## Humanistische Union

# Europäische Dimension von „Cybersicherheit“ (vollständig)

Die Richtlinie für Netz- und Informationssicherheit. Aus: vorgänge Nr. 209 (Heft 1/2015), S. 72-79

*Red.) Eine neue Richtlinie soll den Mitgliedstaaten der Europäischen Union zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS) verhelfen. Der bisherige Diskussionsstand geht dabei nicht besonders weit, mehr noch setzen Überlegungen einzelner Länder, die nur in interinstitutionellen Verhandlungen geäußert werden, die Sicherheit von EU-Bürger_innen regelrecht aufs Spiel. Nur vor dem Hintergrund einer gesamteuropäischen Debatte kann eine wirksame Richtlinie entstehen.*

#### Der Vorschlag der Europäischen Kommission vom Februar 2013

Am 7. Februar 2013 stellte die damalige Kommissarin fu?r die Digitale Agenda, Neelie Kroes, den Vorschlag fu?r eine EU-Richtlinie zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union(1) (NIS) vor. Die NIS-Richtlinie ist eine der Maßnahmen der europäischen Cybersicherheits-Strategie(2)und nicht zu verwechseln mit der Cybercrime-Richtlinie(3), die sich mit der Strafbarkeit von Angriffen auf Informationssysteme beschäftigt.

Das Ziel der NIS-Richtlinie ist eine Erhöhung der Sicherheit des Internets sowie der Netz- und Informationssysteme.(4) Die Notwendigkeit des Gesetzesvorschlags wird mit dem gemeinsamen Binnenmarkt begründet, denn "[...] die Robustheit und Stabilität der Netze und Informationssysteme [sind] eine Voraussetzung fu?r die Vollendung des digitalen Binnenmarkts und fu?r das reibungslose Funktionieren des Binnenmarkts u?berhaupt."(5)Mit einer gemeinsamen Strategie für die Netz- und Informationssicherheit (NIS) können große finanzielle Verluste vom Binnenmarkt abgewendet werden, so die Erklärung zur Richtlinie. Die Rechtsgrundlage für die Richtlinie ist Artikel 26 des Vertrags über die Arbeitsweise der Europäischen Union.(6)

Betreiber_innen kritischer Infrastrukturen von Netzwerk- und Informationssystemen, aber auch „wichtige Anbieter von Diensten der Informationsgesellschaft“ sowie öffentliche Verwaltungen sollen stärker in die Pflicht genommen werden, Sicherheitsrisiken zu bewältigen.(7)Die Richtlinie strebt eine Mindestharmonisierung der Netz- und Informationssicherheit an, denn die uneinheitlichen Ansätze innerhalb der Europäischen Union führen zu einem unterschiedlichen Schutzniveau für Verbraucher_innen und Unternehmen in der EU. In fünf Kapiteln formuliert die Europäische Kommission in ihrem Gesetzesvorschlag folgende Kernpunkte:

- Kapitel I definiert den Anwendungsbereich. Dazu gehören „digitale Informationssysteme“ (Internet), öffentliche Verwaltungen und Betreiber kritischer Infrastrukturen, also Betreiber aus Sektoren wie Strom, Transport, Wasser und Energie.
- Kapitel II setzt den Rahmen für nationale NIS-Strategien, die in allen Mitgliedstaaten zu entwickeln sind. Darüber hinaus soll ein Mindestniveau nationaler Kapazitäten im Bereich der Netz- und Informationssicherheit geschaffen werden, indem eine fu?r die NIS zuständige Behörde eingerichtet wird, die angemessenen personell, finanziell und technisch ausgestattet werden soll. Außerdem sollen

IT-Notfallteams (Computer Emergency Response Teams – CERT) eingerichtet werden.
- Ein gemeinsames Kooperationsnetz zur Bewältigung von Sicherheitsrisiken und Vorfällen soll gebildet werden, mithilfe dessen sich die Mitgliedstaaten gegenseitig über Vorfälle informieren. Die Europäische Agentur fu?r Netz- und Informationssicherheit (ENISA) soll die Arbeit dieses Netzes auf Anfrage unterstu?tzen (Kapitel III). Den zuständigen Behörden mu?ssen alle Sicherheitsvorfälle gemeldet werden, die ihre Netze und Informationssysteme und auch die Kontinuität kritischer Dienste beeinträchtigen.
- Kapitel IV beschäftigt sich mit der Meldung von Sicherheitsvorfällen.
- Kapitel V befasst sich mit Sanktionen im Falle von Verstößen gegen die Richtlinie. Die Ausgestaltung der Sanktionen bleibt den Mitgliedstaaten vorbehalten.

Der Anhang der Richtlinie beschreibt die Aufgaben der CERTs und stellt eine Liste betroffener Typen von Marktteilnehmer_innen auf.

**Stärken und Schwächen des Kommissionsentwurfs**

Die NIS-Richtlinie spricht ein sehr relevantes Problem der Informationsgesellschaft an. Informationstechnik durchdringt inzwischen alle Bereiche des gesellschaftlichen Lebens. Bürger_innen aber auch Unternehmen und der Staat selbst werden immer abhängiger von funktionsfähiger und sicherer Informationstechnologie. Die Digitalisierung und Vernetzung bietet Chancen aber auch Risiken für die Bewältigung der politischen, wirtschaftlichen und gesellschaftlichen Herausforderungen. Angesichts der wachsenden Bedeutung informationstechnischer Systeme ist es wichtig, die Verwundbarkeiten der Netz- und Informationssicherheit zu minimieren. Daher ist die Initiative der Europäischen Kommission zur Verbesserung der Netz- und Informationssicherheit zu begrüßen.

Als positiver Ansatz der Richtlinie ist auch die in Artikel 14 vorgesehene Meldepflicht von Sicherheitsvorfällen zu bewerten. Durch dieses Mittel können Wiederholungen gleicher Angriffe verhindert und Gegenmaßnahmen entwickelt werden. Dass Sicherheitsverstöße gegen die national zu definierenden Maßnahmen im Bereich NIS offengelegt werden müssen, ist ein Fortschritt. Problematisch ist allerdings, dass die Informationen zuerst nur an die zuständigen Behörden geleitet werden und nicht an die betroffenen Nutzer_innen. Nur sofern ein öffentliches Interesse besteht, unterrichtet die zuständige Behörde die Betroffenen (Art. 14 Absatz 4). Dieses Problem könnte allerdings durch Artikel 31 und 32 („Meldung von

Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde“ und „Benachrichtigung der betroffenen Person von einer Verletzung des Schutzes ihrer personenbezogenen Daten“) der momentan verhandelten EU-Datenschutzverordnung im Sinne der Nutzer_innen gelöst werden.(8)

Leider motiviert die Richtlinie nicht ausreichend durch proaktive Ansätze, um Sicherheitsvorfälle vorzubeugen. Unternehmen und Organisationen werden wenig Anreize geboten, ihre Defizite in der IT-Sicherheit zu beseitigen. Regelmäßige Prüfungen und Belohnungen für das Finden und Beseitigen von Sicherheitslücken könnten z.B. ein solcher Anreiz sein. Allerdings können die in Artikel 17 vorgesehenen Sanktionen dafür sorgen, dass Verstöße gegen die in der Richtlinie festgelegten Maßnahmen nicht folgenlos bleiben und wenigstens nachträglich behoben werden.

Die Richtlinie verliert außerdem kein Wort über die Problematik, dass Mitgliedstaaten selbst Begehrlichkeiten über ausnutzbare Sicherheitslücken haben und diese für eigene Angriffe nutzen können.(9)Die Pläne des BND, noch unveröffentlichte Sicherheitslücken, sogenannte Zero Day Exploits, zu kaufen, setzen bewusst die Sicherheit der Bürger_innen aufs Spiel und fachen den Schwarzmarkt für den

Verkauf von Sicherheitslücken an.

Ein weiterer Schwachpunkt ist, dass Softwareprodukte aus der Richtlinie ausgeklammert sind (Erwägungsgrund 24). Klare Haftungsregeln können jedoch zu einem starken wirtschaftlichen Anreiz für die Hersteller von Software sein, um IT-Sicherheit proaktiv zu betreiben. Eindeutige Haftungsregelungen schaffen Anreize zur Qualitätssicherung.

Problematisch ist des Weiteren das Ausschließen von Kleinstunternehmen aus dem Anwendungsbereich der Richtlinie. Die Größe eines Unternehmens ist nicht zwangsläufig für seine Bedeutung als kritische Infrastruktur ausschlaggebend. Oft wird als Beispiel angeführt, dass der Ausfall eines kleinen Betreibers, z.B. eines lokalen Wasserversorgers, keine größeren Auswirkungen habe. Dabei wird vernachlässigt, dass beispielsweise sehr viele Wasserversorger ähnliche, wenn nicht sogar identische Steuerungssysteme nutzen. Gezielt ausgenutzte Schwachstellen in diesen Systemen können damit eine große Anzahl „kleiner Betreiber“ beeinträchtigen und in der Gesamtheit durchaus eine erhebliche Störung verursachen.(10)

**Die Position des Europäischen Parlaments – Stand März 2014**

Als federführender Ausschuss wurde im April 2013 der Ausschuss fu?r Binnenmarkt und Verbraucherschutz (IMCO) des Europäischen Parlaments benannt. Außerdem erarbeiteten auch der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) und der Ausschuss für Industrie, Forschung und Energie (ITRE) Stellungnahmen zum Richtlinienvorschlag. Berichterstatter ist Andreas Schwab (CDU). Das Europäische Parlament legte seinen Standpunkt(11) in erster Lesung zum Vorschlag der NIS-Richtlinie am 13. März 2014 fest. Während eine Reihe von Änderungsanträgen aus dem LIBE(12), v.a. im Bereich Datenschutz, vom IMCO aufgenommen wurden, haben zahlreiche andere wichtige Änderungsanträge wie z.B. Haftungsregelungen von Softwareherstellern keine Mehrheit gefunden. Der wohl größte Unterschied zum Vorschlag der Kommission bezieht sich auf den Anwendungsbereich der Richtlinie. Laut Parlament soll die Richtlinie nicht für Anbieter von Diensten der Informationsgesellschaft wie z.B. soziale Netzwerke, Suchmaschinen oder Cloud-Computing-Dienste gelten. Stattdessen legt das Europäische Parlament den Fokus auf sogenannte kritische Infrastrukturen, also Sektoren wie Strom, Transport, Wasser und Energie.

Als Begründung führt das Parlament in einem Arbeitsdokument an, dass der Kommissionsvorschlag Dienste der Informationsgesellschaft wie Internet-Zahlungs-Gateways, E-Commerce-Plattformen, soziale Netzwerke, Suchmaschinen, usw. nicht klar definiert. Klare Definitionen seien allerdings im Interesse der Rechtssicherheit der EU-Gesetzgebung nötig. Der Titel des Gesetzes „Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union“ macht damit in der Parlamentsposition einen Anspruch geltend, der so nicht eingelöst werden kann. De facto beschäftigt sich die Richtlinie vor allen Dingen mit kritschen Infrastrukturen und kaum noch mit IT-Sicherheit. Es bleibt somit eine Regelungslücke im Bereich der sensible Daten verarbeitenden Wirtschaft im Internet. Für Dienste der Informationsgesellschaft sieht das Parlament lediglich Kooperation auf freiwilliger Grundlage und damit eine Selbstregulierung der Betreiber vor. Konnte das Parlament dem Druck der IT-Lobby nicht standhalten? Bleibt es bei freiwilligen Regelungen, werden sich Unternehmensverbände wie BITKOM(13), EDIMA und DIGITALEUROPE(14 freuen.

**Interinstitutionelle Verhandlungen – seit Oktober 2014**

Im Oktober 2014 begannen die interinstitutionellen Verhandlungen (Triloge) zur NIS-Richtlinie. Auf Seiten des Rats gab es zwar noch keine Position der Mitgliedstaaten, nach Ansicht der italienischen Präsidentschaft

schienen allerdings die wichtigsten Grundsätze und allgemeinen Leitlinien klar zu sein und erste Sondierungsgespräche mit dem Europäischen Parlament begannen. Anfangs erwartete das Parlament noch im Herbst 2014 eine Einigung im Rat zur Richtlinie. In der Regel beginnen die Trilogverhandlungen erst, wenn alle Insitutionen sich auf ihren eigenen Standpunkt geeinigt haben. Die Hoffnungen auf ein vollständiges Verhandlungsmandat des Rats, den general approach (allgemeine Ausrichtung), wurden jedoch enttäuscht. Die Mitgliedstaaten konnten lediglich stückweise Positionen zum Verhandlungsstand(15) liefern.

Die mit Spannung erwartete (unvollständige) Position des Rats aus Oktober 2014(16) überraschte das Verhandlungsteam auf Seiten des Parlaments sehr, denn der Rat schien kaum zur Kooperation bereit. Der Rat löschte fünf Artikel aus dem Kommissionsvorschlag und ersetzte sie mit den zwei neuen Artikeln 8 (a) und 8 (b) zur Kooperationsgruppe und den CERT-Netzwerken. Die Artikel 9 (Sicheres System für den Informationsaustausch), 10 (Frühwarnungen), 11 (Koordinierte Reaktion) und 12 (NIS-Kooperationsplan der Union) entfielen vollständig. Insgesamt sind dadurch die Bestimmungen des Kapitels III deutlich verwässert, wodurch das ursprüngliche Konzept eines Kooperationsmechanismus ineffektiv wird. Als Begründung wies der Rat darauf hin, dass die strategisch-politische Zusammenarbeit und die operative Zusammenarbeit zwei sich nicht gegenseitig ausschließende Konzepte seien. Sein Fokus liegt allerdings deutlich auf der strategischen Zusammenarbeit. Es lässt sich feststellen, dass die Mitgliedstaaten untereinander kaum zur Kooperation bereit sind. Die ursprüngliche Intention der Kommission, mithilfe von NIS finanziellen Schaden vom europäischen Binnenmarkt abzuwenden, wird in den Mitgliedstaaten als zu starke Einmischung in ihre nationale Sicherheit empfunden. Der europaweite Austausch im Bereich der IT-Sicherheit wird zwar als wichtig eingestuft, unklar ist allerdings, wie offen sich die Mitgliedstaaten tatsächlich über Probleme der nationalen Sicherheit miteinander austauschen wollen. Offen bleibt auch, ob sie es zulassen werden, dass die Europäische Kommission diese Gespräche leitet.

Bis Ende 2014 konnte man sich in zwei Trilogen nicht auf einen gemeinsamen Text einigen. Das Parlament stimmte im Dezember 2014 zwar zu, den Vorschlag des Rats zu berücksichtigen, die Artikel 9 bis 12 zu löschen, aber nur unter der Bedingung, dass wesentliche Elemente aus dem ursprünglichen Kooperationsmechanismus in die neuen Artikel 8a und 8b Eingang finden. Parlament und Rat einigten sich im Dezember 2014 darauf, dass die Verhandlungen erst weitergeführt werden, sobald der Rat eine umfassendere Position zum Richtlinienvorschlag bezieht. Nach über dreimonatiger Verhandlungspause begann die lettische Ratspräsidentschaft die Verhandlungen mit dem Parlament fortzuführen. Das neue Mandat der Letten(17) macht dem Parlament zwar einige Zugeständnisse, Artikel 8a und 8b sind jedoch deutlich schwächer, als der mit den Italienern verhandelte Kompromiss. Das Parlament fordert z.B., dass die Mitgliedstaaten regelmäßige „peer reviews“ (Gutachten) im Bereich NIS einholen, während der Rat nur „Gespräche auf freiwilliger Basis“ vorsieht. Außerdem strebt das Parlament an, dass Erfahrungen mit einschlägigen Stellen wie dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und Datenschutzbehörden ausgetauscht werden – diesen Teil löscht der Rat komplett. Darüber hinaus fortdert das Parlament regelmäßige Berichte über die Zusammenarbeit. Auch eine derartige Berichtspflicht sieht der Rat nicht vor.

Kritisiert wird weiterhin, dass sich NIS v.a. auf sogenannte kritische Infrastrukturen beziehe, wobei offen bleibt, wann ein Betreiber „kritisch genug“ ist. Dies soll von jedem Mitgliedstaat selbst definiert werden. Ob Dienste der Informationsgesellschaft auch zum Anwendungsbereich der Richtlinie gehören sollen, ist noch Verhandlungssache. Am 30. April 2015 fand eine dritte Trilog-Sitzung statt, bei der keine Einigung erzielt wurde. Die Standpunkte des Rates und des Europäischen Parlaments liegen immer noch weit auseinander. Ein weiterer Trilog ist für Juni geplant

**Fazit und Forderungen an eine wirksame NIS-Richtlinie**

In der Sache verdient der Vorschlag zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit Unterstützung, er geht aber nicht weit genug. Bestenfalls dokumentieren die

vorgeschlagenen Maßnahmen erfolgte Angriffe und reagieren auf diese. Präventive Maßnahmen – etwa die verantwortungsvolle Veröffentlichung bekannter Sicherheitslücken enthält die Richtlinie nicht. Auch die Schaffung von Anreizen für Hersteller von IT-Systemen, in mehr Sicherheit zu investieren, sieht die Richtlinie nicht vor. Die Enthüllungen von Edward Snowden, die jüngsten Attacken auf den Bundestag, auf den französischen Fernsehsender TV5 Monde oder auf die belgische Tageszeitung Le Soir machen deutlich, wie sehr die Sicherheit von Netz- und Informationssystemen gefährdet ist.

Eine gesamteuropäische Debatte zu NIS ist dringend notwendig. Mit all ihren Schwächen kann die vorgelegte NIS-Richtlinie nur ein erster Schritt in Richtung IT-Sicherheit sein. Was wir brauchen, sind generelle Mindeststandards für die IT-Sicherheit von Produkten und Dienstleistungen sowie klare Haftungsregelungen für Hersteller. Die Kommission ist deshalb weiterhin in der Bringschuld, Gesetzesvorschläge zu unterbreiten, damit die europäische Netz- und Informationssicherheit gewährleistet werden kann. IT-Sicherheit ist eine Vertrauensfrage. Leider scheinen die Mitgliedstaaten untereinander kaum zur Kooperation bereit zu sein. Dass laut Parlament die Richtlinie nicht für Anbieter von Diensten der Informationsgesellschaft gelten soll und stattdessen nur für sogenannte kritische Infrastrukturen, ist ambitionslos und eine große Schwäche. Eine starke NIS-Richtlinie muss alle Bereiche der Informationstechnologie durchdringen, um wirksam zu sein. Es wundert auch, dass das Europäische Parlament zur gleichen Zeit einen sehr starken Abschlussbericht zur Sonderuntersuchung des Parlaments zum Überwachungsprogramm der NSA und anderer Geheimdienste(18)verabschiedet hat. In diesem Abschlussbericht geht es auch um die Verbesserung der IT-Sicherheit in der EU. In diesem Bericht werden klare Ziele und greifbare Lösungsmöglichkeiten aufgeführt:

- Mehr in IT-Kapazität und -Sicherheit der EU investieren. Das verringert die Anfälligkeit der EU gegenüber Angriffen.
- Mehr in lokale und unabhängige Technologien der EU investieren und IT-Schlüsselkapazitäten aufbauen. Ein digitaler „New Deal“ ist erforderlich. Der Wettbewerbsvorteil europäischer IT-Industrie soll genutzt werden.
- Scharfe Verurteilung der Senkung von IT-Sicherheitsstandards mithilfe von „Backdoors“ („Hintertüren“) durch die Geheimdienste.
- Aufforderung an die Kommission, ihre bestehenden Befugnisse im Rahmen der Datenschutzrichtlinie für elektronische Kommunikation und Telekommunikation in vollem Umfang zu nutzen, um den Schutz der Vertraulichkeit von Kommunikation durch Maßnahmen zu verbessern.
- Verwendung von quelloffener Software in allen Umgebungen, in denen die IT-Sicherheit eine wichtige Rolle spielt.
- Forderung genereller Verschlüsselung der Kommunikation einschließlich E-Mails und SMS.
-

Noch laufen die Verhandlungen zur NIS-Richtlinie. Der Abschlussbericht zur Sonderuntersuchung des Parlaments zum Überwachungsprogramm der NSA und anderer Geheimdienste bietet zahlreiche Lösungsvorschläge. Nun liegt es an den Verhandelnden diese umzusetzen, damit die Bürger_innen vor Bedrohungen geschützt werden.

***ZORA SIEBERT*** *Jahrgang 1986, studierte Europäische Studien und Internationale Beziehungen an den Universitäten Magdeburg, Brno, Straßburg und Passau. Seit 2012 ist sie Mitarbeiterin des Mitglieds des Europäischen Parlaments Jan Philipp Albrecht in Brüssel. Dort ist sie u.a. für die Betreuung des Ausschuss fu?r Binnenmarkt und Verbraucherschutz (IMCO) zuständig.*

**Anmerkungen:**

(1) Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf.

(2) Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum,

ttp://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_de.pdf.
(3) Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0321+0+DOC+XML+V0//DE#BKMD-4

(4) Vgl. Begründung NIS-Richtlinie, S. 2., http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf.

(5) Vgl. Begründung NIS-Richtlinie, S. 9, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf.

(6) Vertrag über die Arbeitsweise der Europäischen Union, Artikel 26: (1) Die Union erlässt die erforderlichen Maßnahmen, um nach Maßgabe der einschlägigen Bestimmungen der Verträge den Binnenmarkt zu verwirklichen beziehungsweise dessen Funktionieren zu gewährleisten., https://dejure.org/gesetze/AEUV/26.html.

(7) Vgl. Begründung NIS-RICHTLINIE, S 2 http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf

(8) http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52012PC0011&from=en.

(9) http://www.zeit.de/digital/internet/2014-11/bnd-zero-day-exploit-sicherheit.

(10) Vgl. Prof. Dr.-Ing. Jochen H. Schiller, Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informations-technischer Systeme / Drucksache 18/4096 vom 25.02.2015.

(11) Position des Europäischen Parlaments vom 13.3.2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0244+0+DOC+XML+V0//DE.

(12) Änderungsanträge des LIBE http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-521.696%2b02%2bDOC%2bPDF%2bV0%2f%2fDE.

(13) http://www.bitkom.org/files/documents/BITKOM_Position_on_Cybersecurity_and_NIS-Directive. pdf.

(14) http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&En
.

(15) Ratsposition zu NIS vom 3. Oktober 2014, http://statewatch.org/news/2015/jan/eu-council-NIS- prep-trilogue-13848-14.pdf.

(16) Ratsposition zu NIS vom 3. Oktober 2014, http://statewatch.org/news/2015/jan/eu-council-NIS- prep-trilogue-13848-14.pdf.

(17) Ratsposition zu NIS vom 5. März 2015, http://statewatch.org/news/2015/mar/eu-council-NIS-con

solidated-multi-col-6788-15.pdf.

(18) Zusammenstellung des LIBE-Ausschuss über alle Dokumente zur Sonderuntersuchung des Parlaments zum Überwachungsprogramm der NSA und anderer Geheimdienste, http://www.europarl.europa.eu/committees/en/libe/subject-files.html?id=20130923CDT71796.

---