake-News und alternative Fakten (altmodisch auch Lügen genannt) die öffentliche Meinung in ihrem Sinn zu beeinflussen, ist nichts Neues. Das Internet, soziale Medien und Plattformen wie Wikileaks haben die Zahl der Informationsanbieter jedoch dramatisch steigen lassen. Klassische journalistische Ethik und Wahrhaftigkeit sind dabei vielfach auf der Strecke geblieben. Eine Richtigstellung und Bewertung durch klassische Medien und Experten oder gar staatliche Stellen ist schwierig. Die Lebenserfahrung zeigt uns, dass doch immer irgendetwas hängen bleibt. Letztendlich müssen jede Bürgerin und jeder Bürger für sich entscheiden, was sie glauben und was nicht. Dabei hilft nur eines: Bildung. Insofern sollten wir in Europa ein bisschen weniger anfällig für alternative Fakten sein als die US-Bürgerinnen und -Bürger, da das Bildungsniveau in Europa im Mittel höher ist.

## Ergänzung nach der französischen Präsidentenwahl

Am Freitagabend vor der Stichwahl in Frankreich wurden die *Macron-Leaks* veröffentlicht: eine große Menge von Dokumenten, die sowohl in Teilen gefälscht, verändert und auch echt waren. Die Veröffentlichung wird APT 28 zugeschrieben, auch wenn es dafür keine Beweise gibt.[14]

Ergänzte Fassung aus *MaxPlanckForschung 1/2017*. Nachdruck mit freundlicher Genehmigung.

## Anmerkungen

1 *https://people.csail.mit.edu/rivest/pubs/Riv16z.slides.pdf*
2 *https://freedom-to-tinker.com/2015/04/15/decertifying-the-worst-voting-machine-in-the-us/8*
3 *https://www.schneier.com/blog/archives/2015/04/an_incredibly_i.html*
4 *http://heise.de/-290710*
5 *http://nymag.com/daily/intelligencer/2016/11/activists-urge-hillary-clinton-to-challenge-election-results.html*
6 *http://www.faz.net/aktuell/politik/bundeswahlleiter-will-bundestagswahl-vor-hackerangriffen-schuetzen-14651555.html*
7 *http://www.faz.net/aktuell/politik/inland/aus-sorge-vor-hackangriffen-verzichten-niederlande-auf-wahlcomputer-14824128.html*
8 *https://www.dni.gov/files/documents/ICA_2017_01.pdf*
9 *http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-german-christian-democratic-union/*
10 *https://www.wirtschaftsschutz.info/SharedDocs/Kurzmeldungen/DE/ITSicherheit/Warnmeldung_Neu.html*
11 *http://www.sueddeutsche.de/politik/bundesregierung-ist-alarmiert-hackerangriff-aufdeutsche-parteien-1.3170347*
12 *http://www.spiegel.de/netzwelt/netzpolitik/bundestagswahl-2017-bsi-chef-arne-schoenbohm-warnt-parteien-vor-hacker-angriffen-a-1136542.html*
13 *http://www.tagesschau.de/inland/deutsche-geheimdienste-russland-101.html*
14 *https://www.heise.de/tp/features/Macron-Leaks-Die-Geschichte-zum-massiven-Hack-3711374.html*



Dagmar Boedicker

## Wider den lähmenden Pessimismus

*Wie kommt es, dass viele Europäer.innen das Europaparlament und die Kommission verwünschen und meinen, sie wären glücklicher für sich allein in ihrem mehr oder weniger kleinen Land? In weniger als einer Generation haben sich die Europäische Union und Deutschland so stark verändert, dass sie kaum wiederzuerkennen sind. Die in den 80ern noch optimistische Perspektive auf eine in Zukunft pfleglich behandelte Umwelt, wachsenden Wohlstand und mehr Gerechtigkeit hier und in der Welt ist Wut oder Resignation gewichen. Was ist passiert?*

*erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de*

Von zwei Blöcken mit gegensätzlichen [illegible] überschaubaren Einflusssphären [illegible] Generation wird es weltweit an [illegible]einrichtungen gelehrt und praktidere fühlt sich als Sieger, wenn a[illegible]chen Eliten verdummt zu haben. Die EU hat ihren Platz in der M[illegible]ng, Deregulierung, unbeschränkmehr das Beste aus zwei Welte[illegible]hr bis hin zur „marktkonformen Partei ergreifen und ein aktuelles Problem nach dem anderen bewältigen. Starke Konzepte scheint sie dafür nicht zu haben, jeder Mitgliedstaat versucht, den eigenen Nutzen auf Kosten der anderen zu maximieren.

Demokratie“ unserer Kanzlerin, trotz bröckelnder Infrastruktur, löcheriger Daseinsvorsorge und kastrierter Kontrolleure von wirtschaftlichen Aktivitäten. Diejenigen, die hoheitliche Aufgaben nicht schnell genug als überflüssig deklarieren konnten, kritisieren heute dreist das Versagen der Polizei, um sich für den Wahlkampf in Stellung zu bringen. Wie Christian Lindner (FDP), der anlässlich des Attentats in Berlin vom Dezember 2016 die Sicherheitsbehörden rügte, sie hätten bei der Rundum-Überwachung des Attentäters versagt.

Osteuropäische Länder, die nach der Umklammerung durch die UdSSR der EU und NATO beitraten, holen eine nationalistische Phase nach, die sie zwischen dem Großen Krieg und dem Fall des Eisernen Vorhangs übersprungen haben.

Ökonomisch beherrscht das Modell des bisherigen Siegers fast den gesamten globalen Norden nach dem Motto *There Is No*

Auch der technische Fortschritt ist dem marktliberalen Dogma untergeordnet. Das müsste nicht so sein, wenn es um anderes