Chaos Computer Club Schweiz CCC-CH
Birsfelderstrasse 6
4132 Muttenz
E-Mail: vorstand@ccc-ch.ch
URL: https://www.ccc-ch.ch/

Chaos Computer Club Schweiz CCC-CH, Birsfelderstrasse 6, 4132 Muttenz

Nachrichtendienst des Bundes NDB
Andrea Schär
Papiermühlestrasse 20
3000 Bern
E-Mail: Andrea.Schaer@ndb.admin.ch

16. April 2017

Vernehmlassungsantwort zum Ausführungsrecht in Sachen Geheimdienstgesetz NDG: E-NDV und E-VIS-NDB

Liebe Damen
Liebe Herren

Der Chaos Computer Club Schweiz (kurz: CCC-CH) ist Teil der intergalaktischen Gemeinschaft von Lebewesen, die sich vertieft mit Computertechnik und ihren gesellschaftlichen Implikationen (Technikfolgenabschätzung) befassen.

Uns schliessen sich Menschen an, die kompromisslos freiheitsliebend sind und auch weiterhin in einer freiheitlichen Gesellschaft leben möchten. Anders als in den frühen 1980er Jahren, in welchen die Ursprünge des Chaos Computer Clubs (zumal in Deutschland) liegen, umfasst die Digitalisierung mittlerweile alle Lebensbereiche: ob Smart-TV, Videobrille, Kühlschrank, Wasserkocher, Kinderpuppen, Handy oder PC – immer mehr Geräte werden bewusst oder unbewusst ans Internet angehängt. Jedes dieser Geräte stellt eine mögliche Datenquelle dar, die der NDB oder ausländische "Partnerdienste"[1] anzapfen können. Dies wissen Bundesrat und NDB sehr genau: das NDG muss in diesem Kontext als ein Macht- und Herrschaftsinstrument verstanden werden, was es dem Bund

[1] Tatsächlich werden wir von unseren sogenannten Freunden schamlos ausgespäht, wie dies z. B. für den deutschen Auslandsgeheimdienst BND gegenüber der Schweiz belegt ist.

erlaubt bis in tiefste Winkel unserer Intimsphäre, die selbst Gedankenwelten[2] umfassen können, einzubrechen. Die Bevölkerung hat sich von den diffusen Terrorängsten leiten lassen und den Vorwänden von Bundesrat und den unterstützenden Parteien geglaubt, das NDG sei die probate Antwort auf islamistischen und anderen Terror. Was heute der islamistische Terror ist, waren gestern noch Schweizer Anarchisten und Kommunisten: es kann schnell gehen und plötzlich ist die Bevölkerung wieder der eigentliche Feind, insbesondere falls grössere Gegenöffentlichkeiten sich bilden sollten, welche die Macht der etablierten Politik gefährden sollten. Es ist zudem aus der Praxis der "Partnerdienste" hinreichend bekannt, dass Masssenüberwachung allen voran diplomatischen und wirtschaftlichen Zielen dient, doch dient sie auch dazu soziale Bewegungen auszuleuchten, um dem eigenen Land jeweils Vorteile in politischer und wirtschaftlicher Hinsicht zu verschaffen sowie die politische als auch wirtschaftliche Macht zu sichern. Der Bundesrat und die unterstützenden Parteien haben diese Tatsache bewusst nicht an die grosse Glocke gehängt, weil damit das Narrativ des NDG als Instrument der Terrorbekämpfung gefährdet wäre.

Der CCC-CH lehnt das Geheimdienstgesetz NDG, einschliesslich aller darauf aufbauender Verordnungen, als Ganzes ab und wird sich an jedweder Kampagne beteiligen, die dazu beiträgt, die Schweizerische Eidgenossenschaft als das darzustellen, was sie nun zweifelsohne wird: ein Land, wo Menschenrechte massenweise mit Füssen getreten werden. Die Weltöffentlichkeit soll erfahren, dass sich die Schweiz von ihren freiheitlichen Prinzipien verabschiedet hat und sich ebenfalls aus der totalitären Trickkiste bedient, die dazu geeignet ist, die Bevölkerung jederzeit – vom Zeitgeist abhängig – zu entmachten.

Wir beteiligen uns dennoch an der Vernehmlassung, um die bevorstehenden Gefahren darzulegen und in gewissen Punkten Technikfolgenabschätzung zu betreiben, was angesichts der Erfahrungen aus dem – gerade näheren – Ausland gut gelingen kann. Der deutsche Bundesnachrichtendienst (BND) ist schliesslich seit Jahrzehnten im Bereich der "Strategischen Aufklärung" aktiv – jüngst wurde im Rahmen des Untersuchungsausschusses zur NSA-Überwachung in Deutschland (NSAUA), der auch zu einem BND-Untersuchungsausschuss mutierte, bekannt, dass der BND massenweise deutsches Recht verletzt und ausländischen Bürgern im digitalen Raum überhaupt keine Menschenrechte einräumt; ein Weg, den die Schweiz unbeirrt nun auch beschreitet. In technologischer Hinsicht dürfte sich die Schweiz aus sehr ähnlichen (bis gleichen) Trickkisten und Methoden bedienen, um ihre Überwachungspraxis auszuüben und insbesondere auch zu koordinieren. Gerade beim "Terrorkampf" wäre es absurd anzunehmen, dass die Schweiz völlig anders nach Terroristen trachtete als Deutschland oder die USA. Entspechend wird die Schweiz weder frei von Skandalen bleiben, noch strukturell weniger Grundrechte verletzen als dies ihre "Partnerdienste" tun. Die Schweiz wird fortan wie alle Länder, die sich extensiv aus totalitären Trickkisten bedienen, Menschenrechte grob missachten – ein Skandal für sich.

[2] Z. B. im Falle der Verwanzung eines Handys, wo selbst Nachrichten und Dokumente im Entwurfsstadium einsehbar sind.

Zur Kritik & und Technikfolgenabschätzung der E-NDV

Art. 1: Zusammenarbeit des NDB mit inländischen Stellen und Personen

Dieser Artikel erlaubt es dem NDB mit *Privatpersonen* als auch *Unternehmen* zusammenzuarbeiten, womit sich abzeichnet, dass der NDB Teile des Spitzelapparats an Private auslagert, deren Aktivitäten sich nicht kontrollieren lassen und die ihre ganz eigenen privaten Datensammlungen unterhalten – ob offiziell oder inoffiziell. Aus freiheitlich-demokratischer Sicht ist damit der Vorteil verbunden, dass die Machenschaften des NDB mit erhöhter Wahrscheinlichkeit an die Öffentlichkeit kommen – wie beispielsweise beim Hacking-Team-Skandal, wo bekannt wurde, dass die Kantonspolizei Zürich CHF 500'000 Steuergelder in italienische Mafia-Strukturen investiert hatte, die sich wiederum auf osteuropäischen Mafia-Märkten trieben, um dort öffentlich unbekannten Sicherheitslücken (sogenannte Zero-Day-Exploits) einzukaufen.

Art. 3: Zusammenarbeit des NDB mit dem Nachrichtendienst der Armee

Was konsequent während dem Abstimmungskampf unter den Tisch gekehrt wurde, wird mit der NDV nun sichtbar: der NDB kann mit dem Nachrichtendienst der Armee (NDA) gemeinsam Informationen beschaffen (Abs. 2 Bst. b), sowie die internationale Zusammenarbeit *[a]bstimmen*. Damit wird ein militärisch-industrieller Komplex begründet, der sich mit dem Ausland vernetzt und weltweit Fangnetze ausbreitet, Massenüberwachung zu betreiben. Die vermeintlich zivile Natur des NDB wird damit direkt eingangs untergraben.

Art. 5: Zusammenarbeit des NDB mit fedpol

Der Artikel legt fest, dass polizeiliche und geheimdienstliche Arbeit verwischt wird, was erstens präventive und repressive Aufgaben des Bundes verwischt und zweitens den Weg ebnet für einen präventiven Sicherheits- oder in der Schweiz – Fichenstaat. Absichtlich verpasst es der Bundesrat von der Vergangenheit zu lernen: er profitiert von der diffusen Terrorangst in der Bevölkerung und nutzt dies schamlos aus, um den neuen – viel mächtigeren – Fichenstaat mit normativen Grundlagen im Detail niederzuschreiben.

Art. 7: Jährliche Festlegung der Grundsätze der Zusammenarbeit

Der Bundesrat unterlässt es, festzulegen, dass die Schweiz mit Geheimdiensten menschenverachtender Regime keine Kontakte pflegen sollte – wie dies damals im Rahmen des Strategischen Nachrichtendienstes (SND) unter Führung von Peter Regli geschah, das mit dem südafrikanischen Apartheid-Regime paktierte.

Ferner schliesst Abs. 4 nicht aus, dass die Schweiz *im Einzelfall* auch mit genau jenen Diensten zusammenarbeiten kann, mit denen nach Aussagen von sowohl Bundesrat

als auch NDB keine "direkten" Kontakte bestehen und die jüngst im Fokus der Öffentlichkeit waren, namentlich *Dienststellen* von CIA, NSA und anderer alltagspraktisch vollends entfesselter Dienste, die nach allen Regeln der Kunst die gesamte Menschheit ausspähen und die auch eine wesentliche Rolle darin spielen, Menschen ohne Gerichtsprozess zu ermorden – etwa im Rahmen von feigen Drohnenmorden aus der Luft.

Es ist eine Schande, dass der Bundesrat gedenkt den NDB ohne jedweden moralischen Kompass zu belassen, so sich dieser auf Kontakte *im Einzelfall* berufen kann, was ihm bereits ermöglicht, an abscheulichen Taten teilzunehmen oder davon zumindest Kenntnis zu erlangen.

Art. 9: Arten der Zusammenarbeit

In diesem Artikel zeichnet sich ab, dass der NDB in einem transnationalen Verbund mit anderen Geheimdiensten zusammenspannen wird, um mitzuhelfen, die Weltbevölkerung auszuspähen: der NDB steigert damit seinen Marktwert und wird einerseits zu einer gefragten Anlaufstelle für ausländische Dienste, wo er seine Datenbeute gegen andere Personenfichen oder Geld austauschen kann, andererseits aber auch zu einem beliebten Angriffsziel, da er durch das NDG und den vorliegenden Verordnungen erstmals seit der Fichenaffäre vom eher zurückgebundenen Geheimdienst ohne vielen Möglichkeiten, legal im Leben von Menschen zu schnüffeln, zu einem offensiv angelegten Geheimdienst mutiert, in dem Grundrechtsverletzungen zur Norm werden: insbesondere haben Menschen im Ausland unter den Bedingungen des NDG überhaupt keinen Anspruch auf Privatsphäre.

Art. 10: Internationale Vereinbarungen von beschränkter Tragweite

Dieser Artikel wird es dem NDB z. B. erlauben die Ausspähung von Glasfaser- oder Kupferleitungen mit anderen Geheimdiensten – wie dem deutschen BND – zu organisieren. Ob der Bundesrat die sogenannte *beschränkte Tragweite* einzuschätzen vermag, ist mehr als fraglich. Es ist ferner denkbar, dass der NDB unter dem Deckmantel der *beschränkten Tragweite* mit anderen Geheimdiensten einen Ring von Zero-Day-Exploits betreibt, um in fremde Computersysteme einzudringen. Auch das sind Tatsachen, in denen dem Bundesrat in aller Regel jegliches Einschätzungsvermögen abzusprechen ist.

Art. 13: Zusammenarbeit und Beauftragung in der Beschaffung mit oder von inländischen Amtsstellen

Dieser Artikel schafft Misstrauen im Land: der NDB kann jederzeit Amtsregister abfragen – notabene auch von kleineren Gemeinden; diese aber können ihren (wohlbekannten) Bürgern keine Auskunft geben, dass Daten von ihnen an den NDB weitergegeben wurden. Zudem ist es Polizeien dadurch möglich auf die so beschafften Daten (über die Datensammlungen des NDB) zuzugreifen, ohne selber den Weg zur Gemeinde zu finden, was im Rahmen eines Strafverfahrens immerhin ein dokumentierter Vorgang wäre, der

dem Beschuldigten zuletzt bekannt würde. Dass ein Verdächtiger Einsicht in Daten des NDB erhält ist umgekehrt praktisch ausgeschlossen.

Art. 16: Zusammenarbeit und Beauftragung in der Beschaffung mit oder von ausländischen Amtsstellen oder von Privaten im Ausland

Es fällt auf, dass (anders als in Art. 15 E-NDV) keine Protokollierung über die Zusammenarbeit mit ausländischen Amtsstellen oder Privaten im Ausland zu erfolgen hat, was diskriminierend ist und gleichzeitig bedeutet, dass der NDB wenn immer möglich vorzugsweise mit ausländischen Privaten zusammenarbeiten wird, was seine Aktivitäten noch diffuser machen.

Art. 18: Quellenschutz

Dieser Artikel dient bestenfalls der Beruhigung: auf Grund der Instrumente der Massenüberwachung, die dem NDB zur Verfügung stehen, ist der Quellenschutz – zumal im digitalen Raum – auf normativer Ebene in der Schweiz faktisch aufgehoben.

Art. 20: Durchsuchen von Räumlichkeiten, Fahrzeugen und Behältnissen

Es ist ein Skandal, dass der NDB – anders wie die Polizei – ohne Strafverfahren in z. B. Wohnungen einbrechen und in Fahrzeugen rumfuhrwerken kann. Damit werden Praxen der Fichenaffäre wieder restauriert.

Art. 22: Schutz von Berufsgeheimnissen

Dieser Artikel gilt analog zu Art. 18 E-NDV und insbesondere angesichts der Anhänge E-VIS-NDB als Platzhalter, um den Schein von Rechtsstaatlichkeit zu wahren.

Art. 23: Eindringen in Computersysteme und -netzwerke im Ausland

Falls der NDB es wagen sollte, sich in "Cyberwar" zu üben, wird das sehr ruinös werden: es ist nicht damit zu rechnen, dass die Schweiz den Hauch einer Chance hat, sich gegen existierende Heerschaaren ausländischer (und staatlich finanzierter) Büchsenöffner zu wehren. Zudem hat die Schweiz bei den meisten ihrer Systeme weder die Kontrolle über Hard- noch Software. Die Hardware ist meistens chinesischer, die Software in aller Regel US-amerikanischer Herkunft. Ein möglicher "Vergeltungsschlag" der Schweiz gegenüer einem anderen Land könnte in ihren Folgen (wegen mangelnden Wissensvorsprüngen und Unwissen über existierende Hintertüren) rasch zum nationalen Gejammer verkommen.

Art. 24: Zweck der Kabelaufklärung

Die wesentliche Kritik und Ablehnung sowohl der Funk- als auch Kabelaufklärung er-

folgt bereits im Rahmen der Kritik an Anhang 13 E-VIS-NDB.

Art. 25: Durchführender Dienst

Wie schon im Abstimmungskampf ständig von uns betont, ist es mit dem Zentrum für Elektronische Operationen (ZEO) das Schweizer Militär und nicht der NDB, der in erster Linie dafür missbraucht wird, die Bevölkerungen im In- und Ausland massenhaft auszuspähen: der NDB kriegt "nur" die Ergebnisse der ZEO-Massenüberwachung. Damit wird mithin nichts Geringeres gemacht als das Schweizer Militär gegen die eigene Bevölkerung zu richten: es ist uns nicht gelungen diesen Umstand der Schweizer Stimmbevölkerung während dem Abstimmungskampf zu vermitteln. Dies ist anders als in Deutschland, wo mit dem BND zwar eine militärnahe Institution die Massenüberwachung ausübt, es allerdings nicht geradewegs die Bundeswehr ist, die dies tut. Die Schweiz geht hiermit einen sehr denkwürdigen Weg, wo eigentlich zu erwarten wäre, dass sich von links bis rechts Widerstand regt.

Art. 26: Aufgaben des ZEO

Insbesondere Abs. 4 ist eine sehr interessante Art, jedwede Kontrolle komplett auszuschalten: durch die Nutzung zusätzlicher, etwa dem Bundesverwaltungsgericht nicht bekannter Suchbegriffe (auch: Selektoren), können ganz neue Ergebnisse erzeugt werden – an jeder Kontrolle vorbei.

Art. 27: Datenbearbeitung

Die Kabelaufklärung wird offenkundig – genauso wie die bereits existierende Funkaufklärung – dafür genutzt werden, eine Vorratsdatenspeicherung von 18 Monaten für Inhalts- und von fünf Jahren für Kontakt- und Bewegungsdaten anzulegen. Das ist ein skandalöser Vorgang, weil schon beim Überwachungsgesetz BÜPF die 12 Monate Vorratsdatenspeicherung im Metadatenbereich zuviel schienen. Hier nun sollen sogar zwei Formen von Vorratsdaten angelegt werden, die vom Parlament weder behandelt wurden noch im Abstimmungskampf je Thema waren; vorauszusehen aber war diese Entwicklung, weil schon für die Funkaufklärung (gem. VEKF) genau die gleichen Fristen (heute) gelten – nicht minder fragwürdig.

Art. 28: Aufgaben der Betreiberinnen von leitungsgebundenen Netzen und der Anbieterinnen von Telekommunikationsdienstleistungen

Dieser Artikel konstituiert das Schweizer "PRISM"- und "Tempora"-Programm, wobei Daten entweder von Zugangsprovidern abgefangen werden oder direkt von Anbietern von Telekommunikationsdiensten ausgeleitet werden: in beiden Fällen werden die (privatwirtschaftlichen) Akteure verwanzt – und zwar mit dem ZEO von einer Stelle des Schweizer Militärs. Das ist ein sowohl ordnungspolitisch als auch rechtsstaatlich höchst fragwürdiger Vorgang.

Art. 31: Bekanntgabe von Personendaten an inländische Behörden

Die Kritik ist der Kritik von Anhang 3 E-NDV zu entnehmen.

Art. 32: Bekanntgabe von Personendaten durch kantonale Vollzugsbehörden

Dieser Artikel ist äusserst kritisch, da nie klar ist, ob die Verdachtsgrundlagen, die der NDB über Personen speichert, substantiert sind. Es können damit Personen in den Fokus staatlicher Zwangsmassnahmen geraten, denen zuletzt keine Straftat nachgewiesen werden kann. Ein Beispiel in der Schweiz, wo auf teils falschen Informationen des damaligen Inlandsgeheimdienstes Dienst für Analyse und Prävention (DAP) gesetzt wurde, ist der Fall des sogenannten "Rütli-Bombers": die betreffende Person hat in der Folge Arbeit und Familie verloren.

Art. 33: Bekanntgabe von Informationen an Strafverfolgungsbehörden

Es gilt die Kritik von Art. 32 E-NDV: spezifisch im Zusammenhang mit Strafverfolgungsbehörden ist zusätzlich die Gefahr inhärent, dass die Polizei auf gefälschten Beweisgrundlagen arbeitet. Schliesslich hat der NDB die Möglichkeit Computer von Verdächtigen anzugreifen und dort auch Daten zu manipulieren: dies kann absichtlich, versehentlich (technisch bedingt) als auch durch unabhängige Dritte geschehen, weil das verwanzte Gerät des Betroffenen auch für solche (zusätzlich) angreifbar werden kann. Staatstrojaner können Sicherheitsfunktionen von Geräten abschalten, so dass diese schlechter geschützt für weitergehende Angriffe sein mögen (z. B. Anti-Virensoftware oder persönliche Firewalls).

Art. 34: Bekanntgabe von Personendaten an ausländische Behörden

Es ist als kritisch zu erachten, wenn der NDB mit ausländischen Strafverfolgungsbehörden oder anderen Stellen arbeitet, ohne über gesicherte Beweise oder über einen dringenden Tatverdacht zu verfügen: analog zur Kritik an Art. 32 E-NDV kann dies das Leben von Menschen ruinieren.

Art. 35: Ausnahme vom Öffentlichkeitsprinzip

Die Ausnahme vom Transparenzgrundsatz staatlichen Handelns ist ein grosser Fehler, da die Bevölkerung damit direkt auf Whistleblowing oder Datenlecks angewiesen ist, um über das wahre Ausmass des Handelns vom NDB Kenntnisse zu erlangen.

Art. 37: Wahrung weiterer wichtiger Landesinteressen

Der juristisch schwammige Begriff der *weitere[n] wichtige[n] Landesinteressen* konstituiert die diplomatische und wirtschaftliche Spionage, für die im Abstimmungskampf von

der Befürworterseite kaum bis nicht informiert wurde. Solche Praxen können die Beziehungen zum Ausland schwer beeinträchtigen, wie dies im Zuge der Snowden-Enthüllungen vorgeführt wurde. Es wäre wünschenswert gewesen, der Gesetzgeber hätte sich auf den Schutz der hiesigen (kritischen) Infrastrukturen fokussiert, anstatt sich dem ruinösen Wettbewerb hinzubegeben, ausländische Systeme auszuschöpfen.

Art. 53: Berechtigung zum Tragen einer Dienstwaffe

Es ist – obwohl im Gesetz vorgesehen – nach wie vor nicht ersichtlich, wieso der NDB selber über Waffen verfügen soll. Sind NDB-Agenten an Leib und Leben bedroht, sollte die ohnehin vorhandene Zusammenarbeit mit den kantonalen oder anderen polizeilichen (Bundes-)Stellen gesucht werden.

Art. 57a: Übergangsbestimmung zur Archivierung

Es ist schamlos, dass bereits vorhandene Daten um weitere 30 Jahre in ihrer Schutzfrist aufbewahrt werden sollen, um möglicherweise weitergehend in der Vergangenheit zurückliegende grobe Fehler der NDB-Vorgängerdienste DAP und SND zu decken.

Art. 58: Inkrafttreten

Wünschenswert wäre, die Verordnung würde restlos gestrichen und gar nie in Kraft treten.

Anhang 1: Auskunftspflichtige Organisationen

Es ist besorgniserregend wie viele Organisationen, die über erhebliche Datenmengen und -quellen verfügen, verpflichtet werden, mit dem NDB zusammenzuarbeiten. Gerade die SBB sind bekanntlich Betreiber eines grossen Netzes von Videoüberwachungsanlagen, auf die der NDB Zugriff nehmen kann; zudem verfügen die SBB zunehmend über Bewegungsprofile der Zugreisenden, die es dem NDB erlauben, weitergehende Bewegungsprofile von Menschen zu erstellen.

Anhang 3: Bekanntgabe von Personendaten an inländische Behörden und Amtsstellen

Die Funktion des NDB als Datenstaubsauger und -drehscheibe der Nation wird in diesem Anhang sehr deutlich: der NDB selber wird verpflichtet, zahlreiche inländische Stellen bei der Vervollständigung ihrer ganz eigenen Datenbestände mit Personendaten zu unterstützen. Dass die meisten der Empfängerstellen mit Terrorbekämpfung nichts am Hut haben – was bekanntlich das Narrativ des Abstimmungskampfes war – ist offensichtlich.

Anhang 4, Punkt 2: Verordnung vom 27. Juni 2001 über das Sicherheitswesen in Bundesverantwortung

Wenn Private für Gebäudesicherheit eingesetzt werden können, ist nicht ausgeschlossen, dass Datenbestände mit besonders schützenswerten Personendaten auf physischen Wegen die Räumlichkeiten des NDB verlassen, respektive Infrastruktur des NDB elektronisch verwanzt wird: in freiheitlich-demokratischer Hinsicht kann dies dazu führen, dass die Machenschaften im NDB bekannt werden; auf der anderen Seite – je nach Intention des Angreifers – können aber auch Personen massenweise (durch Veröffentlichung) ihrer Privatsphäre beraubt werden. Gerade angesichts der Tatsache, dass der Bundesrat plant, dem NDB auch die zentrale Verwaltung hochdiskriminierender Daten, wie Medizindaten, anzuvertrauen (gemäss E-VIS-NDB in den Anhängen), kann dies das Leben vieler Menschen sehr negativ beeinträchtigen.

Anhang 4, Punkt 6: Verordnung vom 15. Oktober 2008 über das Informationssystem der Bundeskriminalpolizei

Hierfür gelten die Kritiken von Art. 32 und 33 E-NDV im weitesten Sinne.

Anhang 4, Punkt 7: Verordnung vom 26. Oktober 2016 über das automatisierte Polizeifahndungssystem

Es gilt hier die Kritik von Art. 32 E-NDV sinngemäss: Fahrzeuge auf vagen Verdachtsgrundlagen auszuschreiben, ist kein Weg, der besonders zielführend scheint.

Anhang 4, Punkt 8: Verordnung vom 8. März 2013 33 über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro

Es gilt die Kritik von Anhang 4, Punkt 7 E-VIS-NDB sinngemäss.

Anhang 4, Punkt 9: Verordnung vom 17. Oktober 2012 35 über die elektronische Kriegführung und die Funkaufklärung

Es ist masslos und technisch nicht nachvollziehbar, wie Funkaufklärung dabei helfen soll, Cyber-Angriffe abzuwehren.

Anhang 4, Punkt 10: Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs

Diese Änderung erlaubt es dem NDB auf die Überwachungsmittel und Datenbestände des Dienst ÜPF zuzugreifen, welcher dieser im Rahmen des Überwachungsgesetzes BÜPF hat. Dieses Gesetz wird gegenwärtig seinerseits nach einer Totalrevision bald in massiv verschärfter Form in Kraft gesetzt und erweitert die systematische Speicherung aller Kontakt- und Bewegungsdaten der Schweizer Bevölkerung auf zusätzliche Anbieter, von Zugangsprovidern bis hin zu privaten und gewerblichen Anbietern von WLAN-Access-Points.

Im Abstimmungskampf zum NDG wurde dies mit keiner Silbe erwähnt: der NDB erhält dadurch Zugriff auf alle Datenbestände vom Dienst ÜPF, was ihm erlaubt, seine minutiösen Personenfichen (gem. den Anhängen in E-VIS-NDB) zu vervollständigen.

Anhang 4, Punkt 12: Verordnung vom 9. März 2007 über Frequenzmanagement und Funkkonzessionen

Es ist nach wie vor und im Sinne der Netzneutralität davor zu warnen, den Staat als Störfriede normativ festzulegen.

Zur Kritik & Technikfolgenabschätzung mit der E-VIS-NDB

Art. 1: Gegenstand

Nicht nur ist erschreckend, dass in umfassendem und strukturiertem Masse (wie im Anhang später offenkundig wird) Personenfichen angelegt werden sollen, sondern dass sogar für Fälle, wofür es noch keine spezifische Kategorie gibt, nach der Menschen und Organisationen eingeteilt werden, nun tatsächlich noch der *Restdatenspeicher* nach Art. 57 NDG eingeführt wird. Damit unterstreicht der Bundesrat, dass er sich für die Zukunft noch einige Überraschungen offenhält, wen er sonst noch alles der systematischen Fichierung zuführen will.

Art. 3: Ablage von Daten

Bezeichnend ist die spezifische Bemerkung, wonach auch Dokumente, welche nicht unmittelbar textuell erfasst werden können mittels Optical Character Recognition (*OCR*) durchsuchbar gemacht werden sollen. Eingeübt ist diese Praxis schon länger, wie aus dem GPDel-Bericht von 2003 zur Onyx-Funk-Massenüberwachung hervorgeht. Neu wird hiermit klar, dass grundsätzlich keine Dokumente, die auch durch Glasfaser- oder Kupferleitungen fliessen von den Augen des NDB verschont bleiben werden. Im Übrigen können auch Bild- und Videodokumente mit Verfahren der Muster- und Texterkennung durchsucht werden, wobei durch textuelle Transkription der darin enthalten linguistischen Informationen in jedem Fall die Freitextsuche ermöglicht wird. Ein insgesamt fürwahr totalitärer Schachzug.

Art. 6: Systemübergreifender Zugriff und temporäre Auswertung

Nach Abs. 1 soll es Benutzer geben, die auf *alle Informationssystem des NDB gleichzeitig zugreifen* können sollen, was zumindest und für einmal in positiver Hinsicht – und je nach moralischem Kompass der Mitarbeitenden – das Potenzial birgt, dass Informationen über Machenschaften des NDB einfacher an die Öffentlichkeit gelangen.

Art. 7: Operationsbezogene Daten

Abs. 6 könnte makaberer kaum sein: Daten sollen *bis zum Tode der erfassten Person, jedoch höchstens 45 Jahre aufbewahrt* werden können, und das dann auch noch auf Datenträger, die ausserhalb jedweden Kontrollbereichs liegen, da es sich bei den *operationsbezogenen Daten* um Daten handelt, die einem nur vereinzelten Personenkreis (Abs. 3) zur Verfügung steht.

Art. 8: Löschen von Daten

Dieser Artikel sieht eine weitere Vorratsdatenspeicherung von (bis zu) drei Monaten beim NDB vor.

Art. 11: Qualitätssicherung

Es ist absurd, dass die *Rechtmässigkeit*, *Zweckmässigkeit*, *Wirksamkeit* und *Richtigkeit* der beim NDB gespeicherten Daten nicht kontinuierlich, sondern nur in jährlichen Abständen geprüft werden sollen und dazu dann noch nur *stichprobenweise*. Die Befürworter der NDG-Vorlage haben schliesslich immerzu beteuert, dass der NDB nur in sehr wenigen Fällen überhaupt (invasiv) überwachen wird. Würden die im Abstimmungskampf genannten Fallzahlen von 10-25 auch nur ansatzweise stimmen, wäre eine Kontrolle auf kontinuierlicher und ständiger Basis sehr einfach und kostengünstig möglich. Dass dem offenbar nicht Rechnung getragen wird, zeigt auf, dass der Abstimmungskampf mit regelrechten "Fake-News" gewonnen wurde. Alleine im Zuge der *Kabelaufklärung* werden von allen Schweizer Bürgern früher oder später Treffer erfolgen, die in den Datenbanken des NDB landen: die Millionen von Personenfichen, die zuletzt tatsächlich entstehen, sollen entsprechend nur *stichprobenweise* und entsprechend *jährlich* überprüft werden. Dieser und weitere (spätere) Artikel, die sich mit der Kontrolle der Daten beschäftigen, sind entsprechend entlarvend.

Art. 14 / 15: SiLAN / Datenübermittlung ausserhalb von SiLAN

Es erscheint widersprüchlich von einem *besonders geschützten Informatiknetzwerk zu sprechen*, um dann in Art. 14 Abs. 3 und Art. 15 einen erheblichen Personenkreisen aufzuführen, der auf *SiLAN* zugreifen können soll. Gerade die Kantone, welche über Art. 15 ebenfalls in SiLAN integriert werden, dürften hinsichtlich ihrer IKT frei von Homogenität sein und sich in den getroffenen IKT-Schutzmassnahmen stark unterscheiden: von erhöhten Sicherheitsschwankungen ist auszugehen.

Art. 20: Periodische Überprüfung der Personendaten [IASA NDB]

Es gilt die Kritik von Art. 11 E-NDV sinngemäss.

Art. 21: Aufbewahrungsdauer [IASA NDB]

Die Fristen für Daten in der Datenbank *IASA NDB* umfassen die eigentliche produktive Zeit von einem (ganzen) Erwachsenenleben, indem sie mit 30 oder 45 Jahren belegt sind – abgesehen der Gefahr, dass diese sensiblen Daten an die Öffentlichkeit oder in ihrer Gänze zu fremden Geheimdiensten "abfliessen" könnten (sofern sie nicht ohnehin ausgetauscht werden sollen). Nicht nur ist dies völlig masslos und gefährlich, sondern wiederum entlarvend, betrachtet man die Aufbewahrungsfristen: während im Bereich "Terrorbekämpfung", welcher im Abstimmungskampf als einziger wichtiger Grund für das NDG angeführt wurde, 30 Jahre lang gespeichert wird, gilt für alle anderen Zwecke, um die es eigentlich geht, die Speicherfrist von 45 Jahren.

Art. 27: Periodische Überprüfung der Personendaten [IASA-GEX NDB]

Es gilt die Kritik von Art. 11 E-VIS-NDB sinngemäss.

Art. 28: Aufbewahrungsdauer [IASA-GEX NDB]

Es gilt die Kritik von Art. 21 E-VIS-NDB sinngemäss: die Speicherfristen sind völlig masslos und gefährlich

Art. 33: Periodische Überprüfung der Personendaten [INDEX NDB]

Es gilt die Kritik von Art. 11 E-VIS-NDB sinngemäss.

Art. 36: Daten [GEVER NDB]

Es ist spannend, dass der Bundesrat mit der expliziten Möglichkeit Daten über die *effizienten Arbeitsläufe* im NDB unverschlüsselt abzulegen, die darüber hinaus *VERTRAULICH* und *GEHEIM* klassifiziert sind, sich offenbar insgeheim wünscht, dass diese früher oder später offen im Internet kursieren – zumindest schränkt er diese Möglichkeit nicht grad eben ein.

Art. 44: Periodische Überprüfung [ELD]

Es gilt die Kritik von Art. 11 E-VIS-NDB sinngemäss: würden die Behauptungen vom Abstimmungskampf stimmen, wäre die Kontrolle kontinuierlich möglich.

Art. 45: Aufbewahrungsdauer [ELD]

Es gilt die Kritik von Art. 21 E-VIS-NDB: (jahrelange) Vorratsdatenspeicherung ist abzulehnen.

Art. 49: Periodische Überprüfung [OSINT]

Es gilt die Kritik von Art. 11 E-VIS-NDB sinngemäss.

Art. 50: Aufbewahrungsdauer [OSINT]

Es gilt die Kritik von Art. 21 E-VIS-NDB sinngemäss.

Art. 54: Periodische Überprüfung [Quattro P]

Es gilt die Kritik von Art. 11 E-VIS-NDB sinngemäss.

Art. 55: Aufbewahrungsdauer [Quattro P]

Es gilt die Kritik von Art. 21 E-VIS-NDB: der NDB verfügt mit der hier gewünschten Vorratsdatenspeicherung zu fünf Jahren über Bewegungsprofile von Menschen, welche aus der Schweiz ein- und ausgehen. Das sind überdies Datenpunkte von Bewegungsdaten, die anfallen, selbst ohne dass die betroffenen Personen über ein Mobiltelefon verfügen müssten.

Art. 59: Periodische Überprüfung [ISCO]

Es gilt die Kritik von Art. 11 E-VIS-NDB sinngemäss.

Art. 60: Aufbewahrungsdauer [ISCO]

Es gilt die Kritik von Art. 21 E-VIS-NDB sinngemäss: eine Speicherung über fünf Jahre personenbeziehbarer (und damit identifizierender) Daten, die als eigentliche Kandidaten für Suchbegriffe (oder Selektoren) in der Funk- und Kabelaufklärung gelten, ist eine Anmassung.

Art. 61: Struktur [Restdatenspeicher]

Der *Restdatenspeicher* ist seiner Natur (oder Struktur) nach entlarvend: der Bundesrat kann damit vermeiden, weitere Datenbanken mit Personen- und Organisationsdaten konkret zu benennen, die das Potenzial hätten für einen öffentlichen Aufschrei zu sorgen, weil sie beispielsweise Bürger oder Organisationen führen, denen man nicht einfach anhängen kann mit "Terrorismus", "Gewaltextremismus", "Proliferation", "verbotenem Nachrichtendienst" usw. zu tun zu haben, die aber auch fichiert werden sollen, weil sie beispielsweise unbequem und machtgefährdend sind. Die bereits gesetzliche Existenz und nun Verordnung dieser Datenablage deutet an, dass es der Bundesrat auf weitere Überwachungsbereiche abgesehen hat, die er nicht kundtun möchte.

Art. 64: Periodische Überprüfung [Restdatenspeicher]

Es gilt die Kritik von Art. 11 E-VIS-NDB sinngemäss.

Art. 65: Aufbewahrungsdauer [Restdatenspeicher]

Es gilt die Kritik von Art. 21 E-VIS-NDB sinngemäss: ohne klaren Sinn und Zweck sollen sensible Personen- und Organisationsdaten für ganze 10 Jahre gespeichert werden. In anderen Ländern (mit Verfassungsgericht) würde ein solches Ansinnen mit grosser Wahrscheinlichkeit für ungültig erklärt werden.

Art. 66: Struktur [Beschaffungen im Ausland]

Bei dieser Datenablage handelt es sich um einen eigentlich zweiten Restdatenspeicher: hier kann bunt alles fichiert werden, was sich irgendwie geartet im Ausland befindet.

Art. 67: Daten [Beschaffungen im Ausland]

Es ist weder klar, was der genaue Zweck dieser Datensammlung ist noch kommen Menschen und Organisationen im Ausland in den Genuss irgendwelcher Menschenrechte, als hätte die Schweiz die Europäische Menschenrechtskonvention (EMRK) nie unterschrieben oder (bereits) gekündigt.

Art. 69: Verwendungssperre [Beschaffungen im Ausland]

Es gilt die Kritik von Art. 11 E-VIS-NDB sinngemäss.

Art. 70: Aufbewahrungsdauer [Beschaffungen im Ausland]

Es gilt die Kritik von Art. 21 E-VIS-NDB sinngemäss.

Art. 74: Inkrafttreten

Es wäre sehr wünschenswert diese skandalöse Verordnung würde gar nie in Kraft treten.

Anhang 1: Katalog der Personendaten in IASA NDB und IASA-GEX NDB

Mit nicht weniger als 25 Kategorien von Merkmalen sollen Menschen in den zwei Staatsschutzdatenbanken *IASA NDB* und *IASA-GEX NDB* fichiert werden, die also (vermeintlich) Menschen führen, welche die innere oder äussere Sicherheit der Schweiz (gem. Art 6 NDG Abs. 1) gefährden oder die (vermeintlich) "gewalttätigem Extremismus" anhängen. Die darin – auf nur vager Grundlage – verdächtigte Menschen müssen sich vor dem Schweizer Staat regelrecht ausziehen lassen und das möglicherweise ganz ohne das sie es merken. Die vorhandenen Kategorien, die von biologischen Merkmalen, über das Beziehungsnetz bis zu den Medizin- und Finanzdaten reichen, zeigen auf, dass der Schweizer Fichenstaat wieder mit aller Kraft zurückschlagen soll. Es ist eine absolute Schande und entmenschlichend, eine solche minutiöse Fichierung von Menschen zu planen. Jedwede Beteuerung vom Abstimmungskampf, man habe aus der Fichenaffäre gelernt, wird an-

gesichts dieses Ansinnens, Menschen lückenlos zu durchleuchten, der Lüge überführt – zumal der vorliegende Katalog für die meisten Datenablagen gilt, welche der NDB betreiben soll, auch gerade für jene, wie dem *Restdatenspeicher* oder den *Beschaffungen aus dem Ausland*, die ohne klaren Zweck sind.

Anhang 3: Katalog der Personendaten im INDEX NDB

Es gilt die Kritik vom Anhang 1 E-VIS-NDB sinngemäss.

Anhang 5: Katalog der Personendaten in GEVER NDB

Es gilt die Kritik vom Anhang 1 E-VIS-NDB sinngemäss.

Anhang 7: Katalog der Personendaten in ELD

Die scheinbar wenigen Kategorien von Daten sind genau jene, die in aller Regel ausreichen, um eine Person zu identifizieren und sie in Massen von anderen Menschen darzustellen. Die Elektronische Lagedarstellung (ELD) ist schliesslich die Idee in der Schweiz eine Art "Minority Report"[3] wahr werden zu lassen: beispielsweise lässt sich auf einer Karte ein Mensch verfolgen oder in Menschenmengen anzeigen. Das schliesst nicht aus, dass über die konkrete Person durch die zahlreichen Beschaffungsmassnahmen nicht noch viel umfassendere Daten vorliegen der Art, wie sie im Anhang 1 offenbart werden. Auch diese Kategorien von Daten stellen – zumindest vervollständigt – bereits eine initiale Personenfiche dar.

Anhang 9: Katalog der Personendaten im OSINT-Portal

Es gilt die Kritik von Anhang 1 sinngemäss: bloss weil die Daten online oder in sonstigen zugänglichen Kontexten (relativ einfach) abgegriffen werden können, bedeutet das nicht, dass der NDB diese zu umfassenden Personenfichen zusammenstellen muss. Im OSINT-Portal ist es dem NDB ohne Weiteres möglich, z. B. die gesamten Social-Media-Aktivitäten aller Bürger (ob im In- oder Ausland) zu umfassenden, nach den vorliegenden sehr sensiblen Kategorien zu fichieren und bereits aus diesen Daten Menschen als potenziell gefährlich einzustufen. Dies kann nicht nur zu Chilling-Effects führen, sondern auch Personen gefährden – so die über zehn Jahre aufbewahrten Datensammlungen kopiert werden. Dies kann freilich auch durch Cyberangriffe von Privaten oder staatlichen Akteuren geschehen. Mit solchen umfassenden Datensammlungen besonders schützenswerter Personendaten wird der NDB zu einem interessanten, weil lohnenswerten Angriffsziel. Er hat schliesslich dazu beigetragen, sehr strukturierte Datensammlungen von Menschen anzulegen, die sowohl wirtschaftlich als auch geheimdienstlich anziehend wirken.

Anhang 11: Katalog der Personendaten in Quattro P

[3] Dystopischer US-amerikanischer Hollywood-Film

Es gilt die Kritik von Anhang 1 im Zusammenhang mit der Kritik von Anhang 7 im besonderen Masse: hier werden weitergehende personenidentifizierende Daten gesammelt, die auch vor den biometrischen Daten keinen Halt machen – auch wenn dies geschickt mit Begriffen wie *Daten Ausweis-Chip* verschleiert wird. Zudem stellt dies eine Fichierung der Bewegungen von Menschen aus und in die Schweiz dar, wofür z. B. *Ort* und *Datum* der Grenzkontrolle erfasst werden.

Anhang 13: Katalog der Personendaten in ISCO

Es ist offenkundig, dass es sich bei diesen personenidentifizierenden Daten um Selektoren handelt, um nach Dokumenten jedweder Art, in denen diese vorkommen, mit Mitteln der Massenüberwachung (Funk- und Kabelaufklärung) zu suchen. Es werden auch die sogenannten harten Selektoren erwähnt: *Kommunikationsmittel* und *Fernmeldeanschlüsse*. Durch solche Selektoren lassen sich im Daten-Heuhaufen Treffer generieren, die (in Kombination) diese Menschen, Anschlussnummern und Kontaktadressen zum Inhalt haben. Über die Relevanz solcher Treffer ist damit nichts gesagt. Überwachung mit Funk- und Kabelaufklärung ist eine masslose Form der Überwachung, wo potenziell die gesamte Kommunikation von (in- und ausländischen) Bevölkerungen überwacht wird, um vermeintlich eine Nadel zu finden. Massenüberwachung ist inhärent ineffizient, fehlerbehaftet und menschenverachtend: jede Person wird zum Datum reduziert; wer zu häufig auffällt, nach welchen (weitergehenden, inhaltlichen) Suchmerkmalen auch immer, muss damit rechnen in den näheren Fokus zu geraten – sofern die laufende Funk- und Kabelaufklärung alleine nicht ohnehin schon die Personenfiche zu vervollständigen vermag.

Anhang 15: Katalog der Personendaten im Restdatenspeicher

Es gilt die Kritik von Anhang 1 E-VIS-NDB.

Anhang 17: Katalog der Personendaten in den Speichersystemen für Daten aus genehmigungspflichtigen Beschaffungsmassnahmen und aus Beschaffungen im Ausland

Es gilt die Kritik von Anhang 1 E-VIS-NDB.

Abschliessende Bemerkungen und einziger Trost

Die Verordnungen zum Geheimdienstgesetz NDG dokumentieren minutiös den vorgesehenen systematischen Übergriff auf zahlreiche Amtsregister, privaten und öffentlichen Datensammlungen und -strömen (einschliesslich solchen, die mit dem Überwachungsgesetz BÜPF für die Strafverfolgungsbehörden zur Verfügung stehen); das verbunden mit weitreichendem Zugriff für zahlreiche Stellen von Bund, Kantonen und nicht näher bezeichneten Privaten. Es ist nur eine Frage der Zeit bis ein Beamter mit moralischem

Kompass oder eine anderweitige moralisch gefestigte Person von einem privaten Vertragspartner (ähnlich dem Snowden-Fall mit Booz Allen Hamilton) auf die Idee kommt, die systematischen Grundrechtsverletzungen der Schweizer Dunkelkammer der Nation NDB an die Öffentlichkeit zu tragen, um eine erneute Fichenaffäre in der zumindest digital totalitären (weil im Cyberspace totalüberwachten) Schweiz des 21. Jahrhunderts auszulösen. Dies bleibt dann aber auch der einzige Trost.

Chaotische Grüsse

Für den CCC-CH: Hernâni Marques