Thomas Gruber

Zur Militarisierung der kryptologischen Forschungslandschaft an deutschen Forschungseinrichtungen

Die ganze Mathematik ist in drei Teile geteilt: die Kryptographie (bezahlt von der CIA, dem KGB und Ähnlichen), die Hydrodynamik (unterstützt von den Hersteller.innen von Atom-U-Booten) und die Himmelsmechanik (finanziert vom Militär und anderen Institutionen, die sich mit Raketengeschossen auseinandersetzen, wie die NASA).[1]
– Vladimir Arnold

Für jede Form des Umgangs mit sensiblen Daten gilt eine zentrale Prämisse: Was nicht mitgehört und mitgelesen werden soll, wird verschlüsselt. Daher sind Techniken der Verschlüsselung auch in zahlreichen Bereichen des alltäglichen Lebens zu finden – in der privaten Kommunikation, bei bargeldlosen Geldtransfers, bei der Speicherung von personenbezogenen Daten (wie beispielsweise Patientenakten) und vielem mehr. Kaum verwunderlich also, dass sich das auch in der Forschung zu Verschlüsselungstechniken widerspiegelt: Die Kryptologie ist derzeit eines der am intensivsten beforschten Teilgebiete der angewandten Mathematik. Ebenso offensichtlich wie der individuelle und zivile Nutzen sicherer Verschlüsselung ist allerdings auch ein staatlicher, wirtschaftspolitischer und militärischer. Die Forschung an neuen Verschlüsselungstechniken wird dabei gepaart mit Angriffen auf bereits etablierte Systeme, was zur Abschirmung eigener kritischer Daten und der simultanen Abhörung des gewählten Feindes oder Gegners befähigt.

Mit einem Blick auf die Arbeit deutscher Forschungseinrichtungen stellt sich die Frage, inwiefern sich ein militärischer Nutzen der Kryptologie auch in der hiesigen zivilen Forschungslandschaft abbildet und welche Konsequenzen sich daraus ergeben. Nach einer kurzen begrifflichen und historischen Einordnung der Kryptologie soll hierzu anhand fachtypischer Beispiele die Militarisierung der kryptologischen Forschungslandschaft veranschaulicht werden. Die Formen der militärisch-akademischen Kooperation lassen sich dabei wie folgt gliedern:

- Militärische Drittmittelkooperationen mit deutschen Universitäten
- Kriegsrelevante Forschungsprojekte an deutschen Forschungsinstituten mit universitärer Beteiligung
- Offener Austausch zwischen militärisch und zivil Forschenden auf kryptologischen Fachtagungen
- Beeinflussung der zivilen Forschungslandschaft durch militärische Interessenträger.innen

Begrifflichkeiten und Forschungsbereiche der Kryptologie

Fachlich teilt sich die Kryptologie in die *Kryptographie*, die Forschung zu möglichst sicheren Systemen der Verschlüsselung, und die *Kryptoanalyse*, die Suche nach erfolgversprechenden Angriffsschemata und Schwachstellen etablierter Kryptosysteme.[2] Beide Fachbereiche sind in der Kryptologie allerdings fast untrennbar eng verwoben – mit gutem Grund. Mathematisch lässt sich die Sicherheit eines Kryptosystems nicht beweisen – in endlicher Zeit ist jede Verschlüsselung zu brechen. Mit Hilfe der Kryptoanalyse kann aber verdeutlicht werden, ob dieser endliche Zeitraum für ein Menschenleben realistisch wäre. Das Abwägen, Ausprobieren und die Suche neuer Angriffstaktiken auf Kryptosysteme ist also auch ein ständiger Legitimationsfaktor für die Güte der Verschlüsselung.

Der Namens- und Definitionsraum kryptologischer Forschung begründet sich weitgehend auf eine mathematisierte Darstellung von Strukturen und Algorithmen zur Ver- und Entschlüsselung von Nachrichten. Dabei sind die verschiedenen Verfahren in der Kryptologie so zahlreich wie vielfältig: Es existieren *symmetrische* (*Private-Key*) und *asymmetrische* (*Public-Key*) Verschlüsselungstechniken, Methoden zum sicheren Schlüsselaustausch, Identifikationsverfahren und vieles mehr. Auch kryptoanalytische Angriffe auf gesamte Kryptoverfahren oder auf verwundbare Teile der theoretischen Konzepte nehmen eine zentrale Rolle in der kryptologischen Forschung ein.

Die historische Verbindung zwischen Kryptologie und Krieg

Schon die Stichworte *Mathematik* und *Krieg* verleiten oft zur Assoziation mit der von der nationalsozialistischen Wehrmacht im Zweiten Weltkrieg genutzten Chiffriermaschine *Enigma* und deren spektakulärer Entschlüsselung durch alliierte Mathematiker.innen in Bletchley Park. Und auch sonst ist die Militärgeschichte durchzogen mit der Entwicklung möglichst sicherer Kryptosysteme und feindlichen Angriffen auf dieselben: die *Skytale*, die von den Spartanern 404 v. u. Z. benutzt wurde, um Kriegsbotschaften zu übermitteln;[3] die *Caesar-Chiffre*, mit der der römische Feldherr seine Kommunikation auf dem Schlachtfeld verschlüsselte;[4] die Nutzung der *Vigenère-Chiffre* durch die Südstaaten im US-amerikanischen Bürgerkrieg und die erfolgreichen kryptoanalytischen Angriffe der Nordstaaten;[5] die Entschlüsselung des *Zimmermann-Telegramms*, das zum Kriegseintritt der USA im Ersten Weltkrieg führte;[6] die kryptoanalytischen Angriffe des US-Militärs auf japanische Militärcodes, die den Kriegsverlauf der 1940er-Jahre im Pazifik grundlegend änderte[7], und vieles mehr. Zu beachten ist dabei vor allem eine Parallele: Die taktisch relevanten Nachrichten, die innerhalb einer Kriegspartei versandt wurden, sollten so sicher als möglich verschlüsselt sein. Erfolgreiche feindliche Angriffe auf die verwendete Verschlüsselung veränderten andererseits nicht selten den Kriegsverlauf erheblich. Mit der zunehmenden Bedeutung der Kryptographie im zivilen Sektor der Kommunikation gerät oft die Tatsache in den Hintergrund, dass die Kryptologie ein Kind des Krieges ist. Denn die kryptologischen Anwendungen reichten in den ersten Jahrhunderten ihrer Entstehung kaum

über die Ver- und Entschlüsselung kriegs- oder staatsrelevanter Nachrichten hinaus.

An der Bedeutung der Kryptologie für die Kriegsführung hat sich selbstverständlich auch in modernen Kriegen nichts geändert. Allein die *National Security Agency* (*NSA*) dient in ihrer Geschichte und nach aktuellen Erkenntnissen über ihr Wirken als exemplarische Stellvertreterin für die zentrale Rolle der Kryptologie im militärischen und wirtschaftlichen Wettstreit zwischen Nationalstaaten.[8,9] Die NSA wurde auf Befehl des US-Präsidenten Harry S. Truman im Jahr 1952 unter Geheimhaltung und ohne Rücksprache mit dem Kongress als Zusammenschluss diverser militärischer Geheimdienste – zunächst zur *Armed Forces Security Agency* – gegründet. Zwar blieb die NSA nach wie vor dem US-Verteidigungsministerium unterstellt, doch sollte sie nach Trumans initialer Intention der gesamten US-Regierung dienen; eine Aufgabe, die nach wie vor die Ziele der Behörde bestimmt. Die NSA akquiriert sensible elektronische Kommunikationsdaten, entschlüsselt diese und wertet sie schließlich unter militär- und wirtschaftspolitischen Gesichtspunkten aus. Geschichtlich hat sich allein die politische Lage, nicht die Zielsetzung der geheimdienstlichen Arbeit gewandelt: Im Kalten Krieg, im selbsterklärten *Kampf gegen den Terrorismus* oder in der Spionage in „befreundeten" Staaten – immer war und bleibt das Ziel, mit kryptologischen Mitteln einer militärischen und wirtschaftlichen Überlegenheit des US-amerikanischen Staates zuzuarbeiten

Direkte Drittmittelkooperation mit deutschen Universitäten

Für eine geheime Kommunikation zwischen zwei Personen mittels eines symmetrischen Kryptosystems gilt es, sich zunächst auf einen gemeinsamen Schlüssel zu einigen, mit dem die Nachrichten verschlüsselt werden können. Da aber Nachrichtenkanäle oft abhörbar sind, muss eine sichere Methode zum Schlüsselaustausch über jene Kommunikationswege gefunden werden. Der Diffie-Hellman-Schlüsselaustausch beispielsweise nutzt die diskrete Exponentialfunktion als sogenannte *Einwegfunktion*, also eine Funktion, deren Umkehrfunktion – der diskrete Logarithmus – nur unter enormem Rechenaufwand zu lösen ist.

An dieser Stelle knüpft auch die Fragestellung des Bundesministeriums der Verteidigung an, von dem die Universität Leipzig 2013 mit einer Studie zu den „Möglichkeiten und Grenzen der Berechnung des diskreten Logarithmus" beauftragt wurde.[10] Das militärische Interesse an der Berechenbarkeit einer Funktion, mit der die Sicherheit ganzer Kryptosysteme steht und fällt, ist denkbar vielseitig begründet: Einerseits bietet sie Ansatzpunkte für kryptologische Angriffe auf feindliche Kommunikationsstrukturen in deutschen Kriegseinsätzen oder auf andere selbstgewählte Ziele außerhalb kriegerischer Handlungen wie Privatpersonen, Staaten oder Unternehmen. Andererseits gibt eine solche Analyse Aufschluss über die derzeitige und zukünftige Sicherheit der eigenen Kryptosysteme, mit denen die Kommunikation in ebendiesen Konflikten verschlüsselt wird. Die Auslagerung einer solchen Studie in ein universitäres Forschungsprojekt scheint sinnvoll: Das Thema des diskreten Logarithmus entstammt direkt der theoretischen algebraischen Forschung.

Im mathematischen Sinne stellt die diskrete Exponentialfunktion mit einer gut gewählten strukturellen Basis eine äußerst vielversprechende Einwegfunktion dar – ein diskreter Logarithmus kann zunächst nicht in realistischer Zeit rechnerisch bestimmt werden. Die Angreifbarkeit einer Verschlüsselung hängt allerdings nicht allein von einer Berechenbarkeit des diskreten Logarithmus ab, sondern auch von möglichen Schwachstellen der zugrunde liegenden mathematischen Strukturen und der jeweiligen Umsetzung des Verschlüsselungsalgorithmus. Im Oktober 2015 stellten einige Kryptolog.innen auf der *Conference on Computer and Communications Security* (z.Dt. *Konferenz zur Computer- und Kommunikationssicherheit*) einen Angriff auf eine weit verbreitete Implementierung des Diffie-Hellman-Schlüsselaustauschs (namens *DHE_EXPORT*) vor – die *Logjam-Attacke*. Diese kryptoanalytische Attacke basiert auf einer massiven Vorberechnung von Werten gewisser diskreter Logarithmen und benötigt daher eine enorme Rechenleistung der verwendeten Infrastruktur.[11] Allerdings stehen gerade großen Unternehmen sowie staatlichen und militärischen Akteur.innen jene Hochleistungsrechner meist auch zur Verfügung. Die Analyse geleakter NSA-Dokumente legt nahe, dass der amerikanische Geheimdienst den Logjam-Angriff bereits durchführen kann, was bedeuten würde, dass ein erheblicher Teil einiger im Internet genutzter Verschlüsselungssysteme angreifbar wäre (genauer 66 % aller IPsec-VPNs und 26 % der SSH-Server).[12]

Einige der neuesten Angriffsschemata auf die diskrete Exponentialfunktion befassen sich mit der vergleichsweise jungen *Elliptic Curve Cryptography* (kurz *ECC*).[13] Gravierende Fehler in der Implementierung der ECC-Kryptosysteme wären zwar vermeidbar, sind allerdings keinesfalls immer offensichtlich – oft werden unsichere Algorithmen erst in diesbezüglichen mathematischen oder informatischen Forschungsprojekten aufgedeckt. Ein Beispiel für die Ausnutzung einer unzureichenden Implementierung sind sogenannte *Seitenkanalattacken*: Angreifer.innen können bei einem ECC-System häufig schon über die Rechenzeit der Exponentialfunktion Informationen über den verwendeten Schlüssel gewinnen.[14]

Forschungsprojekte an externen Forschungsinstituten mit universitärer Beteiligung

Außerhalb des engeren universitären Kontexts finden sich Interessent.innen für kriegsrelevante Forschung auch an externen Forschungseinrichtungen. Institute zur Förderung angewandter Forschung – wie beispielsweise die Fraunhofer-, Leibnitz- oder Max-Planck-Institute – verstehen sich meist als Dienstleister für Staat, Militär, Industrie und Wirtschaft, in deren Kreisen sie Forschungsergebnisse als Produkte vermarkten und vertreiben. Allerdings überschneidet sich nicht selten die personelle Besetzung eines Instituts stark mit nahegelegenen Hochschulen – viele Projekte überlagern sich in die staatlich wohlfinanzierte Bildungseinrichtung und die Forschungsinhalte werden von den Lehrstuhlinhaber.innen zur Weiterbearbeitung an den Mittelbau und die Studierenden herangetragen. So wird auch eine unproblematisierte Form der Rüstungsforschung an deutschen Forschungseinrichtungen möglich, die Mitglieder der Hochschulen mit einbezieht und einen Verweis auf den außeruniversitären Charakter der Projekte bei kritischen Nachfragen über kriegsrelevante Forschung zulässt.

Kryptologisch relevant ist in diesem Sinne beispielsweise die Zusammenarbeit zwischen der Arbeitsgruppe *Cyber Analysis and Defense* des *Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie* (*FKIE*) mit Sitz in Wachtberg-Werthhoven und den Hochschulen in Bonn.[15] Große Teile der Angestellten des FKIE und dessen Institutsleitung finden sich in der Personalstruktur des Instituts *Informatik 4* der Universität Bonn wieder und auch inhaltlich entsprechen sich einige Forschungsbereiche der beiden Einrichtungen.[16,17,18] Kriegsrelevante Forschungsergebnisse werden über das FKIE beworben, wie beispielsweise regelmäßig auf der stark militärisch geprägten Fachausstellung des *Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung* (*AFCEA*) – im Jahr 2015 unter dem Motto „IT ‚organisiert' – Bundeswehr und Behörden in der digitalen Welt".[19,20] Eines der laufenden kryptologisch orientierten Projekte am FKIE ist die Entwicklung eines Systems für den „sicheren Informationsaustausch zwischen militärischen Einheiten" in der „vernetzten Operationsführung" namens *IDP/MIKE*.[21] Die Zusammenarbeit zwischen dem FKIE und den Bonner Hochschulen wird hierbei nicht öffentlich benannt, sie findet sich aber thematisch in mehreren studentischen Abschlussarbeiten wieder.[22,23,24]

Das Ziel des IDP-MIKE-Systems ist, ein *Virtual Private Network* (*VPN*) zu implementieren, das in militärischen Einsatzszenarien eine fehlerresistente und dynamische private Kommunikation innerhalb einer Kriegspartei ermöglicht. Ursprünglich bildet ein VPN – wie schon der Name sagt – ein privates Netzwerk für ausgewählte Kommunikationspartner.innen, die sich in einem offenen oder unsicheren Netzwerk (z. B. im Internet oder einem öffentlichen lokalen Netzwerk) befinden. Innerhalb des VPN kann schnell und zuverlässig kommuniziert werden, nach außen wird die Kommunikation verschlüsselt. Herkömmliche VPNs fußen meist auf der Annahme eines während der Kommunikation feststehenden Rechners ohne plötzliche Verbindungsabbrüche und der Eigeninitiative der einzelnen Nutzer.innen beim Kommunikationsaufbau. Beide Voraussetzungen sind in Kriegsszenarien nicht immer erfüllbar, der taktische Mehrwert eines VPNs zwischen den militärischen Einheiten wäre allerdings unbestreitbar. Daher stehen bei der Entwicklung der IDP-MIKE-Software drei wünschenswerte Eigenschaften im Mittelpunkt:

- Das VPN soll von fachfremden Nutzer.innen (z. B. Soldat.innen)
- unter schwierigen Einsatzbedingungen (z. B. Krieg)
- möglichst wartungsfrei verwendbar sein.[25]

Für die Softwarelösung bedeutet das konkret, dass netzwerkfähige Geräte innerhalb einer Kriegspartei sich selbstständig erkennen, miteinander verbinden und bei einem Netzwerkausfall erneut die Kommunikation aufbauen können – insgesamt also eine mobile, dynamische VPN-Lösung. Tests zur Praktikabilität des IDP-MIKE-Systems wurden auf dem Kommunikationsserver *QUAKSBw* (*Querschnittlicher Anteil Kommunikationsserver Bundeswehr*) durchgeführt, der ein Bindeglied zwischen sprach- und datenbasierter Kommunikation sowie den Fernmeldemitteln der Bundeswehr darstellt.[26,27] Schließlich wurde IDP/MIKE auch auf der Rüstungsmesse der AFCEA vorgestellt und als militärische Kommunikationslösung beworben. Der Weg kryptologischer Methoden und Forschungsansätze von einem externen Institut über die universitäre Forschungslandschaft in die deutsche Kriegsplanung ist im Fall des VPNs am FKIE daher einwandfrei nachvollziehbar und unmissverständlich kommuniziert.

Austausch auf kryptologischen Fachtagungen

Neben der direkten Beeinflussung akademischer Forschungsthemen durch Drittmittelkooperationen steht militärischen und geheimdienstlichen Akteur.innen auch der Besuch von internationalen Forschungskonferenzen offen. Gerade bei der Suche nach neuen Kooperationsmöglichkeiten bieten die akademischen Konferenzen einen umfassenden Einblick in die aktuell beforschten Themengebiete. Die Teilnehmenden der meisten Konferenzen sind verschiedenster Nationalitäten. Und so teilen die Forscher.innen, egal welcher Herkunft, ihr Wissen mit den Zuhörer.innen aus Militär und Rüstungsindustrie. Das nimmt auch Forscher.innen deutscher Universitäten nicht aus, die auf kryptologischen Konferenzen meist sehr zahlreich vertreten sind und Ergebnisse ihrer universitären Forschung direkt an Interessierte aus Militär und Rüstungsindustrie weitergeben.

Im Jahr 2009 wurde beispielsweise der NSA-Mitarbeiter J. F. Dillon vom Programmkomitee der *International Conference on Finite Fields and Their Applications* (z.Dt. *Internationale Konferenz zu endlichen Körpern und deren Anwendungen*) eingeladen, um über seinen Erkenntnisstand zur Existenz von *APN-Polynomen*[28] zu referieren.[29] Der Nutzen dieser Polynome besteht in der Kryptographie vor allem in ihrer Robustheit gegenüber kryptoanalytischen Angriffen (genauer: der Differenziellen Kryptoanalyse).[30,31] Dillon stellte in seinem Vortrag die Akquise neuer Erkenntnisse mit einer abschließenden Frage an die Forschungsgemeinde über die Existenz von APN-Polynomen vor.[32]

Die Sicherheit von Kryptosystemen gegenüber der Differenziellen Kryptoanalyse spielt für die NSA-Forscher.innen seit der Implementierung des *Data Encryption Standard* (*DES*) eine zent-

Thomas Gruber

Thomas Gruber ist Mathematiker und promoviert an der Universität Bremen zum Thema Verquickung mathematischer und informationstechnologischer Forschung an deutschen Forschungseinrichtungen mit der modernen Kriegsführung. Er ist Stipendiat der Rosa-Luxemburg-Stiftung und Mitglied der Informationsstelle Militarisierung (IMI) in Tübingen.

rale Rolle. Schon im Jahr 1974 legte die NSA dem Unternehmen IBM nahe, den diesbezüglichen Entwicklungsstand unveröffentlicht zu lassen, was erst im Jahr 1994 bekannt wurde.[33] Die Nutzung des exklusiven Wissens über die Angreifbarkeit und Sicherheit von Kryptosystemen für die Kriegsführung ist leicht nachvollziehbar: Während die NSA selbst sichere Kryptostandards verwendet, können die neu entdeckten Angriffsschemata für eine Kryptoanalyse der feindlichen militärischen Kommunikation genutzt werden. Bis heute hat sich an dieser Praxis nur wenig geändert – zu groß ist anscheinend der kalkulierte Nutzen von Hintertüren in aktuellen Verschlüsselungsschemata für den Geheimdienst.

Beeinflussung der zivilen Forschungslandschaft durch militärische Interessenträger.innen

Die Beeinflussung der kryptologischen Forschung durch militärische Interessenträger.innen beschränkt sich allerdings nicht nur auf Verschwiegenheit bei neuen kryptologischen Forschungserkenntnissen. Sie umfasst auch die Distribution kompromittierter Kryptostandards, die es Angreifer.innen ermöglichen, die jeweilige Verschlüsselung zu brechen. In jüngster Vergangenheit waren dabei vornehmlich Public-Key-Systeme oder Methoden zum Schlüsselaustausch betroffen, die auf der Basis elliptischer Kurven arbeiten.

Ein prominentes Beispiel der geheimdienstlichen Beteiligung bei der Verbreitung eines unsicheren Kryptosystems ist der Pseudozufallsgenerator *Dual_EC_DRBG*.[34] Im Jahr 2013 wurde via eines von Edward Snowden geleakten Dokuments bekannt, dass eine Sicherheitslücke im Dual_EC_DRBG existiert, die der Sicherheitsfirma RSA von der NSA mit 10 Millionen Dollar bezahlt wurde.[35] Zufallszahlen sind essentieller Bestandteil vieler Kryptosysteme – so auch beispielsweise des Diffie-Hellman-Schlüsselaustauschs. Ein ausreichendes Zusatzwissen über die im Kryptosystem verwendeten Zufallszahlen würde es Angreifenden ermöglichen, das gesamte Verschlüsselungsverfahren offenzulegen.

Ungeachtet seiner Schwachstelle erfuhr der Pseudozufallsgenerator Dual_EC_DRBG weite Verbreitung in der kryptologischen Anwendung und der akademischen Forschung. Begründet liegt die Anerkennung solch fehlerhafter Standards vornehmlich in der Politik der US-Normierungsbehörde *NIST* (kurz für *National Institute of Standards and Technology*). Das NIST gibt Empfehlungen für die Normierung etablierter Kryptosysteme und beherzigt dabei geheimdienstlich und von Unternehmen entwickelte Implementierungen, wie die der NSA und des Sicherheitskonzerns RSA. Die NIST-Standards sind außerdem weitgehend alternativlos, die einzigen Ausnahmen bilden von Forscher.innen entwickelte, quelloffene Implementierungen, die als Antwort auf die Sicherheitslücken entstehen. Der Nutzen weit verteilter fehlerhafter Kryptosysteme für die moderne Kriegsführung ist also noch unmittelbarer als der einer bloßen Zurückhaltung von Informationen: Durch gut getarnte Hintertüren in den jeweiligen Implementierungen, die durch eine Veröffentlichung in NIST-Standards als sichere Verschlüsselungsschemata legitimiert werden, bleiben Abhöraktionen lange Zeit unbekannt. Die NIST-Kurven und -Algorithmen werden auch von feindlichen Akteur.innen genutzt und bieten damit eine willkommene, offene Flanke für kryptoanalytische Angriffe.

Fazit

Ob historisch oder in der aktuellen Forschung – die Kryptologie ist und war stets eine wichtige Informationsquelle staatlicher und militärischer Interessenträger.innen bezüglich der Kommunikationssicherheit und der Datenakquise. Neue Ergebnisse der kryptologischen Forschung wirken sich dabei oft stark auf taktische Neuerungen in geheimdienstlichen und militärischen Aktionen aus, wie auch die staatlichen und militärischen Akteur.innen erheblichen Einfluss auf die universitäre Forschung zur Kryptologie nehmen.

Bei der Analyse möglicher Militarisierungstendenzen innerhalb der kryptologischen Forschungslandschaft fällt auf, dass sich Entwicklungen im Forschungssektor oft nur schwer auf einzelne Staaten beschränken lassen. Das liegt zum einen an den selbstverständlichen internationalen Kooperationsbestrebungen von Forscher.innen, zum anderen am transnationalen Agieren von Geheimdiensten, staatlichen Institutionen und Konzernen. Auch ist es oft nicht mehr möglich, militärische Interessen von staatlichen oder wirtschaftlichen zu trennen – zu nah liegen die (geo-) politischen Ziele der jeweiligen Akteur.innen meist beisammen. Staatlich legitimierte (und oft mit der Wahrung von Menschenrechten begründete) Kriege dienen häufig wirtschaftlichen Interessen wie der Absatzmarkterschließung. (Das bestätigten auf Seiten der deutschen Politik auch der ehemalige Bundespräsident Horst Köhler und der ehemalige Verteidigungsminister Guttenberg.[36,37])

Für ein Fazit über die Militarisierung der kryptologischen Forschungslandschaft an deutschen Universitäten muss ob der Intransparenz der geheimdienstlichen und staatlichen Kooperationsprojekte differenziert werden. Einerseits besteht ein starker Informationsfluss aus der universitären Forschung in militärische Anliegen; die Universitäten und Forscher.innen erhalten im Gegenzug Geld, Stiftungsprofessuren, genießen ein gesteigertes Renommee in militärischen Kreisen oder nutzen Kooperationsmöglichkeiten zum Aufbau von Netzwerken. Eine äußerst restriktive Veröffentlichungspolitik bis hin zur Erwirkung von Geheimhaltungsklauseln für die Forschenden verhindert allerdings meist den Rückfluss der Ergebnisse in die akademische Forschung. Andererseits beinhalten die staatlichen Veröffentlichungen zu neuen Kryptostandards oft zusätzlich fehlerhafte, fehleranfällige oder mit Hintertüren versehene Komponenten, die wiederum nach und nach von universitären Forscher.innen und deren Kollektiven oder Whistleblower.innen aufgedeckt werden müssen. Ein parasitär anmutender Informationsfluss von Seiten der Geheimdienste und die willentliche oder zumindest in Kauf genommene Sabotage universitärer Kryptologie für Geldmittel und infrastrukturelle oder personelle Verbesserungen prägen also die Form der Militarisierung der Kryptologie.

Diese höchst bedenklichen Militarisierungstendenzen stehen allerdings jedweder wissenschaftlichen Intention einerseits und der Idee der gesamten Kryptologie andererseits krass entgegen. Wissenschaftliche Arbeit lebt von Transparenz und einer öffentlichen Diskussion von Forschungsergebnissen. Sollte außerdem die absichtliche Verbreitung fehlerhafter Kryptosysteme weiter um sich greifen, muss die Legitimation der gesamten institutionalisierten Forschung eines Bereiches, der sich mit einer verlässlich sicheren und vertraulichen Kommunikation befasst, infrage gestellt werden.

Sowohl gesamtgesellschaftlich als auch wissenschaftlich wäre also ein grundlegendes Interesse begründet, der Militarisierung der kryptologischen Forschung entgegenzuwirken. Dieser Position entgegen stehen die Geldgeber.innen für militärrelevante Forschung, staatliche Tendenzen zur Liberalisierung des Bildungssektors und in diesem Zuge meist auch die einzelnen Universitätsleitungen. Zivil- und Transparenzklauseln – also die Selbstverpflichtung einer Institution, nur für friedliche Zwecke zu forschen und die aktuellen Drittmittelkooperationen zu veröffentlichen – in den Grundordnungen einzelner deutscher Universitäten stellen eine erste politisch erkämpfte Antwort auf die Militarisierung der Forschung dar. Gerade im Bereich der Kryptologie als stark transnational agierende Wissenschaft mit einem gewissen US-Zentrismus kann aber eine Zivilklausel oft nur Drittmittelprojekte an den jeweiligen Institutionen verhindern. Diese Einschränkung betrifft also nur einen kleinen Teil der militärrelevanten Forschung zur Kryptologie. Jede weitere Form des Widerstands bedarf daher einer kritischen Öffentlichkeit, sowohl einer gesamtgesellschaftlichen – ausgedrückt im politischen Kampf – als auch einer wissenschaftlichen. Die Frage nach Verantwortung stellt sich also nicht nur an die politische Öffentlichkeit, sondern auch an die direkt involvierten Forscher.innen, die als Fachkundige am besten Forschungskooperationen auf den gesellschaftlichen Nutzen und die Verträglichkeit prüfen können. Fern von monetären Interessen gälte es innerhalb der kryptologischen Forschungsgemeinschaft das Vertrauen gegenüber Akteur.innen aus dem Militär-, dem Staats- und dem Wirtschaftssektor in Frage zu stellen.

Anmerkungen

1 *Übersetzung des Autors aus dem Englischen.*
2 *Die Möglichkeiten zur Wahl eines Verschlüsselungsverfahrens und des Austausches eines Schlüssels sind so unterschiedlich wie zahlreich – im Verlauf des Artikels werden entsprechende Grundlagen umrissen.*
3 *Jordan, Craig: Secret History: The Story of Cryptology. Chapman & Hall/CRC, 2013. S. 4–5*
4 *ebd., S. 11–12*
5 *Kahn, David: The Codebreakers: The Story of Secret Writing. Simon & Schuster, 1996. S. 217–218*
6 *Jordan, Craig: Secret History: The Story of Cryptology. S. 185–187*
7 *ebd., S. 293–311*
8 *ebd., S. 342–367*
9 *United States SIGINT System, January 2007 Strategic Mission List, http://cryptome.org/2013/11/nsa-sigint-strategic-mission-2007.pdf, 29.02.2016.*
10 *Kleine Anfrage: Militärische und sicherheitstechnische Forschung in Sachsen seit 2009, http://edas.landtag.sachsen.de/viewer.aspx?dok_nr=12635&dok_art=Drs&leg_per=5&pos_dok=-1, 01.03.2016. S. 6*
11 *Adrian, David, et al.: Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. 22nd ACM Conference on Computer and Communications Security, 2015*
12 *Wobei bei der Nutzung von elliptischen Kurven ebenso auf eine fehlerfreie Implementierung zu achten ist, wie die oben stehenden Ergebnisse zeigen.*
13 *Stinson, Douglas R.: Cryptography: Theory and Practice, Third Edition. Chapman & Hall/CRC, 2006. S. 254–267*
14 *Remote Timing Attacks are Still Practical, http://eprint.iacr.org/2011/232.pdf, 02.03.2016.*
15 *Beide Bonner Hochschulen besitzen eine seit 2015 in der jeweiligen Grundordnung verankerte Zivilklausel.*
16 *Fraunhofer FKIE: Institutsleitung, http://www.fkie.fraunhofer.de/de/ueber-uns/institutsleitung.html, 02.03.2016.*
17 *Fraunhofer FKIE: Forschungsbereiche, http://www.fkie.fraunhofer.de/de/forschungsbereiche.html, 02.03.2016.*
18 *Universität Bonn: Institute of Computer Science 4, https://net.cs.uni-bonn.de/start/, 02.03.2016.*
19 *AFCEA Fachausstellung 2015, https://www.afcea.de/29_fa-131.html, 02.03.2016.*
20 *FKIE auf der AFCEA Fachausstellung 2015, https://www.afcea.de/1400.html?tx_mhbranchenbuch_pi1[detail]=29&cHash=6f0eb2587cd75b505dff8d2363a26a97, 02.03.2016.*
21 *IDP / MIKE – Sicherheit zwischen Kommunikationspartnern, http://www.fkie.fraunhofer.de/de/forschungsbereiche/cyber-analysis-and-defense/projekt-idp-mike.html, 02.03.2016.*
22 *Christof Fox: Konzeption eines SOA-konformen Discovery Mechanismus zur Verbesserung der Fehlertoleranz eines Gruppenschlüsselmanagements, http://www.leischner.inf.fh-bonn-rhein-sieg.de/aa/thesis/08_Fox_MIKE-IDP.htm, 10.2.2016.*
23 *Shirish Negi: Evaluation and Optimization of the Group Key Management IDP-MIKE over VHF Data Links, https://net.cs.uni-bonn.de/de/nc/aktuelles/newsansicht/708/e8d00ec903a483e2f6d361bfa-9b8438e/, 02.03.2016.*
24 *Anastasia Danilova: Bewertung des IDP-MIKE-Systems in Bezug auf Replay- und DoS-Angriffe, http://net.cs.uni-bonn.de/nc/news/singleview/584/2ccfc86b9375cec3546458bceb644c07/, 02.03.2016.*
25 *http://www.fkie.fraunhofer.de/de/forschungsbereiche/cyber-analysis-and-defense/projekt-idp-mike.html, 02.03.2016.*
26 *http://www.leischner.inf.fh-bonn-rhein-sieg.de/aa/thesis/08_Fox_MIKE-IDP.htm, 10.2.2016.*
27 *Oberst Warnicke: Das Kommunikationssystem der Bundeswehr für den Einsatz (KommSysBwEins), https://www.afcea.de/fileadmin/downloads/Fachausstellung/23._Fachausstellung_2009/Anmeldung/2 - 20101214_KommSysBw Eins - Vortrag AFCEA_SKUKdo - mit.pdf, 02.03.2016.*
28 *Almost Perfect Nonlinear Polynomial*
29 *Abstracts of the 9th International Conference on Finite Fields and their Applications, http://claudeshannoninstitute.ucd.ie/fq9/AllFq9Abstracts.pdf, 29.02.2016.*
30 *Wikipedia: S-Box, https://de.wikipedia.org/wiki/S-Box, 02.03.2016.*
31 *Highly resistant Boolean functions for cryptography, http://iml.univ-mrs.fr/~ritzenth/AGCT/talks/rodier.pdf, 02.03.2016.*
32 *APN Polynomials: An Update, http://mathsci.ucd.ie/~gmg/Fq9Talks/Dillon.pdf, 02.03.2016.*
33 *Coppersmith, Don: The Data Encryption Standard (DES) and its strength against attacks. IBM Journal of Research and Development, 1994, 38. S. 243–250*
34 *Exclusive: Secret contract tied NSA and security industry pioneer, http://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131221, 29.02.2016.*
35 *Hintertüren und Schwächen im kryptographischen Standard SP 800-90A, https://www.mathematik.de/ger/presse/ausdenmitteilungen/artikel/dmvm-2014-0012.pdf, 29.02.2016.*
36 *Köhler: Krieg für freien Handel, http://www.sueddeutsche.de/politik/bundeswehreinsaetze-koehler-wirtschaftsinteressen-militaerisch-durchsetzen-1.950594, 02.03.2016.*
37 *Guttenberg auf Köhlers Spuren, http://www.taz.de/!5132558/, 02.03.2016.*