GCHQ-DATENBANK „FLYING PIG“: Gesammelte Daten über TLS/SSL-Zertifikate dienen der Erleichterung von Angriffen etwa auf Onlinebanking.

Zentrale der National Security Agency in Fort Meade, US-Bundesstaat Maryland

Fliegendes Schwein

Datenschutz Die schlechte Nachricht: NSA und GCHQ knacken verschlüsselte Kommunikation im Internet – mit großem Einsatz und großem Erfolg. Das zeigen Dokumente Edward Snowdens. Die gute Nachricht: Es ist dennoch möglich, Daten zu schützen.

Wenn Weihnachten naht, können sich die Mitarbeiter der Überwachungszentrale GCHQ im englischen Cheltenham vom harten Alltagsgeschäft des Ausspähens erholen. Statt Verschlüsselungen in aller Welt zu knacken, spielen sie ihr „Kryptos Kristmas Kwiz“. Anspruchsvolle Zahlen- und Buchstabenrätsel sind zu lösen. Die stolzen Gewinner des Wettstreits erhalten eine besondere Teetasse, eine „Kryptos“-Tasse.

Verschlüsselung – die Nutzung mathematischer Methoden, um Kommunikation vor Ausspähung zu schützen – wird für elektronische Transaktionen aller Art genutzt, von Regierungen, Firmen und privaten Nutzern. Aber ein Blick in das Archiv des Whistleblowers Edward Snowden zeigt: Nicht alle Verschlüsselungstechniken halten, was sie versprechen.

Skype zum Beispiel, das von 300 Millionen Menschen genutzte Programm zum Videotelefonieren, wird als sicher gepriesen. In Wahrheit gibt es diese Sicherheit nicht. „Dauerhafte Skype-Sammlung begann im Februar 2011“ – so steht es in einem NSA-Schulungspapier aus dem Snowden-Archiv. Knapp ein halbes Jahr später, im Herbst 2011, meldeten die Spione laut diesen Unterlagen Vollzug. Daten von Skype sind seitdem für die Überwacher zugänglich. Software-Gigant Microsoft, dem Skype gehört, erklärt dazu: „Wir versorgen Regierungen nicht mit direktem oder freiem Zugang zu Kundendaten oder Codierungsschlüsseln.“ Das ist offensichtlich nur ein Teildementi: Direkte und bezahlte Übermittlung der Kommunikation der Skype-Nutzer ist damit nicht ausgeschlossen. Seit Februar 2011 ist Skype aufgrund der Anordnung eines geheimen Gerichts als Datenquelle für die NSA verfügbar.

Die „dauerhafte Skype-Sammlung“ ist ein weiterer Schritt der Behörde in dem Wettlauf, den sich Überwacher und Überwachte im Internetzeitalter liefern. Man-

FOTO: NATIONAL SECURITY AGENCY / DPA

che Codierungen sind allerdings auch so gut, dass sie Jahrzehnte überdauert haben und zu Standards geworden sind.

Für die NSA ist Kommunikation, wenn sie verschlüsselt abläuft, ein einziges Ärgernis. In einem internen Schulungsdokument, das der SPIEGEL einsehen konnte, fragt der Referent: „Wussten Sie, dass allgegenwärtige Verschlüsselung im Internet eine große Bedrohung für die Fähigkeit der NSA darstellt, Aufklärung in Datennetzen zu betreiben oder feindliche Schadsoftware zu bezwingen?“

Aus den Snowden-Dokumenten lässt sich ersehen, welche Verschlüsselungsverfahren wohl noch sicher sind und welche von der NSA geknackt wurden. Die Dokumente sind etwa zwei Jahre alt, aber Experten halten es für unwahrscheinlich, dass die Schnüffler mittlerweile wesentlich weiter gekommen sind. Snowden selbst erklärte nach seiner Flucht im Juni 2013 in Hongkong: „Richtig eingesetzte, starke Verschlüsselung gehört zu den wenigen Dingen, auf die man sich verlassen kann.“

Eine durchaus erstaunliche Bilanz: Trotz aller Bemühungen gibt es Programme, die teilweise mehr als 20 Jahre alt sind – und dennoch wohl bis heute sicher.

Aufgrund der digitalen Revolution ist Kryptografie nicht mehr ein exklusives Werkzeug von Geheimagenten. Inzwischen nutzt nahezu jedermann verschlüsselte Internetverbindungen, sei es beim Onlinebanking, beim Internetshopping oder beim Telefonieren. Netzaktivisten organisieren Kryptopartys, auf denen sie Interessierten das Verschlüsseln beibringen, um sicher und privat zu kommunizieren.

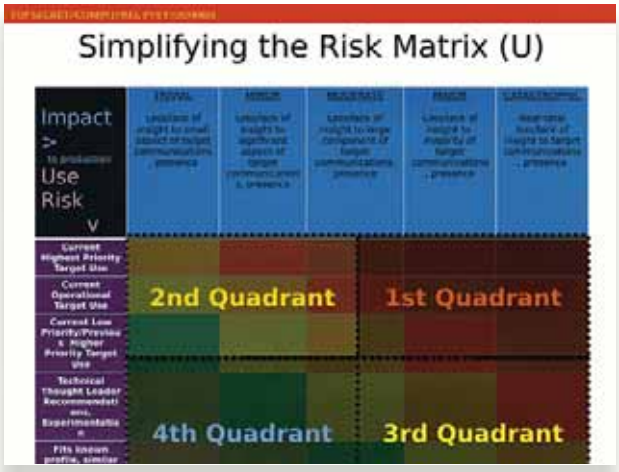
Kanzlerin Angela Merkel und ihr Kabinett nutzen Kryptotelefone. Und die Bundesregierung fordert auch die Bürger auf, sich zu schützen. Der Präsident des Bundesamts für Sicherheit in der Informationstechnik, Michael Hange, erklärte: „Wir schlagen Kryptografie vor, also konsequente Verschlüsselung.“

Das kann den Geheimdiensten nicht passen. Die Fünf-Augen-Allianz – die Geheimdienste Großbritanniens, Kanadas, Australiens, Neuseelands und der USA – verfolgt ein klares Ziel. Sie will Verschlüsselung im Netz an so vielen Stellen wie möglich aushebeln. Für ihren Feldzug gegen die Privatheit standen der NSA 2013 über zehn Milliarden Dollar zur Verfügung, der Etat des britischen GCHQ ist Staatsgeheimnis, dürfte aber bei über einer Milliarde Pfund im Jahr liegen.

Im vorigen Jahr berichtete der *Guardian* über eine Präsentation des NSA-Entschlüsselungsprogramms „Bullrun“ von 2010. Darin heißt es: „Im vergangenen Jahrzehnt hat die NSA einen aggressiven, vielschichtigen Ansatz verfolgt, um die verbreiteten Verschlüsselungstechniken zu knacken.“ Und: „Gewaltige Mengen verschlüsselter Internetdaten, die bislang weggeworfen wurden, lassen sich nun auswerten.“

Noch ist es eine Minderheit der Internetnutzer, die sich um ihre Privatheit sorgt und ihre Daten schützt. Den anderen erscheint das Verschlüsseln, das sie fälschlicherweise für eine Geheimwissenschaft halten, schlicht zu kompliziert. Oder sie glauben, dass die Experten der Geheimdienste ihnen haushoch überlegen seien und jede Verschlüsselung knacken könnten.

Dem ist nicht so. Wie ein Dokument aus dem Snowden-Archiv belegt, scheiterte die NSA zumindest bis 2012 an der Entschlüsselung mehrerer Kommunikationsprotokolle. Welche das sind, lässt sich diesem Dokument, einer NSA-Präsentation für eine Konferenz im Jahr 2012, entnehmen. Die NSA-Kryptologen teilten ihre Ziele in fünf Gruppen ein, entsprechend dem Schwierigkeitsgrad des Angriffs und entsprechend seinem Ergebnis – von „trivial“ bis „katastrophal“.



RISIKOMATRIX: So schätzt die NSA Verschlüsselungsverfahren und ihre unterschiedlichen Anwender ein: E-Mails sind „trivial“, Facebook ist ein „kleineres“ Problem. Mit OTR, Tor und Truecrypt-Verschlüsselungen hingegen gibt es „größere Probleme“.

Als „trivial“ gilt demnach die Verfolgung des Weges, den ein Dokument im Netz nimmt. „Geringe“ Probleme bereitet es angeblich, Facebook-Chats mitzuschneiden; immerhin „mäßiger“ Aufwand ist zu betreiben, um Mails des Moskauer Anbieters Mail.ru zu entschlüsseln. Alle drei Schwierigkeitsstufen scheinen der NSA allerdings noch keinen großen Kummer zu bereiten.

Der beginnt wohl auf Stufe vier. „Größere“ Probleme bereiten den NSA-Überwachern offenbar E-Mail-Dienstleister, die auf starke Verschlüsselung setzen, etwa Zoho oder das für anonymes Surfen im Internet entwickelte „Tor“-Netz. Tor steht für „The onion router“ und ist ein freie offene Software, mit der sich der Nutzer einen verschlungenen Weg durch mehr als 6000 Computer von Freiwilligen bahnt. Die Daten werden, wie bei einer Zwiebel, von einer Verschlüsselung nach der anderen umhüllt und wieder befreit. Für Überwacher ist so kaum zu rekonstruieren, woher der Aufruf einer bestimmten Website stammte.

„Größere“ Probleme hat die NSA auch mit Truecrypt, einem Programm zur Verschlüsselung von Dateien auf Computern, und mit dem sogenannten Off-the-record-Protokoll (OTR) zur Codierung von Chats. Beides sind Open-Source-Projekte, also Programme, deren Quellcode jeder Interessierte einsehen kann. Solche Software, darin sind sich die Experten einig, ist viel schwieriger von Geheimdiensten zu manipulieren als Systeme, die Konzerne wie Apple oder Microsoft entwickeln. Schließlich kann sich bei Open-Source-Projekten jeder den Programmcode ansehen, heimliche Hintertüren lassen sich kaum einbauen. Bei der Überwachung eines Chats stellte die NSA frustriert fest: „Keine Entschlüsselung verfügbar für diese OTR-verschlüsselte Nachricht.“

„Katastrophal“ – Stufe fünf – wird es für die NSA, wenn eine Zielperson beispielsweise eine Kombination aus Tor und einem weiteren Anonymisierungsdienst, wie dem quelloffenen Instant-Messaging-System Cspace, nutzt. „Fast vollständiger Verlust von Erkenntnissen über die Kommunikation und den Aufenthaltsort der Zielperson“ sei die Folge einer solchen Kombination.

Zur sicheren Verschlüsselung von Gesprächen und Textchats auf Mobiltelefonen gibt es das Protokoll ZRTP, das der NSA anscheinend größere Probleme macht. Es wird etwa in den Open-Source-Programmen RedPhone und Signal verwendet. Ihr Entwickler Moxie Marlinspike sagt: „Es ist sehr befriedigend, dass für die NSA die mit unseren Apps verschlüsselte Kommunikation wie ein Blick durch Milchglas ist.“

Entwickelt hat ZRTP unter anderen der Amerikaner Phil Zimmermann, der Mann, der den bis heute gebräuchlichsten Verschlüsselungsstandard für E-Mails und Dokumente geschaffen hat. Er ist bekannt unter der Abkürzung PGP, ausgeschrieben: Pretty Good Privacy – ziemlich gute Privatsphäre. Auch an diesem mehr als 20 Jahre alten Verschlüsselungsstandard bei-

ßen sich die NSA-Spione offenbar die Zähne aus. In einem weiteren Dokument, das der SPIEGEL einsehen konnte, heißt es über E-Mails, die sich die NSA vom E-Mail-Provider Yahoo verschafft hat: „Für diese PGP-verschlüsselte Nachricht ist keine Entschlüsselung verfügbar."

Phil Zimmerman schrieb PGP im Jahr 1991. Der Anti-Atomwaffen-Aktivist wollte sich unbehelligt mit Gleichgesinnten austauschen. Sein System erfreute sich schnell hoher Beliebtheit unter Dissidenten in aller Welt. Da es auch außerhalb der USA verwendet wurde, setzte die US-Regierung gegen Zimmermann Ermittlungen wegen des „Exports von Munition" in Gang. Zimmermann veröffentlichte daraufhin mit Freunden den Quellcode als Buch – dies war durch die in der Verfassung garantierte Meinungsfreiheit abgedeckt.

PGP gibt es heute in verschiedenen weiterentwickelten Varianten, die häufigste ist „GNU Privacy Guard" des deutschen Programmierers Werner Koch. Zu den Eigenheiten der Spionagewelt gehört es, dass auch britische und amerikanische Geheimdienstmitarbeiter eine PGP-artige Software zum Verschlüsseln nutzen.

Tatsächlich decken sich die Interessen von Hackern, die ihre Privatheit schützen wollen, und US-Behörden häufiger, als man erwarten könnte. Das Tor-Projekt – für das auch die Co-Autoren dieses Artikels, Jacob Appelbaum und Aaron Gibson, arbeiten – wurde ursprünglich mit Unterstützung der U. S. Navy entwickelt, um US-Geheimdiensten eine sichere Kommunikation zu ermöglichen.

Die Snowden-Dokumente können einerseits also all jene beruhigen, die der NSA alles zugetraut haben: Es scheint noch geschützte Wege zu geben. Andererseits belegen die Dokumente, dass die Überwachung schon sehr weit geht.

Ein Beispiel: „Virtual Private Networks", VPN, wie es vor allem Mitarbeiter von Firmen und Institutionen mit mehreren Standorten nutzen. Der Schutz des Netzes ist hier tatsächlich nur virtuell, nicht echt. Denn die NSA betreibt ein großes VPN-Projekt, um solche Verbindungen massenhaft zu knacken und die darüber ausgetauschten Daten mitzulesen – etwa das Netz der griechischen Regierung.

Schon für Ende 2009 ist in einem NSA-Dokument davon die Rede, dass tausend Anfragen zur Entschlüsselung von VPN-Verbindungen verarbeitet werden müssten – pro Stunde. Bis Ende 2011 sollte diese Zahl auf 100 000 pro Stunde gesteigert werden. „Mindestens 20 Prozent" dieser Anfragen sollte das System vollständig erfüllen, also den Datenverkehr „entschlüsseln und wieder einschleusen".

Mit anderen Worten: Bereits für Ende 2011 sahen die Pläne der NSA vor, 100 000 vermeintlich sichere VPN-Verbindungen pro Stunde parallel auszuspähen.

Als unsicher muss auch das Protokoll PPTP gelten, ein zentraler Bestandteil vieler VPN. In der NSA-Präsentation „Einführung in den VPN-Ausspähprozess" wird stolz vom Projekt „FOURSCORE" berichtet, das PPTP entschlüssle.

Dadurch sei der Zugang zu zahlreichen Netzwerken gelungen. Ausgespäht wurden etwa die russische Transaero Airlines, Royal Jordanian Airlines und die Moskauer Telekommunikationsfirma Mir Telematiki. Als Erfolg gepriesen wird auch die Überwachung der internen Kommunikation afghanischer, pakistanischer und türkischer Diplomaten.

Für die etwas besseren Verfahren wie IPSEC hat die NSA Angriffsmöglichkeiten entwickelt, mit denen nicht das Verfahren geknackt wird, sondern die Schlüssel entwendet werden.

Weniger Aufwand ist notwendig für einen Angriff auf all jene vermeintlich sicheren Verbindungen, die jeder Internetnutzer ständig verwendet: um Bankgeschäfte zu erledigen, online einzukaufen oder den Web-E-Mail-Account einzusehen.

Sicher ist nichts davon. Die NSA kann mit einem Programm sogar das Protokoll SSH („Secure Shell") knacken. Mit SSH-Verbindungen loggen sich Administratoren ein, um mit anderen Computern zu arbeiten und sie zu steuern. Die Schnüffler sammeln die so gewonnenen Daten zusammen mit anderen Informationen über geknackte Verschlüsselungen in einer Datenbank. Für andere Systeme gibt es ebenfalls Datenbanken.

Telefonsysteme in aller Welt beruhen auf entzifferter Verschlüsselung und sind so gestaltet, dass sie für das Abschöpfen anfällig sind. In den Snowden-Dokumenten lässt sich nachvollziehen, dass die NSA sich Zugang zu Daten verschafft hat, die von Strafverfolgern bei Ermittlungen beschafft wurden, zum Beispiel in Russland und im Irak. Die NSA erklärt zu diesen und allen anderen Vorwürfen, dass sie sich strikt an die US-Gesetze halte.

Die NSA reklamiert für sich und ihre Verbündeten, solche Verbindungen routinemäßig und millionenfach zu knacken. Für Ende 2012 sieht ein NSA-Dokument zehn Millionen geknackte https-Verbindungen pro Tag vor. Besonders interessieren sich die Überwacher für den Moment, in dem ein Nutzer sein Passwort eintippt: 20 000-mal im Monat sollte das System Ende 2012 jeweils „mindestens 100 Passwort-basierte Verschlüsselungsanwendungen entdecken". Erkenntnisse über Verschlüsselungen mit den verbreiteten Protokollen TLS und SSL sammelt der britische Geheimdienst in der Datenbank „Flying Pig", fliegendes Schwein.

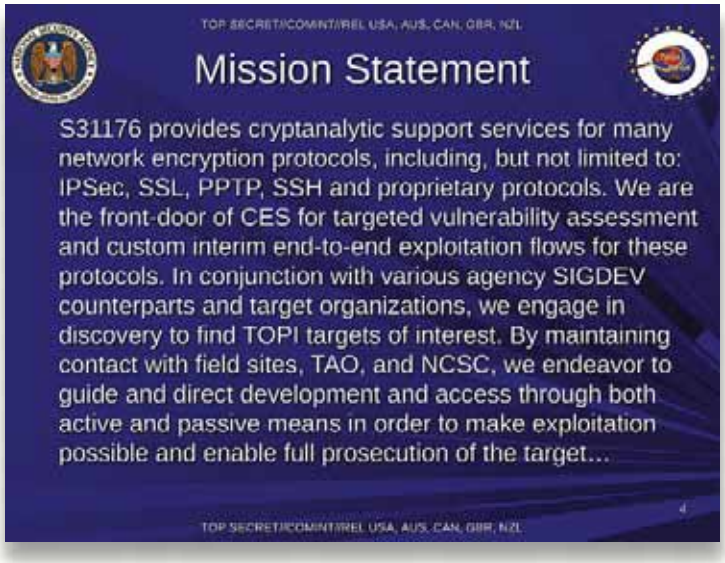
Die Spione Ihrer Majestät speichern in dieser Datenbank alle Informationen über die Nutzer von Verschlüsselungsprogrammen, deren sie habhaft werden können: wann wer mit wem und mit welcher Verschlüsselung telefoniert oder E-Mails austauscht.

In der Schattenwelt der Geheimdienste amüsieren sich die Überwacher wahrscheinlich köstlich darüber, was arglose, normale Internetnutzer für sicher halten. Allein im britischen Geheimdienst GCHQ waren vor rund vier Jahren 832 Personen über das NSA-Projekt „Bullrun" informiert, dessen Ziel dieser Großangriff auf die Internetverschlüsselung ist.

Skype jedenfalls macht den Spähern offenbar keine Mühe mehr. Wer sich darüber unterhält, sollte allerdings nicht glauben, dass nur amerikanische Spione mithören und mitschauen können.

Auch der russische Geheimdienst hat laut verlässlichen Berichten Skype schon vor Jahren geknackt.

Jacob Appelbaum, Aaron Gibson, Christian Grothoff, Andy Müller-Maguhn, Laura Poitras, Michael Sontheimer, Christian Stöcker



LEITSPRUCH EINER NSA-ENTSCHLÜSSELUNGSABTEILUNG
„Aktive und passive Maßnahmen, um Auswertungen und volle Verfolgung von Zielen zu ermöglichen."

Lesen Sie weiter auf Seite 80
Die geheimen Todeslisten: Wie Amerikaner und Briten in Afghanistan Taliban jagten – gezielte Tötungen gehörten zum Alltag.

US-Drohne über Kandahar, Afghanistan

Obamas Listen

Afghanistan Der Kampfeinsatz am Hindukusch geht zu Ende, doch ein Blick in geheime Dokumente der Nato zeigt: Amerikaner und Briten jagten Taliban weitaus skrupelloser als bisher bekannt. Auch Drogenhändler waren zum Abschuss freigegeben.

Der Tod kreist am Morgen des 7. Februar 2011 über der Provinz Helmand, er kommt in Gestalt eines britischen „Apache"-Kampfhubschraubers mit dem Namen „Ugly 50". Dessen Mannschaft ist auf der Suche nach einem Afghanen namens Mullah Niaz Mohammed. Der Pilot hat den Auftrag, ihn zu töten.

Der Afghane trägt den Decknamen „Doody", ein Talib aus der „mittleren Ebene", wie es in einer geheimen Liste der Nato heißt. In dem Dokument sind feindliche Kämpfer aufgeführt, die die Allianz für gezielte Tötungen freigegeben hat. „Doody" steht an Nummer 3673, die Nato hat ihm auf der Skala von eins bis vier die Priorität drei eingeräumt. In der Führungsstruktur der Taliban ist er also nicht besonders wichtig.

Um 10.17 Uhr hat die Einsatzzentrale „Doody" identifiziert. Allerdings ist die Sicht schlecht, der Kampfhubschrauber muss noch eine Runde drehen. Dann feuert der Schütze eine „Hellfire"-Rakete ab. Doch während des Manövers hat er den Mullah aus den Augen verloren, die Rakete trifft nicht den Talib, sondern einen Mann und dessen Kind. Der Junge ist sofort tot, der Vater schwer verletzt. Als der Pilot merkt, dass er die Männer verwechselt hat, gibt er 100 Schuss aus seiner 30-Millimeter-Bordkanone auf „Doody" ab und verletzt ihn lebensgefährlich.

Das Kind und sein Vater sind zwei von vielen Opfern der schmutzigen Geheimoperationen, die die Nato jahrelang am Hindukusch durchgeführt hat. Ihr Schicksal ist in vertraulichen Dokumenten der Nato beschrieben, die der SPIEGEL einsehen konnte. Die Dokumente der Isaf-Truppen sowie der Geheimdienste NSA und GCHQ stammen unter anderem aus dem Bestand von Edward Snowden. Sie umfassen erstmals die komplette Liste der westlichen Allianz für das „targeted killing" in Afghanistan. Die Unterlagen zeigen, dass die tödlichen Angriffe nicht nur als letztes Mittel eingesetzt wurden, um Anschläge zu verhindern, sondern zum Alltag im afghanischen Guerillakrieg gehörten.

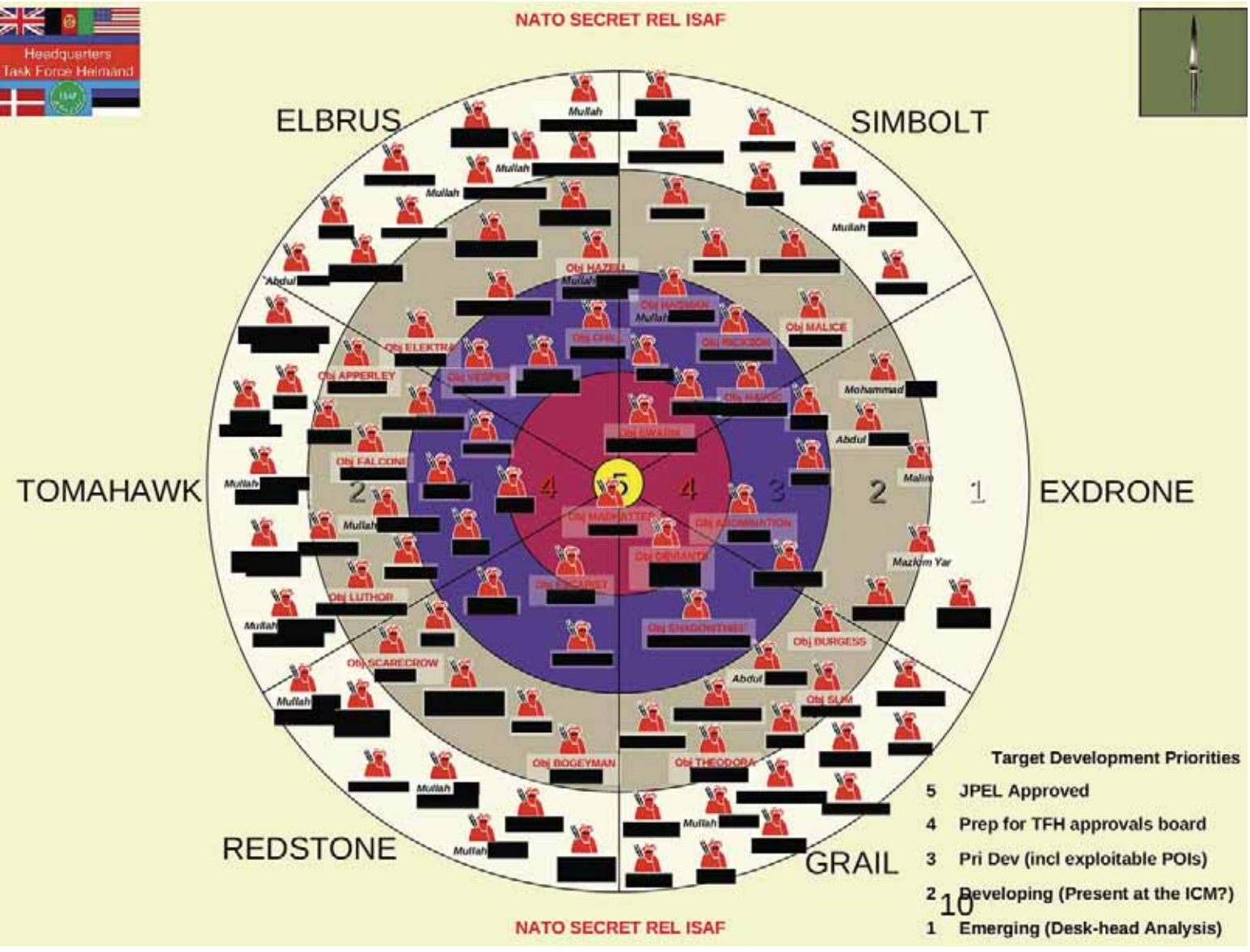
Die Liste, auf der zeitweise 750 Personen standen, belegt nun erstmals, dass die Nato nicht nur auf den Führungskreis der Taliban zielte, sondern auch die mittlere und untere Ebene in großem Stil ausschaltete. Einige Afghanen standen nur deshalb darauf, weil sie angeblich als Drogenhändler die Aufständischen unterstützten.

In dieser Woche endet der 13-jährige Kampfeinsatz am Hindukusch offiziell, aber die Todeslisten werfen rechtliche und moralische Fragen auf, die weit über Afghanistan hinausreichen: Darf eine Demokratie ihre Feinde gezielt töten, wenn es nicht um die Verhinderung eines unmittelbar bevorstehenden Angriffs geht? Und rechtfertigt das Ziel, möglichst viele Taliban auszuschalten, den Tod von unbeteiligten Männern, Frauen und Kindern?

Im Krieg gelten andere Regeln als bei der Verbrechensbekämpfung in Friedenszeiten. Aber der Westen hat den Feldzug in Afghanistan jahrelang mit dem Versprechen verbunden, dort für andere Werte anzutreten. Eine Demokratie, der ein Verdacht ausreicht, um ihre Feinde zu töten, verspielt ihren Anspruch auf moralische Überlegenheit. Sie macht sich mitschuldig. Diese Lehre aus Afghanistan gilt auch für die Konflikte in Syrien und dem Irak, in Pakistan und im Jemen.

Das Material, das der SPIEGEL nun auswerten konnte, stammt aus den Jahren 2009 bis 2011 und fällt in die Amtszeit des US-Präsidenten Barack Obama, der im Ja-

FOTO: KIRSTY WIGGLESWORTH / AP / DPA



IM FADENKREUZ **Ein Isaf-Diagramm von 2011 beschreibt die Einstufung von Taliban-Anhängern in Helmand. Die Nato unterscheidet fünf Kategorien, ein Teil der Verdächtigen steht bereits auf der JPEL-Liste oder soll aufgenommen werden. Anschließend übernimmt die Task Force Helmand die Jagd auf die Taliban.**

nuar 2009 ins Weiße Haus eingezogen war. Für Obama war Afghanistan der „gute“ Krieg, für den es – anders als für den Irakfeldzug – eine Legitimation gab. Den Waffengang im Irak wollte der Präsident schnellstmöglich beenden. In Afghanistan aber wollte er gewinnen.

Nach Obamas Amtsübernahme entschied sich die US-Regierung deshalb für eine neue Strategie. Im Juni 2009 setzte der damalige Verteidigungsminister Robert Gates mit Stanley McChrystal einen Viersternegeneral als neuen Oberkommandierenden ein, der zuvor im Irak gedient hatte. McChrystal, der selten mehr als vier Stunden schläft und täglich sieben Meilen joggt, trat dafür ein, die Taliban mit großer Aggressivität zu verfolgen.

Obama schickte 33 000 zusätzliche Soldaten, verbunden mit der Forderung an die Militärs, ein verbindliches Abzugsdatum zu nennen. Zugleich rückte der Präsident von den großen Zielen ab, die der Westen beim Einmarsch in Kabul verkündet hatte. Die USA würden „nicht versuchen, Afghanistan zu einem perfekten Ort zu machen“, sagte Obama. Es ging nun vor allem um Aufstandsbekämpfung.

Damit begann eine der blutigsten Phasen dieses Kriegs. 2009 starben in Afghanistan 2412 Zivilisten, zwei Drittel davon durch Aufständische, 25 Prozent durch Nato-Truppen und afghanische Sicherheitskräfte. Die Zahl der Operationen gegen die Taliban stieg massiv an, auf 10 bis 15 pro Nacht. Grundlage dafür waren die Listen, die die CIA und die Nato führten – Obamas Listen. „Escalate and exit“ nannten sie die Strategie im Weißen Haus, ausweiten und dann rausgehen.

McChrystals Nachfolger, General David Petraeus, hatte diese Strategie in einem Handbuch beschrieben, dem „Field Manual 3-24“ zur Aufstandsbekämpfung, das bis heute als Standardwerk gilt. Für den Kampf gegen Guerillagruppen wie die Taliban skizzierte Petraeus drei Stufen: Zunächst müsse die Führungsriege des Gegners in einer „Säuberungs“-Phase geschwächt werden. Danach sollten lokale Kräfte die eroberten Gebiete übernehmen. In der dritten Stufe war der Wiederaufbau vorgesehen. Hinter verschlossenen Türen machten Petraeus und seine Leute deutlich, was mit „Säuberung“ gemeint war. Deutsche Politiker erinnern sich an einen Satz von Michael T. Flynn, damals Isaf-Geheimdienstchef in Afghanistan. „Nur ein toter Talib ist ein guter Talib“, erklärte der Offizier den Besuchern bei einem Briefing.

Unter Petraeus begann eine gnadenlose Jagd auf die sogenannten Schattengouverneure sowie örtliche Unterstützer, die den Islamisten nahestanden. Dass die Operationen oft tödlich endeten, betrachteten die Amerikaner als Erfolg. Im August 2010 berichtete Petraeus vor Diplomaten in Kabul stolz von einer Trendwende. Als Beleg führte er eine Bilanz an, bei der manchem Botschafter mulmig wurde. Mindestens 365 Kommandeure der Aufständischen, erklärte Petraeus, seien in den vergangenen drei Monaten ausgeschaltet worden, im Schnitt etwa 4 pro Tag.

Die Existenz der sogenannten JPEL-Unterlagen (für „Joint Prioritized Effects

Präsident Obama vor Armeeangehörigen in New Jersey am 15. Dezember

List“) ist bisher nur in Auszügen beschrieben worden. In den Kriegstagebüchern der US-Armee aus Afghanistan, die WikiLeaks 2010 gemeinsam mit *New York Times*, *Guardian* und dem SPIEGEL veröffentlichte, tauchen die Einsätze von US-Spezialeinheiten zwar auf, allerdings nicht sehr ausführlich (SPIEGEL 30/2010). Die jetzt zugänglichen Dokumente ermöglichen erstmals einen systematischen Blick auf die gezielten Tötungen. Sie schildern die Kriterien, wer warum auf diese Liste geriet.

Wie kühl die Nato mitunter mit dem Leben von Verdächtigen umging, zeigt der Fall des afghanischen Soldaten Hussein, Nummer 3341 auf der Liste. Hussein stehe im Verdacht, an einem Angriff auf einen Stützpunkt der Isaf-Truppen in Helmand beteiligt gewesen zu sein, heißt es in den Unterlagen. Der Afghane, ein Unteroffizier der Armee, sei ein Überläufer und derzeit auf der Flucht. Vermutlich wolle er sich zu den Taliban absetzen.

Im Sommer 2010 setzten ihn die Nato-Leute auf die Liste, als eine von 669 Personen. Er bekam den Decknamen „Rumble“ und war fortan zur Jagd ausgeschrieben, mit der zweithöchsten Priorität.

Die Nato-Soldaten diskutierten die Vor- und Nachteile seiner Tötung. „Hussein auszuschalten bedeutete, einen fahnenflüchtigen Verräter aus den Rängen der Armee zu entfernen und zugleich zu verhindern, dass er sich den Aufständischen anschließt“, heißt es in der Bewertung. „Es wird gleichzeitig ein klares Signal an weitere potenzielle Überläufer gesendet, dass weder Isaf noch die afghanische Regierung willens sind, ein solches Verhalten hinzunehmen.“ Husseins Tötung sollte vor allem als Symbol der Abschreckung dienen.

Gegen einen tödlichen Schlag spreche allerdings, so die interne Bewertung, dass damit sämtliche Informationen, die Hussein eventuell besitze, verloren wären.

Einer Aufnahme in die Liste ging ein mitunter monatelanger Prozess voraus, Belege wurden in dieser Zeit zusammengetragen: abgehörte Telefonate, Berichte von Informanten, Fotos. Am Ende entschied der jeweilige Isaf-Regionalkommandeur, ob ein Verdächtiger gelistet wurde.

Manche der JPEL-Kandidaten wurden auch nur zur Beobachtung oder Festnahme ausgeschrieben. Erstmals enthüllen die Dokumente nun, dass die Nato 2010 sogar Atta Mohammed Noor in die Liste aufgenommen hatte, einen Gouverneur in Nordafghanistan. Der Tadschike und frühere Warlord war in den Kriegswirren durch Schmuggel reich geworden, er galt als jemand, der seine Kontrahenten rücksichtslos aus dem Weg räumt. Die Nato stufte ihn unter Nummer 1722 mit Priorität drei ein, aber sie sammelte nur Informationen über ihn, sie gab ihn nicht zum Abschuss frei.

Wenn bei einem Zugriff auch Zivilisten unter den Opfern sein könnten, musste das Isaf-Hauptquartier in Kabul eingebunden sein. „Als Faustregel galt, dass der Isaf-Kommandeur in Kabul bei einem geschätzten Kollateralschaden von bis zu zehn Zivilisten entscheidet, ob das Ziel das Risiko rechtfertigt“, sagt ein Isaf-Offizier, der jahrelang mit den Listen gearbeitet hat. Sei mit mehr möglichen zivilen Opfern zu rechnen gewesen, hatte das zuständige Nato-Hauptquartier das letzte Wort. Dabei galten Bodyguards, Fahrer und männliche Begleiter als feindliche Kämpfer, egal ob sie es wirklich waren. Nur Kinder, Frauen und Alte zählten als Zivilisten.

Diese Leitlinien, so räumen selbst beteiligte Militärs ein, waren zynisch. Wenn ein Taliban-Kämpfer dauerhaft in tödliche Anschläge verwickelt gewesen sei, habe man eine „Güterabwägung“ vorgenommen. Dann rechneten die Militärs, wie viele Menschenleben durch das „Ausschalten“ gerettet werden könnten und wie viele Zivilisten möglicherweise bei einem Luftschlag umkommen würden.

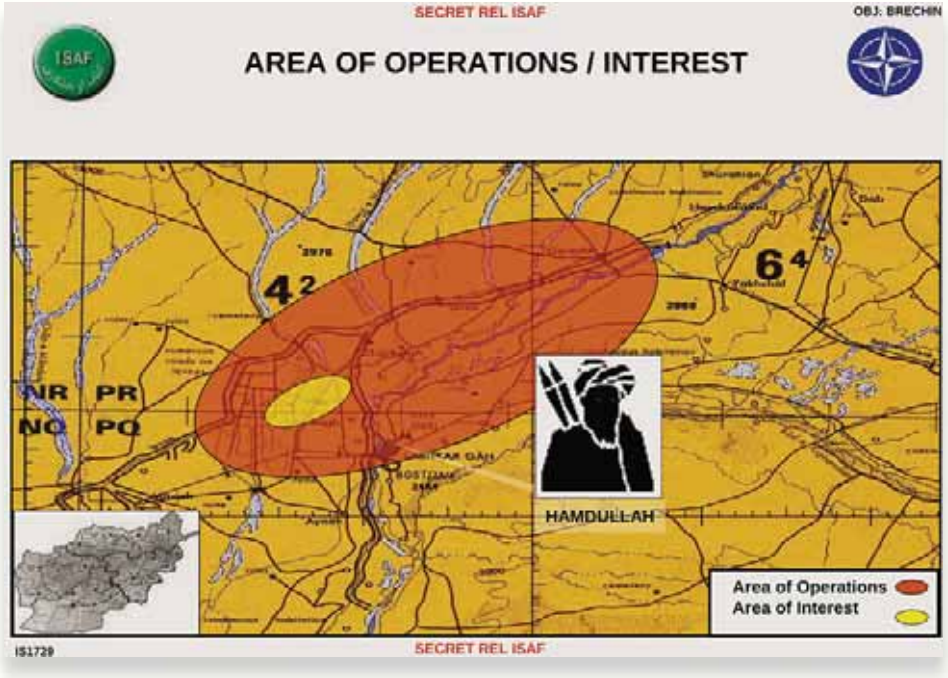
Manchmal, so legen es die Dokumente nahe, reichte schon die Ortung eines Handys, um die Militärmaschine in Gang zu setzen. Die Suche nach den Telefonsignalen der Taliban sei „zentral für den Erfolg von Operationen“, heißt es in einem britischen Geheimdossier aus dem Oktober 2010.

Rund um die Uhr suchten demnach „Predator“-Drohnen und mit Sensoren ausgerüstete britische Eurofighter die Funksignale am Hindukusch nach bekannten Mobiltelefonnummern ab, die den Taliban zugeordnet waren. Sobald die ihre Mobiltelefone einschalteten, begann die Jagd.

Auf langen Listen führten das britische GCHQ und die amerikanische NSA afghanische und pakistanische Nummern von Taliban-Funktionären. Waren die Nummern gefunden, setzte ein ausgeklügelter Mechanismus ein. Gab es von einem Kämpfer bereits eine aufgezeichnete Stimme in den Archiven, wurde diese zur Identifikation herangezogen. Passte das Muster, begannen die Vorbereitungen für eine Operation. Die Angriffe setzten den Taliban so sehr zu, dass sie ihre Kämpfer anwiesen, keine Handys mehr zu benutzen.

Aus dem Papier geht auch hervor, auf welch vager Grundlage offenbar tödliche Operationen durchgeführt wurden. Bei der Stimmidentifizierung genügte es, wenn ein Verdächtiger sich in einem überwachten Gespräch einmal namentlich identifizierte. Innerhalb der nächsten 24 Stunden galt diese Stimmenerkennung demnach als „positive Zielidentifizierung“ und damit

FOTO: JABIN BOTSFORD / THE NEW YORK TIME / REDUX / LAIF



ZIELPERSON Ein Isaf-Dokument zeigt, wie die Task Force Helmand einen Mullah der Taliban zur Zielperson macht. Der Mann galt als regionaler Kommandeur im Süden Afghanistans, der unter anderem Steuern für die Taliban eintrieb.

als Legitimation für einen Luftschlag. Die Gefahr ziviler Opfer stieg dadurch stark.

Zu den wohl umstrittensten Entscheidungen der Nato in Afghanistan zählt die Ausweitung der Operationen auf Drogenhändler. Die Drogenindustrie bringe den Taliban nach Uno-Schätzungen jährlich 300 Millionen Dollar ein, heißt es in einem Dokument der NSA. Die Aufständischen könnten „nicht besiegt werden, ohne den Drogenhandel zu unterbinden“.

Im Oktober 2008 trafen die Verteidigungsminister der Nato laut dem NSA-Dokument eine folgenschwere Entscheidung: Drogennetzwerke seien künftig „legitime Ziele“ der Isaf-Truppen. „Drogenhändler wurden zum ersten Mal in die JPEL-Liste aufgenommen“, heißt es in dem Bericht.

Nach Ansicht von amerikanischen Nato-Kommandeuren wie Bantz John Craddock war kein Nachweis notwendig, dass Drogengelder an die Taliban flossen, um Anbauer, Kuriere und Händler zu legitimen Zielen von Nato-Angriffen zu erklären.

Anfang 2009 erließ der damalige Nato-Oberbefehlshaber Craddock eine Order, wonach die Strategie der zielgerichteten Tötungen von Taliban-Kadern auf Drogenproduzenten ausgeweitet werde. Das führte zu heftigen Diskussionen innerhalb der Nato. Der deutsche Nato-General Egon Ramms erklärte den Vorstoß für „illegal“, er verletze internationales Recht.

Für die Bundesregierung birgt das streng geheime Dossier erhebliche politische Brisanz. Seit Jahren geben deutsche Behörden Mobilfunknummern von deutschen Extremisten, die sich am Hindukusch aufhalten, an die USA weiter, verbunden mit der Behauptung, für gezielte Tötungen sei das Anpeilen der Telefone viel zu ungenau.

Diese Linie ist offenkundig nicht haltbar. Sowohl die Eurofighter als auch die Drohnen, so heißt es in dem Dokument von 2010, hätten „die Möglichkeit, ein bekanntes GSM-Telefon zu lokalisieren“. Aktive Handys dienten den Spezialeinheiten demnach als präzise Peilsender.

Deutschland ist am Hindukusch Mitglied der Abhörgemeinschaft der „14 Eyes“, der 14 Augen. Dazu zählen neben den angelsächsischen Ländern auch Italien, Spanien, Belgien und die Niederlande sowie Dänemark, Frankreich, Schweden und Norwegen.

Diese Länder betreiben in Afghanistan eine eigene technische Plattform mit dem Codenamen „Center Ice“ für die Überwachung und den Austausch von Daten. Einer NSA-Präsentation aus dem Jahr 2009 zufolge fand allerdings auf „Center Ice“ nicht nur bei Handygesprächen ein enger Austausch statt, sondern auch bei Informationen zu Zielen.

Der BND räumte auf Anfrage zwar die Weitergabe von Mobilfunknummern via „Center Ice“ ein, bestritt aber, dass diese zur Zielerfassung von Drohnen taugen. Zudem würden keine Daten weitergegeben, wenn die „schutzwürdigen Interessen der/des Betroffenen das Allgemeininteresse an der Übermittlung überwiegen“. Seit 2005 liefern die Deutschen zudem keine Informationen mehr, mit denen Profile für den Zugriff aufgebaut werden.

Die restriktive Linie hat zu diversen Friktionen mit den Amerikanern geführt. Wenn das von der Bundeswehr geführte Regionalkommando Nord einen Verdächtigen für die JPEL-Unterlagen nominieren wollte, musste erst eine detaillierte Akte mit Beweisen zum Einsatzführungskommando nach Potsdam und schließlich ans Ministerium geschickt werden. Als Kriterium für die Aufnahme galt, dass die Zielperson an Anschlägen beteiligt gewesen, sie angeordnet oder vorbereitet haben musste. Mehrfach drängten die Deutschen darauf, Verdächtige wieder zu streichen. Im September 2010 entfielen nur 11 der 744 Ziele auf das von den Deutschen kontrollierte Nordafghanistan. „Wir Deutschen haben einen Stabilisierungseinsatz geführt und die Amerikaner einen Krieg“, sagt der pensionierte General Ramms.

Die vertraulichen Dokumente könnten nun ein juristisches Nachspiel haben. Die Menschenrechtsorganisation Reprieve erwägt juristische Schritte gegen die britische Regierung. Für besonders relevant erachten die Reprieve-Leute, dass sich auf den Listen Pakistaner befinden, die sich auch in Pakistan aufhielten. „Die britische Regierung hat wiederholt beteuert, dass sie keine pakistanischen Ziele angreift und dort keine Luftschläge ausführt“, sagt Reprieve-Anwältin Jennifer Gibson. Zudem zeigten die Dokumente, dass der „Krieg gegen den Terror“ faktisch mit dem „Krieg gegen Drogen“ verschmolzen worden sei. „Das ist rechtlich äußerst problematisch.“

Die Isaf, welcher der SPIEGEL eine Liste der vertraulichen Dokumente vorlegte und die er um Stellungnahme bat, möchte dazu grundsätzlich keine Fragen beantworten, aus „operativen Sicherheitserwägungen“, wie ein Sprecher sagt. Isaf-Einsätze entsprächen internationalem Recht. Das US-Verteidigungsministerium verweist an Isaf.

Von der kommenden Woche an beginnt in Afghanistan ein neues Kapitel. Die Nato-Truppen sind weitgehend abgezogen, eine neue Regierung ist gewählt. Die Afghanen müssen nun selbst entscheiden, wie ihre Zukunft aussehen soll. Der Westen hat einige seiner Ziele erreicht: Osama Bin Laden ist tot, al-Qaida zumindest in Afghanistan geschlagen. Aber die Taliban sind nicht besiegt, mit dem Anschlag auf eine pakistanische Schule haben sie ihre Schlagkraft bewiesen. Eine Befriedung des Landes ist ohne ihre Einbindung nicht möglich.

Eine CIA-Studie aus dem Juli 2009, die sich mit gezielten Tötungen von hochrangigen Funktionären des Feindes weltweit beschäftigt, kommt zu einem bitteren Fazit. Wegen der zentralen, aber flexiblen Führung der Taliban und der egalitären Stammesstrukturen seien die gezielten Tötungen in Afghanistan nur mäßig erfolgreich gewesen. In dem CIA-Papier heißt es: „Die Taliban haben eine hohe Fähigkeit, ausgeschaltete Führer zu ersetzen.“

Jacob Appelbaum, Matthias Gebauer, Susanne Koelbl, Laura Poitras, Gordon Repinski, Marcel Rosenbach, Holger Stark