Moritz Kütt und Alex Glaser

Retrocomputer für Abrüstungsverifikation und eine kernwaffenfreie Welt

Im Rahmen einer zukünftigen Abrüstung von Kernwaffen müssen Sprengköpfe vor ihrer Zerlegung als authentische Sprengköpfe bestätigt werden. Das erfordert vertrauenswürdige Messsysteme, die diese Identifikation anhand von radioaktiven Signaturen vornehmen können. Verschiedene solche Systeme existieren, bei allen ist jedoch die vertrauenswürdige Datenverarbeitung problematisch. Eine neuer Vorschlag für ein Messsystem basiert auf der Nutzung von Retrocomputern. Information Barrier eXperimental II *ist ein Prototyp eines solchen Systems zur Gammaspektroskopie auf Basis eines* Apple IIe *mit MOS 6502 Prozessor.*[1]

Kernwaffen sind wieder in aller Munde, und Experten schätzen das weltweite Risiko eines Einsatzes höher ein als in den letzten zwei Jahrzehnten – oder gar seit der Kubakrise vom Oktober 1962. Erst im Januar dieses Jahrs hat das renommierte *Bulletin of the Atomic Scientists* die *Doomsday Clock* auf zwei Minuten vor Mitternacht vorgestellt. Die Uhr beschreibt die Nähe der Welt zu einer globalen Katastrophe. Die neue Zeigerposition reflektiert die wachsende Bedrohung durch ein nuklear bewaffnetes Nordkorea, aber auch die öffentlichen Drohungen eines Kernwaffeneinsatzes durch US-Präsident Trump und die angespannten Beziehungen zwischen Russland und den USA.

Gleichzeitig zeigt die Doomsday Clock aber auch Versäumnisse der letzten Jahre auf. Es existieren immer noch rund 15 000 Kernwaffen im Besitz von neun Ländern. Die USA und Russland besitzen mit je rund 7000 Sprengköpfen den größten Anteil. Die Arsenale der anderen Staaten – Frankreich, Großbritannien, China, Israel, Pakistan, Indien und Nordkorea – sind deutlich kleiner. Es ist jedoch klar, dass auch ein sehr begrenzter Einsatz von Kernwaffen zu einer globalen Katastrophe führen würde, mit massiven klimatischen Auswirkungen durch den *Nuklearen Winter* und nie dagewesenen humanitären Konsequenzen sowohl für direkt betroffene Regionen als auch den Rest der Welt. Die komplette Abrüstung dieser Waffen ist nötig, vielleicht nötiger denn je.

Bestrebungen zur Rüstungskontrolle und Abrüstung gibt es prinzipiell seit dem Ende des Zweiten Weltkriegs, als die USA noch über ein Monopol über diese neuartigen Waffen verfügten. Das wichtigste Vertragswerk ist der nukleare Nichtverbreitungsvertrag (NVV), der 1970 in Kraft trat. Er verbietet die Entwicklung von Kernwaffen für Länder, die keine Kernwaffen besitzen (Nichtkernwaffenstaaten). Daneben definiert der Vertrag Kernwaffenstaaten, für die der Besitz von Kernwaffen weiterhin erlaubt bleibt (USA, Großbritannien, China, Frankreich, Russland). Kernwaffenstaaten verpflichten sich aber auch zur nuklearen Abrüstung, wenn auch ohne konkreten Zeitplan. Weitere Verträge sind der noch nicht in Kraft getretene Kernwaffenteststopp-Vertrag sowie bilaterale Vereinbarungen zwischen den USA und Russland.

In den ersten Jahren nach dem Ende des Kalten Kriegs gab es eine kurze Periode, in der weitreichende Fortschritte im Bereich der nuklearen Abrüstung möglich schienen. In diesen Jahren haben sowohl Russland als auch die USA Teile ihrer Kernwaffen-Arsenale abgerüstet und auch die Bestände an Waffenmaterialien reduziert. In der jüngeren Vergangenheit hat sich diese Entwicklung jedoch wieder eher umgekehrt. Nordkorea, Indien und Pakistan sind in den letzten 20 Jahren als neue Kernwaffenstaaten hinzugekommen. Aktuell rüstet insbesondere Nordkorea auf, indem es neben Sprengköpfen auch Tests von Langstreckenraketen durchführt, die diese Kernwaffen zu weit entfernten Zielen bringen könnten. Auch alle anderen Kernwaffenstaaten sind weit von ernsthaften Abrüstungsschritten entfernt; vielmehr modernisieren sie ihre aktuellen Arsenale, um sie für die nächsten Jahrzehnte bereit zu machen, und führen neue Waffengattungen ein.

Vor diesem Hintergrund gab es 2017 einen Lichtblick: Ein neuer internationaler Vertrag zum vollständigen Verbot von Kernwaffen *(Ban-Treaty)* ist erfolgreich verhandelt worden. Der Vertrag ist ein Versuch, eine existierende Regelungslücke zu füllen und Kernwaffen als letzte Kategorie von Massenvernichtungswaffen zu verbieten. Die Verhandlungen bauten auf Ergebnis-

Moritz Kütt und Alex Glaser

Alex und **Moritz** sind Friedensforscher und Aktivisten für eine Welt ohne Kernwaffen. Beide sind Physiker, und arbeiten am *Nuclear Futures Laboratory, http://nuclearfutures.princeton.edu* und dem *Program on Science and Global Security https://www.princeton.edu/sgs/* der Princeton University in den USA.

Ihre Forschung behandelt Verifikationstechnologien für Rüstungskontrolle und damit zusammenhängende politische Fragen. Aktuelle Projekte sind unter anderem: Nukleare Archäologie, Zero-Knowledge Protokolle, Virtual Proofs of Reality, Roboterinspektionen, Disco-Verifikation und Open Source Informationsbarrieren für Sprengkopf-Authentifizierung. Für viele der Projekte entwickeln sie eigene Software und Hardware, und nutzen Ideen aus der Maker-/Hacker-Szene.

sen von drei internationalen Konferenzen auf, bei denen die humanitären Konsequenzen des Einsatzes von Kernwaffen diskutiert wurden. Die Nichtregierungsorganisation *ICAN* (Internationale Kampagne zur Abrüstung von Kernwaffen) spielte bei den Konferenzen und den Vertragsverhandlungen eine wichtige Rolle. Ihre Arbeit des letzten Jahrzehnts wurde durch die Verleihung des Friedensnobelpreises an die Organisation im Dezember 2017 gewürdigt. Derzeit haben 56 Staaten den Verbotsvertrag unterzeichnet, 90 Tage nach der Ratifikation des Vertrags durch den fünfzigsten Staat wird der Vertrag in Kraft treten. Die Staaten, die Kernwaffen besitzen, sind den Vertragsverhandlungen erwartungsgemäß ferngeblieben. Auch fast alle NATO-Mitgliedsstaaten fehlten, Deutschland inklusive. Trotz grundsätzlicher Befürwortung von nuklearer Abrüstung sieht Deutschlands Politik aktuell weiterhin eine Rolle für Kernwaffen im Rahmen der NATO-Mitgliedschaft vor. Das zeigt sich unter anderem durch die Stationierung von 20 amerikanischen taktischen Nuklearwaffen auf einem Bundeswehrstützpunkt in Büchel, Rheinland-Pfalz. In der Vergangenheit forderten Politiker unterschiedlicher Parteien (etwa Guido Westerwelle als Außenminister oder Martin Schulz als Kanzlerkandidat) den Abzug dieser Waffen. Ein solcher Beschluss, möglicherweise verbunden mit dem Beitritt zum Kernwaffenverbotsvertrag, würde ein deutliches Zeichen setzen, und könnte auch den Beitritt einiger weiterer Staaten zum Verbotsvertrag einleiten.

Zentrale Komponente für weitere Schritte zur nuklearen Abrüstung ist die Verifikation der einzelnen Schritte. Durch solche Verifikationsmaßnahmen wird die Einhaltung der Verpflichtungen einzelner Staaten im Rahmen von internationalen Verträgen überprüft. Eine solche Überprüfung wird in der Regel durch andere Staaten oder internationale Organisationen vorgenommen, auch eine Überprüfung durch die allgemeine Bevölkerung ist vorstellbar *(Societal Verification).* Dabei gibt es verschiedene Herausforderungen. Es muss insbesondere sichergestellt werden, dass Staaten, auch solche ohne Kernwaffen, kein kernwaffenfähiges Spaltmaterial für militärische Zwecke erzeugen oder es aus dem zivilen Kernenergiesektor entnehmen. Abzurüstende Sprengköpfe müssen vor ihrer Zerlegung als wirkliche Sprengköpfe authentifiziert werden. Während und nach der eigentlichen Zerlegung muss eine lückenlose Kontrollkette gewährleistet werden, um Rückführungen von Sprengköpfen oder deren Bestandteilen in den militärischen Bereich zu vermeiden.

Sprengköpfe prüfen

Die von uns vorgestellte Technologie adressiert Probleme bei der Sprengkopf-Authentifizierung. Die Verfahren haben ein grundsätzliches Problem: Durch die Messungen werden Informationen enthüllt, die Kernwaffenstaaten als extrem sensitiv ansehen. Solche Messungen würden insbesondere das Design einer Kernwaffe preisgeben und ggf. auch auf mögliche *Schwachstellen* hinweisen. Zudem werden bei erweiterten Abrüstungsverträgen in Zukunft weitere Staaten Teil dieser Verifikationsbemühungen werden, im Rahmen des Ban-Treaty beispielsweise auch Staaten, die selbst keine Kernwaffen besitzen.

Kernwaffen lassen sich eigentlich vergleichsweise leicht anhand der von ihnen emittierten radioaktiven Strahlung identifizieren. Es gibt zwei unterschiedliche Verfahren: Beim *Attributverfahren* werden vor den Messungen gewisse Eigenschaften vereinbart, die dann durch die Messung ermittelt werden. Ein solches Attribut könnte beispielsweise die Anwesenheit von Plutonium sein; ein weiteres Attribut könnte eine festgelegte Untergrenze bestätigen, beispielsweise: Enthält das inspizierte Objekt mehr als zwei Kilogramm Plutonium? Beim *Template-Verfahren* findet die Identifizierung durch Vergleich statt. Ein Objekt wird als Muster bestimmt, alle anderen Objekte damit verglichen. Dabei ist wichtig, die Herkunft und Authentizität des Musters zuverlässig zu bestimmen, etwa durch zufällige Auswahl eines Sprengkopfs von stationierten Systemen durch Inspektoren.

Beide Ansätze werden typischerweise durch *Informationsbarrieren* ergänzt. Das sind Geräte, die komplexe Informationen verarbeiten und anschließend nur limitierte Informationen preisgeben. Eine solche, limitierte Information könnte etwa *Sprengkopf/Kein Sprengkopf* sein, häufig dargestellt durch grüne und rote LEDs. Die Analyse der komplexen Informationen erfolgt durch Datenverarbeitungssysteme. Wichtigste Voraussetzung für die Nutzung von Informationsbarrieren ist, dass beide Parteien Vertrauen in die Geräte haben. Die inspizierte Partei (Host) hat dabei ein Interesse daran sicherzustellen, dass keine sensitiven Informationen preisgegeben werden. Das könnte entweder absichtlich (etwa durch einen Nebenkanal) oder durch eine Fehlfunktion des Instruments geschehen. Die inspizierende Partei (Inspektor) fordert, dass die Informationsbarriere keinen Betrug zulässt und die angezeigten Ergebnisse die Realität korrekt wiedergeben. So könnte ein *Hidden Switch* nur dann aktiviert werden, wenn das Gerät unter bestimmten Bedingungen verwendet wird; überprüft der Inspektor das Gerät früher oder später an einem anderen Ort, würde es einwandfrei funktionieren.

Einige Gründe erschweren die Entwicklung von Informationsbarrieren: Es sind vorab wenige Informationen über das zu messende Objekt bekannt; der *Host* hat quasi unendliche Ressourcen, um einen Betrug zu vertuschen; und die Motivation zum Betrug ist hoch, denn bei Erfolg könnte der Host eigentlich abgerüstete Kernwaffen weiter besitzen. Ein weiteres Problem ist, dass nach bisherigem Stand die Hardware nach Messung an Kernwaffen beim Host verbleibt. Das schließt eine nachträgliche Überprüfung der Messelektronik durch Dritte aus.

Einige Prototyp-Informationsbarrieren wurden in den letzten Jahrzehnten entwickelt, die meisten als Forschungsarbeiten von US-amerikanischen Kernwaffenlabors. Teilweise wurden sie in Kooperation mit russischen Experten entwickelt und erprobt. Das erste und bisher einzige System, dass aus einer Kooperation eines Kernwaffenstaats und eines Nichtkernwaffenstaats hervorgegangen ist, wurde von Norwegen und Großbritannien im Rahmen der *UK-Norway Initiative* entwickelt. Die jeweiligen Entwicklungen unterscheiden sich, insbesondere bei verwendeten Mikroprozessoren und den angeschlossenen Detektoren. Trotz der zentralen Rolle solcher Geräte bei der Abrüstung gibt es jedoch bisher keine zufriedenstellenden Lösungen.

Wir schlagen daher ein alternatives Messsystem vor, das wir *Vintage Verification* nennen. Dabei werden alle informationsverarbeitenden Teile (wie Mikroprozessoren) durch alte oder *klassische* Hardware ersetzt (Retrocomputer). Alt in diesem Sinne ist Hardware aus den 70er und 80er Jahren, als der Einsatz von integrierten Schaltkreisen und Mikroprozessoren in

großem Umfang begann. Solche Hardware wäre deutlich vertrauenswürdiger als moderne Elektronik. Das hat vor allem zwei Gründe. Erstens ist solche Hardware tausendfach (oder gar millionenfach) weniger leistungsfähig. Die Implementierung betrügerischer Funktionen wird dadurch deutlich erschwert, da die Rechenleistung für solche Funktionen gar nicht zur Verfügung steht. Zweitens ist es sehr unwahrscheinlich, dass ein Mikroprozessor, der vor rund 40 Jahren gefertigt wurde, damals schon im Rahmen der Fertigung mit geheimen Betrugsfunktionen ausgestattet wurde, die speziell auf die heutige Anwendung der Abrüstungsverifikation abzielen.

Durch die Entwicklung der in Folge vorgestellten *Information Barrier eXperimental II (IBX II)* wollen wir zeigen, dass es möglich ist, mit Retrocomputern funktionsfähige Informationsbarrieren zu konstruieren. Unser Prototyp basiert auf einem Apple IIe sowie zwei neu entwickelten Erweiterungskarten (siehe Abbildung 1)[2]. Die IBX II kann zwei Objekte mit Hilfe des Template-Verfahrens als *identisch* oder *nicht identisch* klassifizieren. Wir nehmen dazu ein Gammaspektrum mit einem Sodium-Iodid-Szintillationskristall und zugehörigem Photomultiplier auf. Das ist seit vielen Jahrzehnten handelsübliche Hardware für solche Messungen. Die vergleichsweise niedrige Messauflösung kommt weiterhin dem Schutz sensitiver Informationen entgegen.

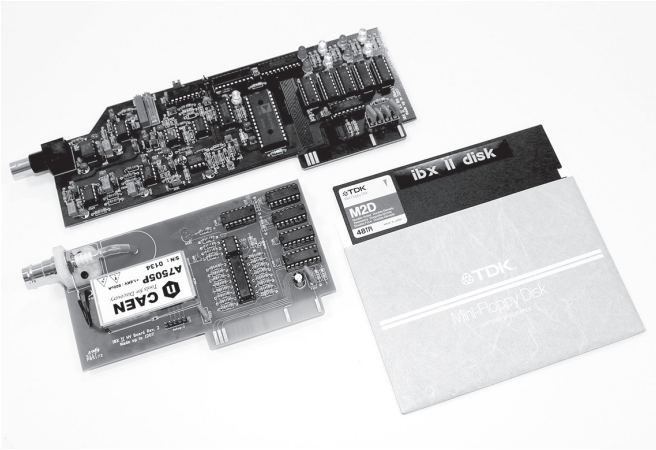

Abbildung 1: Apple IIe Erweiterungskarten und Software für IBX II, Foto A. Glaser

Die Datenverarbeitung der IBX II wird von einem Apple IIe durchgeführt. Dieser Heimcomputer, ursprünglich 1977 auf den Markt gebracht (zunächst in Version Apple II), wurde bis 1993 verkauft. Der Apple II kann als einer der *hackerfreundlichsten* Massencomputer seiner Zeit angesehen werden und war sicherlich das letzte *hackbare* Gerät aus dem Hause Apple. Im Rahmen des Designs kam es zu einem Streit zwischen den beiden Unternehmensgründern Steve Jobs und Steve Wozniak. Jobs wollte das System nur mit zwei Erweiterungssteckplätzen ausstatten. Wozniak dagegen plädierte für 8 Steckplätze, für möglichst viele von Nutzern gebaute Erweiterungskarten. Er konnte sich durchsetzen, und die Nutzergemeinde entwickelte tatsächlich viele Erweiterungskarten über Modem und Drucker hinaus – bis heute.

Herz des Apple IIe ist der MOS 6502 Mikroprozessor. Dieser 8-Bit Prozessor wurde 1975 vorgestellt, im Apple IIe läuft er mit 1 MHz. Der Prozessor war schon zu damaliger Zeit deutlich einfacher entworfen als andere Prozessoren (wie der Intel 8080 oder der Z80) und besitzt nur 3510 Transistoren. Trotz oder gerade wegen des einfachen Layouts und nur 56 Befehlen war er relativ leistungsfähig und robust. Der Prozessor wird bis heute produziert, und der aktuelle Hersteller Western Design Center schätzt, dass weltweit bis zu zehn Milliarden Einheiten dieses Chips produziert wurden. Der Prozessor ist heute quasi Open Hardware. Obwohl originale Designentwürfe nicht verfügbar sind, wurde die Struktur in mehreren Reverse Engineering Projekten ermittelt. Besonders hervorzuheben ist dabei die Arbeit von Visual 6502[3], die die elektrische Struktur durch hochauflösende Fotografien des Chips bestimmt haben. Monster 6502 hat ein funktionierendes Modell des Prozessors im Maßstab 7000:1 nachgebaut[4].

Die erste von uns für die IBX II entwickelte Erweiterungskarte versorgt den Photomultiplier mit der benötigten Hochspannung (1000 V). Sie basiert auf einer einfachen Digital-Analog-Konverter-Schaltung mit R2R-Netzwerk. Damit kann durch Software die Ausgangsspannung gesteuert werden, etwa um sie langsam von 0 auf 1000 V zu steigern bzw. am Ende wieder abzusenken und so das angeschlossene Gerät zu schonen.

Die zweite Karte *(ADC Karte)* dient der Datenaufbereitung und -digitalisierung und nutzt einen 12-Bit Analog-Digital-Konverter (ADC) des Typs AD1674 zur Digitalisierung. Ein Gammaspektrum zeigt die Häufigkeiten, mit denen Gammazerfälle bestimmter Energien gemessen werden (siehe Monitoranzeige in Abbildung 2). Einzelne Gammastrahlen, die im Szintillatorkristall detektiert werden, führen zum Aufbau von Ladung am Ausgang des Photomultipliers. Diese Ladung wird von der entwickelten Messkarte in einen Spannungspuls umgewandelt. Die Energie des Gammateilchens ist proportional zur Höhe dieses Pulses. Um daraus ein Gammaspektrum zu erzeugen, wird die Anzahl der Pulse in unterschiedlichen Energiebereichen (Kanälen) über eine gewisse Zeit gezählt. Der Datenaufbereitungsteil der ADC Karte verstärkt ankommende Pulse und verändert die zeitliche Form der Pulse, um eine bessere Digitalisierung zu ermöglichen. Eine *Peak-Detect-And-Hold*-Schaltung erkennt neue Pulse und gibt ein Signal an den Analog-Digital-Konverter, um einen Konvertierungsprozess zu starten. Während dieses Prozesses hält die Schaltung die Spannung am Eingang des ADC konstant auf der Höhe der Spitze des Pulses. Nach Abschluss der Konvertierung steht ein digitaler Wert am Ausgang

Abbildung 2: Mit Apple IIe aufgenommenes Gammaspektrum Foto A. Glaser

des ADC bereit und lässt sich durch Software auslesen. Software sortiert auch in die Kanäle.

Um die beiden Karten anzusteuern, nutzen wir ein 6502 Assembler-Programm. Eine Inspektion verläuft in vier Schritten: Zunächst wird die Hochspannung eingeschaltet, dann ein Gammaspektrum des Templates aufgenommen. Anschließend kann ein Gammaspektrum eines zu inspizierenden Objekts aufgenommen werden. Im letzten Schritt werden beide Spektren verglichen. Für diesen Vergleich werden die Daten der Spektren in je nur 12 Kanäle zusammengefasst. Die resultierenden Verteilungen werden dann mit einem Chi-Quadrat-Test verglichen. Ist das Resultat kleiner als ein Schwellwert, wird von einer hohen Ähnlichkeit ausgegangen, der Vergleich ist erfolgreich. Ansonsten ist er nicht erfolgreich. Das jeweilige Ergebnis wird entweder am Bildschirm oder über Leuchtdioden ausgegeben. Drei Faktoren beeinflussen die erzielbare Zählrate: Peak-Detect-and-Hold (dauert etwa 10–15 µs), Digitalisierung (10–15 µs) und Verarbeitung mit 6502 (35–50µs). Nach maximal 100 µs ist das Signal aufgenommen, vom 6502 verarbeitet und in den Speicher geschrieben. Theoretisch sind mit der IBX II also bis zu 10 000 Ereignisse pro Sekunde messbar. Typischerweise betreiben wir die IBX II in einem Bereich von 2000 Ereignissen pro Sekunde. Ein Spektrum kann in 1-2 Minuten aufgenommen werden.

Als Teil des Entwicklungsprozesses haben wir zu Testzwecken einen existierenden Apple II Emulator (LinApple) so erweitert, dass er auch die Funktion der beiden Erweiterungskarten enthält. Damit konnten Programmentwicklung und -tests an einem modernen Rechner durchgeführt werden. Interessierte, die unsere Arbeit testen wollen, aber nicht über die notwendige Hardware verfügen, bietet der Emulator einen guten Startpunkt (siehe Endnote 2).

Durch Entwicklung und Test der beiden Erweiterungskarten konnten wir zeigen, dass die Idee, alte Hardware zu benutzen, grundsätzlich funktionieren kann. Bisher noch als Erweiterungskarten im selbst relativ komplexen Apple IIe lässt sich ein ähnliches Design in Zukunft auch auf ein einfacheres 6502-basiertes System anpassen. So ist eine Informationsbarriere vorstellbar, die neben der Hardware der Erweiterungskarten nur einen 6502, etwas ROM für die Software und ausreichend RAM für das Template enthält. Weitere Schritte in Zukunft sind eine Optimierung des Assembler-Programms, aber auch der entwickelten Hardware. Gleichzeitig sollte versucht werden, möglichst verschiedene Wege zu finden, mit denen Alter bzw. Authentizität des verwendeten Mikroprozessors nachgewiesen werden können. Dafür sind nicht-destruktive Methoden, etwa Röntgenmikroskopie, und destruktive Methoden vorstellbar. Gerne nehmen wir Ideen und Hinweise von anderen auf. Auch wenn noch einige Schritte zu tun sind, hoffen wir, dass unser hier vorgestelltes Projekt ein kleiner Beitrag auf dem Weg zu einer kernwaffenfreien Welt ist.

Anmerkungen

1 *Inhalte dieses Artikels wurden auf dem 34c3 vorgetragen.*
2 *Software, Hardware Design und modifizierter Emulator verfügbar unter www.vintageverification.org*
3 *visual6502.org*
4 *monster6502.com*

FIfF e. V. – Pressemitteilung

FIfF-Sachverständigenauskunft zum Trojanereinsatz durch den hessischen Verfassungsschutz

FIfF lehnt Hessentrojaner ab

7. Februar 2018 – Am 8. February 2018 findet eine öffentliche mündliche Anhörung des hessischen Innenausschusses zum Gesetzentwurf der Fraktionen von CDU [illegible] des Verfassungsschutzes in Hessen (HVSG) statt. Weil dem hessische[illegible]nsatz von Trojanern in Form von verdeckter Quellen-TKÜ und geh[illegible]achverständiger eingeladen worden. Wir empfehlen dringend, di[illegible] zu streichen.

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

Einleitung

Geheimdienste, also staatliche Behörden, die wesentlich auf verdeckte Maßnahmen, Tarnoperationen, „Vertrauensleute“ oder verdeckte MitarbeiterInnen setzen, sind inhärent auf Intransparenz angelegt und angewiesen, da Heimlichkeit das primäre Mittel ist, die ihnen übertragenen Aufgaben auszufüllen. Ermächtigungen derartiger Dienste müssen folglich besonders kritisch analysiert werden, da einmal freigegebene Maßnahmen und ermöglichte Methoden meist nur nach Skandalen erneut zur breiten Diskussion gestellt werden (können).

Auch wenn sich die Aufgabenbereiche von Polizeien und Geheimdiensten mittlerweile gefährlich überlappen, sind dennoch die Berichts- und Transparenzpflichten von polizeilichen Behörden – im Gegensatz zu verdeckt tätigen Organisationen – zumindest grundsätzlich auf Offenheit angelegt. Wegen dieses gewichtigen Unterschieds gehen die rechtfertigenden Referenzen des Gesetzentwurfs bezüglich der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz natürlich prinzipiell fehl. **Ein Geheimdienst ist keine Polizei und eine Polizei ist kein Geheimdienst.**