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

Nachrichtendienste zur Überwindung und Eindämmung von Kryptographie. Zur besseren Vergleichbarkeit werden die historische Nachrichtendienstaktivität und die aktuelle Regulierung untersucht. Diese Gegenüberstellung soll den Widerspruch analysieren und erklären. Der Vergleich erfolgt auf einer technisch-organisatorischen Ebene, also wie Verschlüsselung tatsächlich infiltriert oder anhand welcher Indikatoren sie begrenzt wurde und wird, sowie welche Akteure der Regierung dafür inwiefern verantwortlich sind. Die Enthüllungen von Snowden haben erst historische Vergleiche zwischen öffentlichen und geheimen Projekten zur Kommunikationsüberwachung ermöglicht, letztere stellen eine Forschungslücke dar, die Imperatori schließen möchte.

Hypothese ist, dass die Liberalisie… lierung, und der Schwierigkeiten, … ankern, aufgrund öffentlichen Widerstands durch andere Programme kompensiert wurde: z. B. zeigt sich, dass die Schwelle der Regulierung der Schlüssellänge trotz schrittweiser Erhöhung immer unter dem notwendigen Sicherheitsniveau geblieben ist. Einzelfallentscheidungen zeigen bei der Liberalisierung gleichzeitige Zunahme von nicht-öffentlichen Einzelfallentscheidungen durch die NSA.

Allgemein wird die Ausgewogenheit zwischen Sicherheit und Privatsphäre als Dilemma betrachtet. Doch fraglich ist, ob dieses Dilemma bei der Kryptographie eine passende Analogie ist. Es gibt genügend Argumente dafür, dass Verschlüsselung sowohl die Privatsphäre als auch die Sicherheit schützt, indem es beispielsweise Geschäftsgeheimnisse, den elektronischen Handel, finanzielle Angelegenheiten oder gar die allgemeine Infrastruktur absichert. Doch die US-amerikanische Regierung sowie insbesondere ihr Geheimdienst NSA sehen die Verbreitung von starker Verschlüsselung, die die Privatsphäre schützt und Informationen vor jedem anderem Akteur als dem Besitzer verschließt, offiziell als Gefahr für die nationale Sicherheit und bewerten sie deshalb weiterhin als Dual-Use-Technologie. Mittels ihrer Nachrichtendienste torpedieren die USA heutzutage weltweit die Kryptographie.

Das Programm *Bullrun* korrumpiert die weitläufig verwendeten Online-Protokolle wie VPN, VoIP und SSL. Aber die NSA baut auch systematisch Hintertüren in Router, Server und andere Computernetzwerkgeräte von US-Herstellern, sie hat in der …omputernetzwerke weltweit mit …arf sensible Informationen abzu… verschiedene Funktionalitäten zu …urde, Mikrofone, Webcams oder Internetverläufe samt Login-Details von infiltrierten Computern auszuspähen.

Die Arbeit ist für eine Bachelorarbeit ungewöhnlich: die historisch-kritische Arbeit bearbeitet einen komplexen, interdisziplinären Sachverhalt, in dem sowohl technische, rechtliche als auch politische Parameter gut verständlich analysiert und visualisiert wurden. Das Innovationspotential der Arbeit liegt in dieser historischen Analyse der sich wandelnden technischen, prozeduralen und institutionellen Indikatoren der Dual-Use-Regulierung von Kryptographie. Dies ist ein zentrales Thema des FIfF. Die Jury hat sich einhellig für einen zweiten Preis für diese Arbeit entschieden.

Herzlichen Glückwunsch, Philipp Imperatori, zum Weizenbaum-Studienpreis 2019.

Philipp Imperatori, Thea Riebe und Christian Reuter

Verschlüsselungspolitik der USA: Vom Clipper-Chip zu Edward Snowden

2. Preis

Mit der zunehmenden Bedeutung des Internets, vernetzter Kommunikation und der daraus resultierenden Notwendigkeit der Verwendung von Verschlüsselungstechniken für vertrauliche Daten hat sich die Regulierung von Verschlüsselung verändert. Die USA, in denen die größten IT-Unternehmen ihre Produkte entwickeln, haben ihren Einfluss auf diese Unternehmen durch Exportbeschränkungen kontrolliert und haben somit einen besonderen Zugang zur Kommunikationstechnologie von Menschen auf der ganzen Welt. Dieser Artikel gibt einen Einblick in die Politik bis zum Jahr 2000, in welchem sich eine deutliche Liberalisierung des Umgangs mit Kryptographie zeigte. Im Widerspruch dazu stehen die Veröffentlichungen Edward Snowdens, welche Aufschluss über die heutige Agenda der Dual-Use-Regulierung von Kryptographie geben.[1]

US-amerikanische Verschlüsselungspolitik als Forschungsschwerpunkt

Während Kommunikation früher zumeist auf das lokale und private Gespräch begrenzt war, werden seit dem Aufschwung der informationsorientierten Technologien die häufig privaten Daten durch das globale Netz des Internets übermittelt und auf Endgeräten oder Servern gespeichert. Diese Entwicklung ermöglicht zwar den Austausch über weite Distanzen, sie macht es jedoch schwieriger, Informationen vor Dritten, wie IT-Dienstleistern oder Geheimdiensten, zu schützen und stellt dadurch auch ein Risiko für weitere kritische Infrastrukturbereiche dar (Reuter, 2019). Für diese Herausforderung scheint es, sowohl für die Übermittlung als auch die Speicherung, nur eine zweckmäßige Lösung zu geben: die Verwendung einer Wissenschaft, der Kryptographie, zur sicheren Verschlüsselung der Daten (Landau, 2015; Wassenaar Arrangement Secretariat, 2018). Heutzutage gibt es unzählige kryptographische Algorithmen. Sie sind in heutigen Kommunikationsnetzen, Geräten und Dienstleistungen der Informationstechnologie (IT) allgegenwärtig und

werden dabei meistens im Hintergrund ohne Zutun des Nutzers automatisch verwendet. Das setzt jedoch eines voraus: Internetnutzer, die normalerweise wenig Kryptographie-Expertise mitbringen, müssen der Kommunikationsinfrastruktur vertrauen und sich auf die solide Umsetzung von sicheren kryptographischen Verfahren verlassen.

Schon im frühen elektronischen Zeitalter war die US-amerikanische Industrie global führend im Entwickeln von Computern und Kommunikationstechnologien (Southard, 1997, p. 47). Während der Verbreitung des Internets Anfang der 1990er Jahre hatte die US-Wirtschaft einen geschätzten Anteil von 75 Prozent am globalen Softwaremarkt (Marino, 2005, p. 102). Heute wird der Markt der anwendungsbezogenen IT vor allem von US-amerikanischen Großunternehmen wie Apple, Google, Microsoft, Facebook und Amazon dominiert (Andriole, 2018). Davon abgesehen verfügen Unternehmen mit Hauptsitz in den USA im weltweiten Cyber-Security-Software-Markt, also dem Markt für Sicherheitssoftwarelösungen, über eine signifikante Dominanz: Im Jahr 2015 lag ihr Marktanteil bei circa 61 Prozent (Australian Cyber Security Growth Network, 2018).

Diese Wirtschaftsstärke kommt jedoch mit einer bemerkenswerten Politik seitens der Vereinigten Staaten einher. Kryptographie galt über einige Jahrzehnte in den USA als Waffe und durfte aufgrund starker Regulierungen nicht exportiert werden (Black, 2002, p. 353). Durch die Regulierung sollte der Rest der Welt von starken Verschlüsselungen ausgeschlossen werden. Seit jeher galten das reine Hochladen von Verschlüsselungs-beinhaltendem Programmcode auf eine international erreichbare Webseite oder das Senden einer verschlüsselten E-Mail zu einem ausländischem Kollegen als Export (Black, 2002; Haignere, 1998, pp. 326–328; Schwechter, 2016, p. 2). Mit der Digitalisierung und Verbreitung von digitaler Kommunikation, haben sich auch die Regulierungen angepasst. Dabei ist der 14. Januar 2000 ein zentraler Wendepunkt: Die Administration unter US-Präsident Bill Clinton gab weitreichende Reformen bekannt, die die bis dahin seit Jahrzehnten strikten Ausfuhrbeschränkungen umfassend umgestalteten und dabei allem Anschein nach deutlich liberalisierten (Jolish, 2001, p. 213). Dies wurde von der Softwareindustrie als bedeutender Sieg nach einem jahrelangem Kampf mit der Regierung, der auch als sogenannter *Crypto War* bezeichnet wird, gesehen (Diffie & Landau, 2000, p. 1).

Doch schon vor dem Entgegenkommen durch reformierte Regulierungen entwickelte der Auslandsgeheimdienst National Security Agency (NSA) einen alternativen regulatorischen Lösungsansatz, um so einen Kompromiss zwischen den Bedürfnissen der Wirtschaft und denen der nationalen Sicherheit zu finden (Schulze, 2017). Er basierte auf einer eigens entwickelten Kombination aus einem sogenannten *Clipper-Chip* und einem manipulierten Algorithmus mit einem für damalige Verhältnisse allem Anschein nach hohen Sicherheitsniveau. Diese sollte der Verschlüsselungsstandard bei Kommunikationen werden, wobei eine eingebaute Hintertür der Strafverfolgung Ermittlungen ermöglichen sollte. Zwar scheiterte das Projekt aufgrund der fehlenden Umsetzung durch die Wirtschaft, doch es heizte eine umfangreiche Datenschutzdebatte an, die den historischen *Crypto War* vermutlich erst entfesselte (Steven Levy, 1994).

Aus heutiger Sicht wirft die Überwachungs- und Spionageaffäre der NSA, ausgelöst durch den ehemaligen NSA-Agenten Edward Snowden beginnend im Jahr 2013, eine weitere beispiellose Perspektive auf die Verschlüsselungspolitik der USA. Kryptographie scheint in der Sache unverändert noch heute für zahlreiche US-amerikanische Sicherheitsbehörden ein Dorn im Auge zu bleiben. In den Terrorangriffen von Paris im November 2015 sah der CIA-Direktor John Brennan einen Weckruf, der auch Europäer zur Einsicht bringen sollte, dass Verschlüsselung eine Sicherheitsgefahr darstelle (Geminn, 2015, p. 546; Sokolow, 2015). Doch bereits zwei Jahre zuvor hatte Snowden enthüllt, dass die Vereinigten Staaten womöglich bereits Lösungen für die Eindämmung dieser Gefahr gefunden hatten. Der Nachrichtendienst habe es den Enthüllungen Snowdens zufolge schrittweise geschafft, einige der Verschlüsselungstechnologien teilweise zu umgehen oder zu brechen, die heutzutage den globalen Handel, die Bankensysteme, Geschäftsgeheimnisse, Medizinaufzeichnungen, E-Mails, Websuchen, Internetchats und Telefonanrufe schützen, wie die Dokumente zeigen (Perlroth, Larson et al., 2013).

Es stellt sich die Frage, wieso die Beschränkungen ab dem Jahr 2000 gelockert wurden. Schließlich wurden in den Nachfolgejahren große Anstrengungen unternommen Überwachungsprogramme aufzubauen, um Kryptographie global zu überwinden. Es ist fraglich, wie liberal die aktuelle Verschlüsselungspolitik der USA wirklich ist. Dies ist insbesondere unter Anbetracht des technischen Fortschritts innerhalb der letzten Jahrzehnte spannend, welcher stärkere Kryptographie aufgrund gestiegener Rechenkapazitäten und der Verbreitung des Internets erfordert. Ein chronologischer Blick auf die Regulierungen im Detail als auch die Betrachtung von Snowdens Enthüllungen sowie des historischen *Clipper-Chip*-Programms verdeutlichen, dass sowohl Ausfuhrbestimmungen als auch die Arbeit der NSA wesentliche Instrumente US-amerikanischer Verschlüsselungspolitik waren und sind. Es ist unklar, auf welche Weise und in welchem Umfang sie die Kryptographie beschränken und welches der beiden Instrumente im Zuge der nationalen Sicherheitsvorkehrungen priorisiert wird, was die vergleichende historische Analyse dieser scheinbar zweiseitigen Verschlüsselungspolitik interessant macht.

Eine Wissenschaft als Politikum

Es gibt diverse wissenschaftliche Veröffentlichungen, die die historische Verschlüsselungspolitik darstellen. Überblickend und vielseitig hat Sharon K. Black (Black, 2002) die Regulierungen, Überwachungsgesetze und Bestimmungen der USA über mehrere Jahrzehnte bis zur Jahrtausendwende unter Berücksichtigung kausaler und chronologischer Verkettungen untersucht. Zudem erläutern Mendelson, Walker und Witson (1998) detailliert und chronologisch die Regulierungen in ihrer Intensität und schlagen damit einen ähnlichen analytischen Weg wie Black ein. Jedoch unterscheidet dieser explizit zwischen inländischen und Export-Kontrollen und legt seinen Fokus gleichzeitig mehr auf rein gesetzliche Entwicklungen. Landau und Diffie, letzterer, einer der beiden Pioniere der asymmetrischen Kryptographie, zeigen eine zusammenhangsbezogene Perspektive auf, wobei sie die anderen Arbeiten insoweit ergänzen, indem sie einen Erklärungsansatz für den rapiden Liberalisierungsprozess suchen (Diffie, 2000).

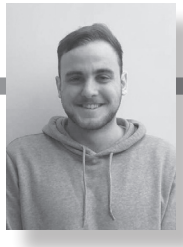
Landau (2015), Schulze (2017), Rubinstein und Hoboken (2014), Gill, Israel und Parsons (2018) und Soesanto (2018) setzen in ihren Veröffentlichungen einen Fokus auf das enthüllte NSA-Agieren unter historischer Bezugnahme. Sie zeigen damit vor allem den nachrichtendienstlichen Umgang mit der Dual-Use-Technologie Kryptographie. Allerdings bieten sie unzureichende Antworten auf die Diskrepanz zwischen der zunehmenden Erleichterung der Kryptographie-Ausfuhrbeschränkungen und den zugleich enthüllten verschlüsselungsuntergrabenden Programmen der NSA. Schließlich bedeutet die *Dual-Use*-Deklaration einer Technologie in den USA obligatorisch zuerst einmal die Begrenzung ihres Exports, also die Festsetzung von Regulierungen, welche damit implizit ein elementares Instrument der Verschlüsselungspolitik darstellen.

Die Begrifflichkeit *Dual-Use* beschreibt in der Forschung zumeist die doppelte Verwendbarkeit von Wissen, Technologie oder Gütern für nützliche und schädliche Zwecke, beziehungsweise für zivile und militärische Zwecke (Oltmann, 2015; Riebe & Reuter, 2019). Beispielsweise kann Kryptographie kriminellen oder kriegerischen Akteuren ermöglichen, ihre verbrecherischen Machenschaften geheim über verschlüsselte Kommunikationen zu organisieren, ohne dass Behörden in der Lage sind, diese Informationen für ihre Ermittlungen abzugreifen. Zugleich kann sie aber auch den Online-Handel oder andere vertrauliche Abwicklungen absichern sowie der Privatsphäre dienen. Bis heute wird die Regulierung von Kryptographie über die Schlüssellänge vorgenommen (Babbage et al., 2008). Das von Sicherheitsexperten empfohlene Sicherheitsniveau liegt mit 128 Bits für die Schlüssellänge mittlerweile weit über dem von den US-Behörden festgelegten Grenzwert von 56 Bits. Das bedeutet, dass jegliche Verschlüsselung, die nach Ansicht der Experten mindestens notwendig ist, damit diese sinnvolle Sicherheit bietet, als Dual-Use-Technologie von den USA bewertet wird und damit den Regulierungen unterliegt.

Darüber hinaus hatte es der Geheimdienst NSA sowohl mittels des im Jahre 1993 verkündeten *Clipper-Chips* als auch mittels der Geheimprogramme, welche durch Snowden zwanzig Jahre später öffentlich wurden, jeweils auf die Dechiffrierung von weitreichenden kryptographischen Kommunikationen durch Hintertüren abgesehen. Nach Kenntnisnahme durch die breite Öffentlichkeit wurden durch beide Projekte jeweils der Impuls zu bedeutenden Debatten gegeben – weil diese in den 1990er Jahren als sogenannter *Crypto War* beschrieben wurde (Steven Levy, 1994), spricht man heute nach der zwischenzeitlichen Beruhigung nun von einer Fortsetzung des *Crypto Wars*, also einem *Crypto War 2.0*, der bis heute andauert (Soesanto, 2018). Während die Clipper-Initiative in einem legalen, freiwilligen und von der NSA manipulierten Verschlüsselungsstandard für Telefonate und Daten mündete, konzentrierte man sich mit den Geheimprogrammen später vor allem auf die Brechung, Infiltrierung und Manipulierung bereits bestehender kryptographischer Standards. Doch vielleicht am bedeutendsten: Wo man damals von einem insgesamt erfolgslosen Vorstoß der NSA gegen nicht zu überwindende Kryptographie aufgrund zu großer Widerstände sprechen konnte, scheint es die NSA mittels des Geheimprojekts geschafft zu haben, Kryptographie überall auf der Welt mittels zahlreicher Wege zu untergraben.

US-amerikanische Unternehmen mussten seit den Snowden-Aufdeckungen bei ihren Kunden um Vertrauen kämpfen: Apple und Google, die die Betriebssysteme für Smartphones dominieren, haben mit automatischen Verschlüsselungen reagiert, die es ihnen auch nach Gerichtsbeschlüssen nicht mehr möglich machen soll, Daten herauszugeben (Craig Timberg, 2014). Zahlreiche Unternehmen erweiterten ihre Sicherheitsmaßnahmen mit Millionen-Investitionen und begannen ein digitales Wettrüsten mit der NSA (Perlroth & Goel, 2013). Während die Unternehmen sich früher durch die Ausfuhrregulierungen beeinträchtigt sahen, ist heute die NSA im Kampf um Verschlüsselung ihr zentraler Gegenspieler. Damals wie heute macht das die US-amerikanische Verschlüsselungspolitik zu einem unverträglichen Faktor für die Wirtschaft des eigenen Landes.

Allgemein wird die Ausgewogenheit zwischen Sicherheit und Privatsphäre als Dilemma betrachtet. Doch fraglich ist, ob dieses Dilemma bei der Kryptographie eine passende Analogie ist. Es gibt genügend Argumente dafür, dass Verschlüsselung sowohl die Privatsphäre als auch die Sicherheit schützt, indem es



Philipp Imperatori, Thea Riebe und Christian Reuter

Philipp Imperatori, Bachelorand am Lehrstuhl *Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)* von Professor Christian Reuter.

Thea Riebe, M.A. studierte Internationale Studien / Friedens- und Konfliktforschung an der Goethe Universität Frankfurt, der TU Darmstadt und der Université de Lausanne, und ist wissenschaftliche Mitarbeiterin in der *BMBF-Arbeitsgruppe KontiKat* der Universität Siegen sowie Doktorandin am Lehrstuhl *Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)* im Fachbereich Informatik (FB 20) der TU Darmstadt.

Prof. Dr. **Christian Reuter** ist Universitätsprofessor und Inhaber des Lehrstuhls *Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)* im Fachbereich Informatik mit Zweitmitgliedschaft im Fachbereich Gesellschafts- und Geschichtswissenschaften der Technischen Universität Darmstadt.

beispielsweise Geschäftsgeheimnisse, den elektronischen Handel, finanzielle Angelegenheiten oder gar die allgemeine Infrastruktur absichert. Doch die US-amerikanische Regierung sowie insbesondere ihr Geheimdienst NSA sehen die Verbreitung von starker Verschlüsselung, die die Privatsphäre schützt und Informationen vor jedem anderem Akteur als dem Besitzer verschließt, offiziell als Gefahr für die nationale Sicherheit und bewerten sie deshalb weiterhin als Dual-Use-Technologie. Mittels ihrer Nachrichtendienste torpedieren die USA heutzutage weltweit die Kryptographie. Aus diesen Gründen ist und bleibt im Besonderen die Verschlüsselungspolitik der USA ein brisantes Thema in der Debatte um die verbreitete Nutzung von Kryptographie sowie eine besondere Herausforderung für den Schutz der BürgerInnen, aber auch für die Freiheit des internationalen Austauschs in Forschung und Handel.

Referenzen

Andriole S (2018, September 26) Apple, Google, Microsoft, Amazon And Facebook Own Huge Market Shares = Technology Oligarchy. Forbes. Retrieved from https://www.forbes.com/sites/steveandriole/2018/09/26/apple-google-microsoft-amazon-and-facebook-own-huge-market-shares-technology-oligarchy/

Australian Cyber Security Growth Network. (2018) Global cyber security software market share by company domicile. Australia's Cyber Security: Sector Competitiveness Plan 2018.

Babbage S, Catalano D, Cid C, Dunkelman O, Gehrmann C, Granboulan L, … Ward M (2008) ECRYPT Yearly Report on Algorithms and Keysizes (2007-2008). (M. Näslund, Ed.).

Black, SK (2002) Encryption. In Adams R (Ed.), Telecommunications Law in the Internet Age (1st ed., pp. 327–387). Morgan Kaufmann Publishers, San Francisco (USA).

Timberg C (2014, September 18) Newest Androids will join iPhones in offering default encryption, blocking police. The Washington Post. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/?arc404=true

Diffie W, Landau S (2000) The Export of Cryptography in the 20th Century and the 21st. Palo Alto, California. Retrieved from https://pdfs.semanticscholar.org/1870/af818dd0075bb5e79764427a7c932fe3cfc6.pdf

Geminn CL (2015) Crypto Wars Reloaded? Datenschutz Und Datensicherheit – DuD, vol. 39, iss. 8, pp. 546–547. https://doi.org/10.1007/s11623-015-0468-7

Gill L, Israel T, Parsons C (2018) Shining a Light on the Encryption Debate: A Canadian Field Guide. Retrieved from https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf

Haignere EF (1998) An Overview of the Issues Surrounding the Encryption Exportation Debate, Their Ramifications, and Potential Resolution. Maryland Journal of International Law, vol. 22, iss. 2, pp. 319–358.

Jolish BD (2001) The Encryption Debate in Plaintext: National Security and Encryption in the United States and Israel. In Y. Frankel (Ed.), Financial Cryptography (Vol. 1962, pp. 202–224). Anguilla, British West Indies: Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45472-1_15

Landau S (2015) NSA and Dual EC_DRBG: Déjà Vu All Over Again? The Mathematical Intelligencer, vol. 37, iss. 4, pp. 72–83. https://doi.org/10.1007/s00283-015-9543-z

Marino LH (2005) The U.S. Export Control Regime for Encryption. The Journal of World Intellectual Property, vol. 1, iss. 1, pp. 101–119. https://doi.org/10.1111/j.1747-1796.1998.tb00005.x

Mendelson KA, Walker ST, Winston JD (1998) The Evolution of recent cryptographic policy in the United States. Cryptologia, vol. 22, iss. 3, pp. 193–210. https://doi.org/10.1080/0161-119891886876

Oltmann S (2015) Dual use research: investigation across multiple science disciplines. Science and Engineering Ethics, vol. 21, iss. 2, pp. 327–341. https://doi.org/10.1007/s11948-014-9535-y

Perlroth N, Goel V (2013, December 5) Internet Firms Step Up Efforts to Stop Spying. The New York Times. The New York Times. Retrieved from http://www.nytimes.com/2013/12/05/technology/internet-firms-step-up-efforts-to-stop-spying.html, http://www.nytimes.com/2013/12/05/technology/internet-firms-step-up-efforts-to-stop-spying.html?hp&_r=0

Perlroth N, Larson J, Shane S (2013, September) N.S.A. Able to Foil Basic Safeguards of Privacy on Web.

Reuter C Ed. (2019) Information Technology for Peace and Security. Wiesbaden: Springer Vieweg.

Riebe T, Reuter C (2019) Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In Reuter C Ed., Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 165–183). Wiesbaden: Springer.

Rubinstein I, Van Hoboken J (2014) Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era. NYU School of Law, Public Law & Legal Theory Research Paper Series, vol. 66, iss. 2, pp. 486–533.

Schulze M (2017) Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016. Media and Communication, vol. 5, iss. 1, pp. 54. https://doi.org/10.17645/mac.v5i1.805

Schwechter MS (2016) Brief Export Controls for Software Companies – What You Need to Know. BakerHostetler. Retrieved from https://www.bakerlaw.com/webfiles/Litigation/2016/Brief/09-01-2016-Schwechter-Brief.pdf

Soesanto, Stefan. (2018). No middle ground: moving on from the crypto wars. Policy Brief. European Council on Foreign Relations (ECFR). Retrieved from https://www.ecfr.eu/page/-/no_middle_ground_moving_on_from_the_crypto_wars.pdf

Sokolow A (2015, November 23) Terror in Paris: Erneut Diskussion über Verschlüsselung. Frankfurter Rundschau. Frankfurt, Deutschland: Frankfurter Rundschau. Retrieved from https://www.fr.de/kultur/erneut-diskussion-ueber-verschluesselung-11140584.html

Southard LS (1997) Securing Information Technology Through Cryptography: An Analysis of United States Policy. Policy Perspectives, vol. 4, iss. 1, pp. 43. https://doi.org/10.4079/pp.v4i1.4190

Steven L (1994, June 12) Battle of the Clipper Chip. The New York Times. Retrieved from https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all

Vella V (2017) Is There a Common Understanding of Dual-Use ?: The Case of Cryptography. Strategic Trade Review, vol. 3, iss. 4, pp. 103–122.

Wassenaar Arrangement Secretariat (2018) The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Retrieved from http://www.wassenaar.org

Anmerkung

1 *Die Grundlage des Artikels ist die Bachelorthesis von Philipp Imperatori am Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) der Technischen Universität Darmstadt, die mit dem zweiten Weizenbaum-Studienpreis ausgezeichnet wurde.*