Philipp Imperatori: Verschlüsselungspolitik der USA. Eine vergleichende Analyse der historischen Entwicklung

Bachelorarbeit, Technische Universität Darmstadt

Es ist mittlerweile sechseinhalb Jahre her, dass wir durch die Enthüllungen von Edward Snowden von der umfassenden Ausspähung unserer Kommunikation erfahren haben. Inzwischen ist das (fast) in Vergessenheit geraten – vielleicht, weil wir uns daran gewöhnt haben, vielleicht, weil wir es tatsächlich im täglichen Leben nicht wahrnehmen, vielleicht wegen der Oberflächlichkeit unserer Zeit, die sich längst anderen Themen zugewandt hat.

Doch der Ursprung der Arbeit, die wir hier bepreisen wollen, liegt noch viel weiter zurück: Als im Jahr 2000, nach der durch die Clipper-Initiative im Jahr 1993 ins Rollen gekommene *Crypto War* zuungunsten der Kontrollwünsche der US Regierung besiegelt war, insbesondere im Rahmen der US-Exportwünsche zur Erhaltung der Priorität des US-Krypto-Marktes eine Liberalisierung effektiver Kryptographie notwendig wurde, begann die geheimdienstliche Überwindung von Kryptographie zur Aufrechterhaltung der Überwachung mittels des geheimen Programms *Bullrun*.

Hier setzt die Arbeit von Philipp Imperatori: *Verschlüsselungspolitik der USA. Eine vergleichende Analyse der historischen Entwicklung* an, die an der Technischen Universität Darmstadt entstanden ist und die wir heute mit einem zweiten Preis des Weizenbaum-Studienpreises auszeichnen.

Seine Hypothese: Wenn die US-amerikanischen Sicherheitsbehörden *Key escrow* angesichts immenser und kaum umkehrbarer Liberalisierungsbewegungen nicht gesetzlich und öffentlich durchsetzen können, dann werden sie in Anbetracht ihrer nationalen Sicherheitsambitionen ihre Prioritätensetzung darauf verlagern, Verschlüsselung, die die Massenüberwachung effektiv behindert, nicht mehr gesetzlich stark zu regulieren, sondern mit anderen Mitteln zu kompromittieren. Dies betrifft insbesondere exklusive Verschlüsselungsexporte.

Daher setzt er die Forschungsfrage: „Welche Prioritäten setzt die US-amerikanische Verschlüsselungspolitik angesichts der Enthüllungen von Snowden unter Berücksichtigung des historischen Kontexts?“

Die Überwachungsprogramme der NSA sind im Sinne der nationalen Sicherheit zweckdienlich zur Eindämmung der Dual-Use-Gefahren. Allerdings bedeutet jede Schwachstelle, die die NSA erkennt, nicht veröffentlicht und nutzt oder in einem kryptographischen Verfahren einbaut oder einbauen lässt, auch die gesamte Schwächung des Verfahrens. Denn wenn der Nachrichtendienst Schwächen nutzen kann, können dies potenziell auch andere Akteure. Zudem ist aufgrund der Geheimhaltung der nachrichtendienstlichen Massenüberwachungsprogramme auch eine transparente Einsicht und deren Regulierung kaum möglich, zumal die NSA dank heutiger weltweiter Vernetzung auch Daten über eine große Anzahl an Menschen außerhalb der USA sammelt, die solchen Vorgängen nicht zugestimmt haben. Somit geht von den verschlüsselungspolitischen Initiativen der NSA, die der allgemeinen Gefahrenbewertung der Kryptographie als Dual-Use-Technologie entspringen, selbst ein Dual-Use-Problem hervor. Edward Snowden sah für die Aufklärung des Dilemmas vermutlich als einzige Möglichkeit das Whistleblowing. Nach Öffentlichwerden der NSA-Aktivitäten wurde der durch Deregulierung beendete erste *Crypto War* mit einer neuen Geschichte fortgesetzt, bei der insbesondere amerikanische Firmen um Vertrauen kämpfen müssen. In dem Bündnis mit dem Namen *Reform Government Surveillance* begannen sie ein digitales Wettrüsten mit der NSA, die jetzt im Kampf um Verschlüsselung ihr zentraler Gegenspieler ist (im Fokus stehen nicht mehr die Ausfuhrgenehmigungen).

Das Ziel der Arbeit besteht darin, die Entwicklung von der *Clipper-Chip* und *Key-Escrow*-Initiative bis zu den Snowden-Enthüllungen 2013 zur Regulierung und Kontrolle von Kryptographie als Dual-Use-Technologie der US-Regierung gegenüber zu stellen. Seine Methode ist die interdisziplinär kompetente Dokumentenanalyse von wissenschaftlichen Veröffentlichungen, politischen Reden, öffentlichen Ankündigungen, Zeitungsartikeln und Gesetzen.

Während Publikationen seit den 1990er Jahren die Regulierung von Kryptographie als Dual-Use-Technologie in den USA und international vergleichen, haben die Enthüllungen von Snowden durch die Bekanntmachung geheimer Projekte zur Kommunikationsüberwachung erst historische Vergleiche zwischen öffentlichen und geheimen Projekten zur Kommunikationsüberwachung ermöglicht. Bisherige Veröffentlichungen zeigen vor allem den nachrichtendienstlichen Umgang mit der Dual-Use-Technologie Kryptographie. Aber sie thematisieren nicht die Diskrepanz zwischen der zunehmenden Erleichterung der Kryptographie-Ausfuhrbeschränkungen und den zugleich enthüllten verschlüsselungsuntergrabenden Programmen der NSA. Denn ihre Arbeiten berücksichtigen nicht, wie sich die Verschlüsselungspolitik auch auf die Ebene der Exportregulierung bis heute auswirkt. Diese Forschungslücke schließt diese Arbeit und verwendet dabei neue Erkenntnisse und Entwicklungen der Snowden-Enthüllungen, um einen historischen Vergleich der Regulierungen, Überwachungsprogramme und der technischen Entwicklung zu ziehen.

Bezüglich der Verschlüsselungs-Methoden, symmetrischen und asymmetrischer Verschlüsselung, befasst er sich der US-Politik folgend hauptsächlich mit Schlüssellänge und Malware.

Ausgangspunkt für den Vergleich bilden die zwei paradox zueinander stehenden Ausrichtungen der US-amerikanischen Verschlüsselungspolitik: der langwierige Prozess hin zu liberalisierten Regulierungen von Kryptographie und zum anderen die weitreichenden Überwachungsprogramme US-amerikanischer

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 Liberalisierung der Kryptographie-Regulierung, und der Schwierigkeiten, *Key escrow* gesetzlich zu verankern, 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 Abteilung TAO circa 50.000 Computernetzwerke weltweit mit Malware infiziert, um bei Bedarf sensible Informationen abzuhören und die Kontrolle über verschiedene Funktionalitäten zu gewinnen, womit es möglich wurde, 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 [illegible] nehmen durch Exportbeschränkungen kontrolliert und haben so[illegible] Menschen auf der ganzen Welt. Dieser Artikel gibt einen Einblick [illegible]iberalisierung des Umgangs mit Kryptographie zeigte. Im Widersp[illegible]ne Aufschluss über die heutige Agenda der Dual-Use-Regulierung von Kryptographie geben.[1]

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

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