FIfF-Konferenz 2014

Der Fall des Geheimen – Ein Blick unter den eigenen Teppich

Wir haben die Rolle Deutschlands und der deutschen Geheimdienste im Kontext der älteren und jüngeren Erkenntnisse – von Echelon über Prism bis Eikonal – zusammen mit rund 400 Besucherinnen und Besuchern beleuchtet und Handlungsoptionen erarbeitet. Natürlich muss die Bearbeitung nun weitergehen.

Am 7. und 8. November 2014 lud das FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung – zur FIfF-Konferenz 2014 ein. Dabei warfen wir den längst überfälligen Blick unter Deutschlands eigenen Geheimdienst-Teppich, denn spätestens nach den jüngsten Enthüllungen zur Rolle Deutschlands im globalen Geheimdienstroulette ist es absurd, nur mit dem Finger über den Atlantik oder auf die Britischen Inseln zu zeigen. Insbesondere Deutschland agiert willentlich als Dreh- und Angelpunkt globaler geheimdienstlicher Aktivitäten und treibt die flächendeckende Überwachung voran.

Wir wollten die Rolle der deutschen Geheimdienste beschreiben und verstehen, wie die Überwachungssysteme gebaut sind, nach welchen Menschen- und Weltbildern sie konzipiert und in welchen Kontexten sie verwendet werden. Mit Experten, Betroffenen, Politikern und der Öffentlichkeit wurden technische, politische, rechtliche, wirtschaftliche und historische Aspekte betrachtet – von Echelon über Prism bis Eikonal. Die Zusammenarbeit von Geheimdiensten, deutschen Telekommunikationsanbietern und Technikern bedarf der besonderen Aufmerksamkeit.

Nötig ist der Blick unter den eigenen Teppich auch, weil die deutsche parlamentarische Aufklärungsarbeit zu den Machenschaften von NSA, GCHQ, BND und Co. nur schleppend vorankommt und angesichts der systematischen Missachtung von Menschenrechten und Grundrechten durch die deutschen Geheimdienste halbherzig wirkt. Zudem sabotiert die Bundesregierung das parlamentarische Unterfangen absichtsvoll und maßgeblich: Sei es durch fast durchgehend geschwärzte oder gänzlich zurückgehaltene Dokumente, durch die Verhinderung von Zeugenvernehmungen oder durch monatelange Verzögerungen. Die Regierung und ihre Geheimdienste haben offenbar aktiv vergessen, dass sie eigentlich vom Parlament kontrolliert werden sollten und nicht andersherum.

Ute Bernhardt, Matthias Bäcker, Wolfgang Coy, Hans-Jörg Kreowski, Constanze Kurz, Wolfgang Nešković, Frank Rieger, Anne Roth, Ingo Ruhmann, Peter Schaar, Erich Schmidt-Eenboom, Patrick Sensburg, Hans-Christian Ströbele, Gregor Wiedemann und Andy Müller-Maguhn trugen mit ihren Vorträgen zum Gelingen der Konferenz bei. Das *Nö-Theater* führte am Samstagabend das Stück *V wie Verfassungsschutz* auf.

Auf den folgenden Seiten dokumentieren wir die Beiträge unserer Referentinnen und Referenten zur Konferenz. Dazu haben wir ihre Vorträge zusammengefasst. Natürlich gilt wie immer das gesprochene Wort: Alle Vorträge wurden aufgezeichnet und sind über die Konferenz-Web-Seite *https://fiffkon.de* unter *https://fiffkon.de/medien.html* zugänglich.

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

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

FIfF-Konferenz 2014

NSA, IT-Sicherheit und die Folgen

Zusammenfassung der Vorträge und Diskussion von Hans-Christian Ströbele, Ingo Ruhmann und Ute Bernhardt

Ruhmann

Das FIfF wurde 1984 gegründet mit dem Thema *Rüstung und Informatik*, vor diesem Hintergrund sollte somit auch der militärische Aspekt des NSA-Skandals diskutiert werden.

Betrachtet man z. B. *XKeyScore*, so zeigen Snowdens Materialien, dass es dabei neben der Ausspähung und Datensammlung ebenso um *Digital Network Intelligence* (DNI) geht, also um *Information Warfare*. Das aber bedeutet, dass nicht mehr nur die umfassende Überwachung durch die NSA thematisiert werden muss, sondern auch deren aktive Manipulation und Sabotage von IT-Systemen. In diesem Zusammenhang ist das *Office of Tailored Access Operations* (TAO) zu nennen. Dessen ca. 900 spezialisierte Hacker entwickeln automatisierte Systeme zur Infiltration von IT-Systeme oder treten selbst in Aktion, wenn dies scheitert. Sie agieren entweder via Internet oder durch die Manipulation von Hardware, während der Produktion und vor deren Auslieferung oder, im Falle eines *Airgaps* (wenn ein IT-System keine Verbindung zum Internet hat), mittels Agenten vor Ort. Das ist jedoch keineswegs etwas Neues, sondern gängige Praxis aus Zeiten des Kalten Krieges. Bereits 1989 wurde über Schadsoftware und Computersabotage berichtet. Auch über die von den Geheimdiensten erstellten Schwachstellendatenbanken, die jetzt einen Teil von XKeyScore darstellen, hat das FIfF bereits 1997 informiert. Damals noch nicht bekannt war allerdings das Ausmaß dieser Manipulationsaktivitäten. Hierbei zeigt sich, dass die Verbreitung von staatlicher Schadsoftware in etwa das gleiche Niveau erreicht hat wie das nichtstaatlicher Viren, Trojaner etc. Ein Blick in den Budgetentwurf der NSA von 2013 beziffert die beantragten Ressourcen für die Internetüberwachung, die Entschlüsselung und die Entwicklung von Angriffswerkzeugen, wie z. B. einem Programm zur Verbreitung von Schadsoftware, auf insgesamt 12 Mrd. US-Dollar. Damit stellt die NSA die am besten finanzierte Hackertruppe der Welt dar. Der größte Anteil dieser Ressourcen in Höhe von 10 Mrd. US-Dollar wurde dabei für die Entwicklung von Angriffstechnologie zum Brechen von Verschlüsselung ausgegeben.

Während der *Heartbleed-Bug* die Aufmerksamkeit auf sich zog, trat der Umstand in den Hintergrund, dass die NSA bereits vor dessen Programmierung „durch spezielle Zugänge zu Unternehmen und [die] Manipulation von Softwarelösungen“ die Fähigkeit besaß, sowohl die aktuelle SSL-Verschlüsselung zu umgehen als auch die älteren gesammelten SSL-verschlüsselten Daten zu dechiffrieren. Das bedeutet aber nichts anderes, als dass das ganze Zertifizierungsprinzip hinterfragt und überdacht werden muss, da es offensichtlich kompromittiert ist.

Dass die von Snowden ausgelöste Debatte um den Datenschutz nur ein Teil der weit größeren Thematik *Cyberwar* ist, erschließt sich aus der Aufgabenbeschreibung der NSA, die sie zu weit mehr als einem nur mit Spionage betrauten Geheimdienst macht. Die NSA ist demnach eine Verteidigungs- und Kampfunterstützungseinrichtung des US-Verteidigungsministeriums. Sie ist also nicht nur ein Geheimdienst, sondern auch die bedeutendste Kampftruppe im Bereich des Informationskriegs. Dieser beinhaltet Medienmanipulation inklusive gezielter Falschinformation und Propaganda sowie die Sabotage, aber auch die Bombardierung von Medieneinrichtungen und Kommunikationssystemen. Als *Cyberwarfare* wird all das bezeichnet, was auf Netzen abläuft. Da der NSA-Direktor gleichzeitig der Kommandeur des *US Cyber Commands* ist, steht er den *information operations units* der US-Streitkräfte vor (von denen die NSA wiederum das größte Kontingent stellt), deren Arbeit allein dem tagtäglichen Krieg im und um den informationstechnischen Bereich gilt. Diese militärischen Operationen richten sich

dabei nicht nur gegen sogenannte Feinde, sondern auch gegen die „Freunde“ und „Verbündeten“ der USA wie Regierungsstellen in Deutschland oder Institutionen wie die Vereinten Nationen oder die Europäische Kommission. Dabei legitimiert die NSA als staatliche Institution ihre Kriegshandlungen durch gesetzliche Befugnisse. Betrachtet man nun die Strategie der Medienbeeinflussung als Bestandteil des Informationskrieges, dann zeigt sich in Verbindung mit der aktuellen Definition des US-Verteidigungsministeriums für *information operations* (den Methoden zur Umsetzung des Informationskrieges), dass sie sich gegen die Willensbildung von Feinden und potenziellen Feinden richten, wobei die Methode der psychologischen Kriegsführung um das Mittel der Computerdisruption erweitert wird.

Diese Definition bedeutet, dass sich der US-Cyberkrieg als eine uneingeschränkte, fortwährende Auseinandersetzung mit Staaten, NGOs, Privatpersonen und Medien darstellt. Dem CERT der Bundeswehr ist dieser Umstand durchaus bekannt, nennt es doch als potenzielle Bedrohung unter anderem nicht nur die feindlichen Nachrichtendienste, sondern auch die befreundeten. Dies führt zu der Feststellung, dass die größte Bedrohung im Netz und für IT-Systeme von der NSA und den mit ihr kollaborierenden Diensten ausgeht, dass die IT-Sicherheitssysteme weitreichend kompromittiert sind und es daher keine Gewissheit über deren Wirksamkeit gibt, dass es die USA sind, die die „Rechtsfreiheit“ des Internets zum uneingeschränkten Cyberkrieg gegen Freund und Feind missbrauchen, und dass deshalb die Datenschutzfrage in diesem Kontext nur ein Teil der Debatte über den „Cyberkrieg unter Freunden“ sein kann. Die Diskussion über Datenschutz und IT-Sicherheit „nach Snowden“ hat also noch gar nicht begonnen!

Bernhardt

Das FIfF entstand vor 30 Jahren aus der Debatte um die Zuverlässigkeit von (militärischen) IT-Systemen. Vor 20 Jahren schon bezeichnete das FIfF das Fernmeldegeheimnis als „strategisches Grundrecht“: Das Fernmeldegeheimnis ist der zentrale Punkt für die Kontrolle der Informationsgesellschaft. Entscheidend ist daher der Schutz von Grundrechten für die IT-Welt. Es gibt seit 1983 das Grundrecht auf informelle Selbstbestimmung und seit 2007 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Ersteres hat sich in Form von Institutionen, z. B. zum Datenschutz in unserer Gesellschaft, etabliert, während letzteres noch nicht institutionell repräsentiert ist. Das bedeutet aber, dass unsere Gesellschaft auf Grundrechten beruht, die von ihrem eigenen Staatsapparat weder garantiert noch eingehalten werden können. Polemisch gesprochen, ist das Telekommunikationsgeheimnis faktisch abgeschafft, der Datenschutz wurde aufgegeben, und die Integrität von IT-Systemen ist gründlich kompromittiert. Was bedeutet aber diese Diskrepanz zwischen dem Grundgesetz und dem ihm zum Teil entgegengesetzten Verhalten einzelner Staatsorgane für unser Staatsverständnis und unsere Staatsform? Welche technischen und gesellschaftlichen Kosten bringt es mit sich, wenn die IT-Systeme einer Gesellschaft, die in bedeutendem Maße von einer IT-Infrastruktur abhängt, kompromittiert sind und wenn die politische Entscheidungsfindung durch information warfare manipuliert wird? Die Geheimdienste haben ihre Rolle erweitert – von einer Kraft der Exekutive hin zu einem politischen Akteur, der seine Mittel nutzt, um die demokratische Debatte zu steuern.

Ströbele

Als langjähriges Mitglied des Parlamentarischen Kontrollgremiums und des NSA-Untersuchungsausschusses spricht Hans-Christian Ströbele über die Arbeit des NSA-Untersuchungsausschusses.

Da die US-Behörden keine Reaktion auf die Anfrage des Untersuchungsausschusses zeigen, konzentriert sich dieser hauptsächlich darauf, herauszufinden, inwieweit auch deutsche Geheimdienste, allen voran der BND, in die verdachtslose und massenhafte Überwachung der Bevölkerung verwickelt sind. Deutschland hat die vorbildlichste Datenschutzgesetzgebung in ganz Europa, auch was die Beschränkungen der Geheimdienste angeht. Im Untersuchungsausschuss wird nun ermittelt, wie der BND z. B. die strategische Satellitenüberwachung in Bad Aibling so filtert, dass der Datenschutz für Grundrechtsträger gewährleistet ist. Es besteht der Verdacht, dass die Geheimdienste in der Weise zusammenarbeiten, dass die einzelnen nationalen Dienste jeweils die Daten von fremden Staatsbürgern sammeln und dann gegen die Daten der eigenen Mitbürger austauschen, die sie nach den nationalen Datenschutzbestimmungen nicht selber erfassen dürfen.

Die methodische Frage, wie mit den technischen Möglichkeiten der Überwachung umgegangen werden soll, die sich aus der stetig wachsenden Ausbreitung und Verknüpfung der IT-Systeme ergeben, entfachte nach dem 11. September 2001 in der NSA selbst einen Konflikt darüber, ob zu einer anlasslosen, umfassenden Vorratsdatenspeicherung übergegangen werden sollte oder ob der Schutz der Bürgerrechte nur einen verdachtsbegründeten, gezielten Einsatz erlaubt. Das mündete in dem Ausscheiden des damaligen für die Datensammlung und Filterung verantwortlichen Direktors Binney, der als Whistleblower den Auslöser für die öffentliche Debatte lieferte und dem NSA-Untersuchungsausschuss bereits als Zeuge zur Verfügung stand. Zwischen der Offenlegung Binneys und den Snowden-Veröffentlichungen hat die NSA die Vorratsdatenspeicherung auf globale Größe ausgebaut. Dabei ist es gar nicht notwendig, die Datenleitungen z. B. in Deutschland direkt zu überwachen, das hat die NSA auch immer bestritten, sondern die Architektur der Netzinfrastruktur vereinfacht die Überwachung. Da der Datenstrom über zentrale Knotenpunkte fließt, genügt es, wenn diese Schnittstellen kompromittiert sind. Der Untersuchungsausschuss soll auch klären, wie genau die Massendatenüberwachung abläuft. Alle Fragen klären solche Ausschüsse nie, aber wesentliche Fragen können

doch beantwortet werden, und so konnte bereits mit der Hilfe des ehmaligen Präsidenten des Bundesverfassungsgerichts, eines weiteren Verfassungsrichters und anderer Rechtsverständiger festgestellt werden, dass die Überwachungsaktivitäten des BND verfassungswidrig sind. Die Reaktion müsste natürlich sein, dass diese Aktivitäten sofort eingestellt werden, was die Bundesregierung nicht durchsetzt und stattdessen eigene Gutachten vorlegt. Eine weitere Erkenntnis ist, dass es wahr ist, dass der BND in Deutschland Daten abschöpft und an die NSA weitergibt, was vorher stets bestritten wurde. Die NSA ihrerseits behauptet ebenso, sich an deutsches Recht zu halten – und hat trotzdem die Kanzlerin abgehört. Es ist also offensichtlich, dass die Vertreter der NSA systematisch lügen. Da kann der Untersuchungsausschuss somit nicht ansetzen. Da der BND aber Daten weitergibt, muss nun ermittelt werden, ob es dem BND überhaupt möglich ist, die Daten von Deutschen aus diesen auszufiltern. Laut Aussage eines Zeugen ist das technisch gar nicht möglich. Die Aktenprüfung umfasst jetzt ungefähr schon 1000 Leitzordner mit 500-800 Seiten Aktenkopien, die zu großen Teilen geschwärzt sind, wofür angeblich 100 Mitarbeiter des Kanzleramtes abgestellt wurden. Wenn der BND aber Deutsche abhören würde, müsste der G10-Ausschuss jede dieser Abhörmaßnamen prüfen und genehmigen, was eine Massenüberwachung unmöglich macht. Betrachtet man die Zeugenbefragung, so kann man sagen, dass sich die öffentlichen Sitzungen in Maßen von den nichtöffentlichen unterscheiden, da die Aussagegrenzen bei letzteren schwächer sind. Bei diesen nichtöffentlichen erfährt der Ausschuss etwas mehr. Bezüglich der Diskussion über die Bespitzelung der Welthungerhilfe in Afghanistan unterlief dem BND-Juristen in der Befragung ein Fauxpas. Er rechtfertigte die Überwachung damit, dass es sich bei den NGO-Mitarbeitern um „Funktionsträger“ handelte und nicht um „Grundrechtsträger“. Auf Nachfrage, was denn einen „Funktionsträger“ ausmachte, erkannte er den Unsinn seiner Aussage und gab zu, dass er sich da vielleicht vertan hätte.

Interessant in diesem Zusammenhang ist jedoch, dass sich der BND mit derartigen Überwachungsoperationen (und von der G10-Kommission abgesegnet) in seiner Arbeit an die weiter oben von Hr. Ruhmann aufgezeigte US-Auffassung angepasst hat, Cyberwar gegen Feinde und potenzielle Feinde zu führen.

Da die Mitglieder des Untersuchungsgremiums nicht das technische Expertenwissen besitzen, um Urteile z. B. über die Tauglichkeit von Filtern zu fällen, lassen sie sich von Sachverständigen, z. B. auch vom Chaos Computer Club, beraten, da diese keinen staatlichen Verpflichtungen unterworfen sind.

Im Übrigen scheut sich der Ausschuss nicht davor, etwaige Falschaussagen der Zeugen als Lügen zu protokollieren.

Warum aber gibt es keinen Aufschrei, bei diesen Zuständen? Jeder könnte aufschreien und jeder sollte aufschreien, das wäre dringend nötig! Leider sieht es aber so aus, dass das Interesse an den Snowden-Veröffentlichungen stark zurückgeht.

Was kann aber nun jeder selbst tun? Man kann z. B. so etwas wie Lavabit, Posteo oder GnuPG und eine dezentrale Internetstruktur nutzen. Wann immer US-Firmen z. B. für die Kommunikation genutzt werden, so werden diese Daten in den USA zentriert; sie sind dort sehr einfach auswertbar. Wenn mehr Menschen ihre Kommunikation verschlüsseln, wird für die Geheimdienste die Überwachung unendlich viel mühsamer, bis es sich schließlich nicht mehr lohnt. Darüber hinaus ist ein Gesetzentwurf zum Whistleblowerschutz eingebracht worden, und die Bundesregierung soll auf Grundlage der EU-Grundrechtecharta ein Vertragsverletzungsverfahren gegen Großbritannien anstreben.

Hans-Christian Ströbele, Ingo Ruhmann und Ute Bernhardt

Hans-Christian Ströbele ist ein erfahrener Politiker, langjähriger Parlamentarier für Bündnis 90/Die Grünen und Rechtsanwalt. Er ist Mitglied des Deutschen Bundestages und beschäftigt sich mit Sicherheits-, Rechts- und Entwicklungspolitik. Er arbeitet im Parlamentarischen Kontrollgremium (PKG) und im NSA-Untersuchungsausschuss.

Ingo Ruhmann ist Informatiker und arbeitet im Bereich Technikfolgenabschätzung, Forschungspolitik, IT-Sicherheit, Information Warfare, *Cyberwar*, Geschichte der Geheimdienste und Datenschutz. Er ist Lehrbeauftragter im Studiengang *Security Management* der Fachhochschule Brandenburg. Er ist Mitglied des FIfF und war Vorstandsmitglied von 1991 bis 1998.

Ute Bernhardt ist Informatikerin und beschäftigt sich seit Jahren mit Forschungspolitik, Datenschutz und IT-Sicherheit, dem Verhältnis von Wissenschaft und Frieden sowie der Beziehung von Informatik und Militär. Sie hat Lehraufträge an der Fachhochschule Bonn-Rhein-Sieg und der FernUni Hagen. Sie ist Mitglied des FIfF und war FIfF-Vorstandsmitglied von 1991 bis 1998.