

Algorithmen und Agenten

Wo es gerade in Deutschland bei der Geheimdienstarbeit hapert

Peter Neumann | **Nicht nur die National Security Agency (NSA) steht seit den Enthüllungen Edward Snowdens unter Beschuss – weltweit sehen sich Geheimdienste mit Entwicklungen konfrontiert, die ihre Leistungsfähigkeit untergräbt oder infrage stellen. Will Deutschland eine größere Rolle in der Welt spielen, führt an einem Ausbau der Kapazitäten kein Weg vorbei.**

Westliche Geheimdienste stehen in jüngster Zeit in der Kritik. Warum, so lautet zum Beispiel der Vorwurf, haben sie nicht die Annexion der Krim durch Russlands Präsidenten Wladimir Putin vorausgesehen? Oder den Vormarsch des so genannten Islamischen Staates?

Wissen und Nichtwissen

Man muss wohl zwischen langfristigen – oder strategischen – und kurzfristigen Entwicklungen unterscheiden. Beispiel Arabischer Frühling: Dass die Situation in vielen arabischen Ländern kritisch war und ist, angesichts einer ganzen Reihe ungelöster Probleme und der tickenden demografischen Zeitbombe, wurde durchaus erkannt, ebenso Putins strategische Absicht, eine russische Quasi-Vorherrschaft über den gesamten postsowjetischen Raum zu etablieren. Bestimmte Ereignisse beziehungsweise das taktische, kurzfristige Handeln lassen sich oft kaum richtig voraussagen, was im Fall der Krim-Annexion auch daran gelegen haben mag, dass die Akteure dies selbst so nicht langfristig geplant hatten. Hier verläuft eine wichtige Linie, was Geheimdienste überhaupt leisten können und was nicht.

Allerdings ist auch richtig, dass aufgrund der geänderten Weltlage seit den Anschlägen vom 11. September 2001 in bestimmten Bereichen wie der Russland-Aufklärung abgerüstet wurde beziehungsweise ein Großteil der Ressourcen auf den internationalen Terrorismus und den Mittleren Osten konzentriert wurden – was womöglich ein Fehler war. Und wenn man nicht wie die USA gleichzeitig die Geheimdienst-Etats stark ausbaut, bedeutet das, dass man in anderen Bereichen sparen muss, und das sollte eigentlich der Vorwurf sein: Gegenüber Russland fehlt es uns schlicht an Kapazitäten. Dabei geht es nicht um die Klage, die nach dem „11. September“ oft zu hören war: Wir brauchen mehr „human intelli-

gence“ (HUMINT), also klassische Spionagearbeit mit menschlichen Quellen möglichst nah am Geschehen, und weniger „signal intelligence“ (SIGINT), also primär technische Aufklärung! Im Gegenteil: SIGINT wird sogar noch wichtiger werden, denn die Menschen kommunizieren immer mehr elektronisch.

Viele Gespräche, die früher per Festnetztelefon oder auch von Angesicht zu Angesicht geführt wurden, werden heute per Mobiltelefon und elektronisch, per E-Mail, Chat, Skype, Message Board und so weiter geführt.

Das Volumen der elektronischen Kommunikation hat unglaublich zugenommen, und zu sagen, wir sollten zukünftiger weniger in die elektronische Kommunikationsüberwachung investieren, wäre kompletter Unsinn. Natürlich ist es auch weiterhin wichtig, Informanten zu rekrutieren, klassische

HUMINT zu betreiben und Quellen zu unterhalten, die einem den Kontext liefern können, dank dem man die elektronische Kommunikation überhaupt erst verstehen kann. Aber HUMINT gegen SIGINT auszuspielen, wäre völlig falsch.

Das große Problem bei der technischen Aufklärung ist, dass wir in Daten zu ertrinken drohen – ein Vorwurf vor allem an die Adresse der NSA: Es wird unglaublich viel gesammelt, ohne dass überhaupt entsprechende analytische Kapazitäten vorhanden sind, alle diese gesammelten Informationen auch auszuwerten. Das ist aber nicht allein ein Problem der NSA, sondern ein grundsätzliches: Wir haben noch nicht die Methoden gefunden, um mit diesen speicherbaren Informationen angemessen umzugehen – und tatsächlich die Informationen zu finden, nach denen wir suchen. Dafür müssen wir zum einen in technisch leistungsstärkere Systeme investieren. Gerade Deutschland muss hier viel tun, die Amerikaner sind uns weit voraus. Zum anderen ist aber auch klar, dass es für die Suche im Heuhaufen nicht die technische Lösung gibt – der Mensch muss genauso eine Rolle spielen. Die Datensuche sollte von menschlichem Wissen, von kompetenten Analytikern geleitet werden, die sich mit den Themen auskennen. Der Computer kennt sich nicht aus, aber er kann viel Arbeit abnehmen. Man braucht also Algorithmen und menschliche Erfahrung.

Der Mensch muss da zum Zuge kommen, wo er am stärksten ist: bei der Herstellung von Kontexten, dem Erkennen „schwarzer Schwäne“, dem Einschätzen einer bestimmten Situation. Die Computerfirma oder der Nachrichtendienst, die dieses Zusammenspiel am besten lösen, werden diejenigen sein, die unglaublich viel Geld verdienen beziehungsweise über die besten Erkenntnisse verfügen werden. Für die Stecknadelsuche in immer größeren Heuhaufen brauchen wir diese Kombination von technischer Stärke, die es erlaubt, einen Heuhaufen schnell zu reduzieren, und dann die menschliche Kompetenz, das Verbleibende richtig zu deuten. Genau diese Zusammenarbeit zwischen Mensch und Computer, das ist meiner Ansicht nach eine der wichtigsten Herausforderungen überhaupt, die wir zu bestehen haben.

Weniger in elektronische Überwachung zu investieren, wäre Unsinn

Inneres und Äußeres, Kontrolle und Effizienz

Die Unterscheidung von inneren und äußeren Angelegenheiten – was aus staatlicher Sicht insgesamt weiterhin sinnvoll ist – wird von vielen Gegnern

oder Leuten, über die wir mehr wissen wollen, nicht mehr respektiert. Mit anderen Worten: Transnationale terroristische Netzwerke scheren sich nicht darum, ob sie nun in die Kategorie „innen“ oder „außen“ fallen – und das ist ein Problem für die Geheimdienstarbeit. Deshalb muss man neue Wege finden, wie Polizei beziehungsweise Inlands- und Auslandsgeheimdienst zusammenarbeiten können – was teilweise durch gemeinsame „Zentren“ schon gelöst ist, in Deutschland beispielsweise durch das gemeinsame Terrorabwehrzentrum. Solche Zentren wird es zukünftig wohl auch für weitere Bereiche geben.

Geht es um das Ausforschen bestimmter Szenen oder Gruppierungen, die Verbindungen zum Ausland unterhalten, sind die Art und Weise, wie die Dienste derzeit vorgehen – in Deutschland der Verfassungsschutz, zum Teil auch die Polizei –, alles in allem durchaus angemessen. Die große Herausforderung ist aber, dass Szenen und „communities“ heutzutage eben nicht mehr nur tatsächlich an bestimmten Orten existieren, sondern dass es sie genauso virtu-

Die dschihadistische „community“ existiert vor allem virtuell

ell gibt. Menschen leben ihr Leben nicht nur an bestimmten Orten, sondern zum Beispiel auch in den sozialen Medien: Das dschihadistische Milieu existiert in manchen Städten, vor allem aber virtuell – womit wir erneut bei den großen Fragen der elektronischen Aufklärung wären: Wo verlaufen zum Beispiel die Grenzen bei der Auswertung sozialer Medien? Wie sieht es dort aus mit der Trennung nach Ausland und Inland, welche Regeln sollen gelten? Das ist noch überhaupt nicht definiert.

Denn stärker als jedes Terroristennetzwerk sprengt das Internet jegliche Definition, die wir von Staatlichkeit haben und auch davon, was privat ist und was nicht. Ist zum Beispiel eine Facebook-Seite privat, wenn sie uns allen Fotos zugänglich macht? Warum sollte sich das ein Geheimdienst nicht anschauen dürfen? Ist Facebook praktisch wie eine Zeitung, oder fallen die darauf ausgetauschten Nachrichten in den Bereich privater Kommunikation? All das ist ungeklärt und stellt Geheimdienste vor Probleme.

Den rechtlichen Rahmen zieht zudem nicht der Gesetzgeber, sondern die Gerichte – wie bei der Entscheidung des Europäischen Gerichtshofs, dass eine E-Mail eben nicht wie ein Brief zu werten ist, was bedeutet, dass E-Mail-Dienste wie Gmail, GMX, Yahoo oder Hotmail nicht für deren Inhalt haftbar sind. Was aber, wenn eine Website wie eine Zeitung anzusehen ist? Muss dann der Betreiber der Webseite oder die Firma, die sie hostet, auch die Verantwortung dafür übernehmen? Wie sieht es mit Diskussionsforen und Kommentarspalten aus? In bestimmten Fällen könnte das bedeuten, dass man einen Internetserviceanbieter wegen bestimmter Inhalte verklagen kann. In den Vereinigten Staaten wurde dies allerdings bereits in den neunziger Jahren rechtlich ausgeschlossen.

Die rasante Entwicklung des Internet hin zu einem sozialen Medium wirft ständig neue Fragen auf, bei denen der Gesetzgeber kaum mithalten kann. Diese Themen betreffen Geheimdienste direkt, zum Beispiel, wenn es darum geht, wer in welchem Maße abgehört oder beobachtet werden darf. Ist es entscheidend, ob die Zielpersonen in Deutschland sitzen oder ob der Chatroom in

Bild nur in Printausgabe verfügbar

Deutschland gehostet ist? Ist der Chatroom beispielsweise in Amerika gehostet, handelt es sich dann um „Ausland“, mit entsprechend anderen Regeln, selbst wenn die Zielpersonen tatsächlich in Deutschland sitzen? Die gewaltigen Grauzonen, die derzeit existieren, hat sich die NSA sehr zunutze gemacht; der Klärungsbedarf ist immens.

Transparenz und Nachwuchssorgen

Ein weiteres großes Thema für Geheimdienste ist Offenheit. In Großbritannien beispielsweise unterlag noch vor 20 Jahren die bloße Existenz des Inlandsgeheimdiensts MI5 der Geheimhaltung. Heute stehen die Dienste viel mehr im Licht der Öffentlichkeit und entwickeln sich langsam zu öffentlichen Institutionen. Zugleich wird Geheimdiensten gerade im Internet – häufig irrtümlich – unheimlich viel Macht zugeschrieben, und deshalb besteht heute auch ein größeres Bedürfnis, dass sich die Geheimdienste selbst erklären und ihre Schritte rechtfertigen. Dass es das lange gar nicht gegeben hat, hat meiner Meinung nach Verschwörungstheorien Vorschub geleistet. Hier müssen die Geheimdienste völlig umdenken – was in den Vereinigten Staaten zum Teil schon passiert ist und in Großbritannien gerade anfängt, während man in Deutschland und anderen kontinentaleuropäischen Ländern davon im Prinzip noch nichts gemerkt hat.

Die Offenheit ist aber auch wichtig in einer anderen Hinsicht: Geheimdienste können die ganze Expertise, die gerade im technischen Bereich gebraucht wird, nicht mehr intern bereitstellen. Ob sie wollen oder nicht: Geheimdienste müssen heute verstärkt mit der privaten Wirtschaft, beispielsweise mit Software- und Computerfirmen, zusammenarbeiten. Diese verfügen über Expertise, die so spezialisiert ist, dass man sie innerhalb einer Bürokratie nicht

so schnell nachzuchten kann. Und die Topleute in der Informatik sind übrigens oft auch nicht diejenigen, die besonders daran interessiert sind, für eine staatliche Bürokratie und 2000 Euro im Monat zu arbeiten.

Das bedeutet: Wenn Geheimdienste „up to date“ bleiben wollen, müssen sie sich dem IT-Sektor öffnen. In den USA hat das schon zu Problemen – Stichwort: Edward Snowden – geführt, denn es wurde zu weit getrieben; in Deutschland hat man genau das umgekehrte Problem, nämlich dass eine solche Öffnung bis-

Die Geheimdienste müssen sich dem IT-Sektor öffnen

lang so gut wie gar nicht betrieben wurde. Heute müssen die Geheimdienste flexibler und offener werden und Regeln dafür entwickeln, wie sie mit privaten Dienstleistern zusammenarbeiten – und sicherstellen, dass diese Dienstleister dann keine Geheimnisse verraten. Ein anderes Problem ist, dass man Informationen an private Dienstleister weitergibt, die im Prinzip in der staatlichen Hoheit bleiben sollten. Dafür muss man Regeln schaffen, die auch vom Gesetzgeber absegnet werden müssen.

Die Geheimdienste sind dabei in einer schwierigen Lage: Auf der einen Seite will man als Bundesnachrichtendienst (BND) oder Bundesverfassungsschutz nicht abgehängt werden, auf der anderen Seite begibt man sich in Abhängigkeiten und setzt sich der Gefahr aus, viele potenzielle Snowdens zu schaffen. Aber ich glaube, dass die Nachrichtendienste kaum eine Wahl haben werden, denn sie haben nicht die Möglichkeit, solche Kapazitäten speziell im technischen Bereich selbst aufzubauen – weil starke Bürokratien nicht so besonders schnell und flexibel sind und weil man nicht so leicht die Art von Leuten rekrutieren kann, die bei großen Computerfirmen arbeiten.

Dabei wird es zukünftig auf die richtige Mischung ankommen: auf Leute mit großer Fremdsprachenkompetenz, die sich mit bestimmten Regionen sehr gut auskennen, dort auch schon mal gelebt haben, die sich auch in unterschiedlichen Kulturen wohlfühlen – oder eben im Internet, das ja praktisch eine Region für sich ist. Kurzum: Wir reden von Menschen, für die eine klassische Beamtenlaufbahn nicht unbedingt so attraktiv ist. Die Idee, dass man sich auf ein Leben in einem „Dienst“ festlegt, mit 35 Jahren bis zur Pensionierung – das ist nicht unbedingt etwas, das die heutige junge Generation anspricht, gerade die Spitzenkräfte aus der IT-Branche, die viele andere Möglichkeiten haben. Da wird man sich etwas Neues überlegen müssen, wenn man weiterhin gute Leute bekommen will.

Kooperation und Eigenleistung

Der Grund, warum Deutschland nicht robuster gegen die NSA-Aktivitäten im eigenen Land vorgegangen ist, ist einfach: Deutschland ist von der NSA abhängig. Wie auf anderen Gebieten der kollektiven Sicherheit auch hat sich Berlin über Jahrzehnte hinweg in eine Position begeben, in der Deutschland von den Kapazitäten anderer profitiert, speziell denen der USA; so konnte die Bundesrepublik viel Geld sparen.

Das funktioniert natürlich nur so lange, wie man der Meinung ist, dass die größten Gegner die gleichen sind, und es keine Interessenkonflikte gibt. Jetzt

gab es diesen ersten Konflikt, und Deutschland war im Grunde hilflos. Wer sich aber in die Abhängigkeit anderer begibt, der darf sich nicht darüber beschweren, wenn diese Abhängigkeit auch mal ausgenutzt wird. Und wer weniger abhängig werden will, muss auch bereit sein, die eigenen Kapazitäten auszubauen. Derzeit ist es so, dass Deutschland ohne die Informationen von Partnerdiensten wahrscheinlich nicht in der Lage wäre, zum Beispiel in der Terrorismusbekämpfung das zu leisten, was es tut. Schon daraus folgt: Deutschland muss mehr in seine Dienste und insbesondere in die Kommunikationsüberwachung investieren.

Das heißt natürlich nicht, dass man weniger mit befreundeten Diensten zusammenarbeitet – im Gegenteil: Je mehr Eigenkapazität man mitbringt, desto größer ist das Interesse anderer, mit einem zu kooperieren; man kann ja etwas zum Tausch anbieten. Was wir derzeit haben, zum Beispiel im elektronischen Bereich, ist nicht „intelligence pooling“, sondern Abhängigkeit. Das heißt: Die Deutschen erhalten Informationen von den Amerikanern, die Amerikaner kommen uns entgegen, weil sie glauben, dass es auch in ihrem Interesse ist, dass es in Deutschland nicht zu Terroranschlägen kommt. Das ist gut so und soll auch lange so weitergehen – aber das ist kein „intelligence pooling“. Wenn jemand nichts anzubieten hat, dann sagt man sich doch als Brite oder Franzose: Warum soll ich überhaupt mit dem BND kooperieren?

Hinzu kommt, dass der BND keine ausreichenden Kapazitäten hat, die es ihm erlauben würden, langfristig an Länder heranzugehen, in denen momentan keine Krise herrscht und in die keine deutschen Truppen entsandt sind. Der BND kümmert sich heute in erster Linie um Länder, in denen Bundeswehrsoldaten aktiv sind, also vor allem Afghanistan und ein paar andere Länder. Auf einer zweiten Stufe stehen Länder, die wegen bestimmter Fragen oder Krisen von besonderem Interesse sind, zum Beispiel der Iran oder der Irak. Und das war es dann auch schon. Der BND verwendet so viel Energie darauf, die Situation in Afghanistan im Auge zu behalten, dass er nur noch wenig Zeit und Kapazitäten übrig hat, sich zum Beispiel anzuschauen, wo es in zehn oder 15 Jahren einen Konflikt geben könnte.

In den meisten Ländern der Welt tut der BND im Prinzip nicht mehr, als Zeitungen zu sammeln und Artikel auszuschneiden – statt Leute zu rekrutieren und jene langfristige strategische Arbeit zu leisten, die es dem Dienst im Krisenfall ermöglichen würde, auf Quellen zurückzugreifen und kompetente Antworten zu geben. Das ist mit dem Budget, das dem BND zur Verfügung steht, schlicht nicht möglich.

Deutschlands neue Rolle

Von Deutschland wird heute mehr erwartet als noch vor 20 Jahren. Außenpolitisch heißt das, dass Berlin sich mit praktisch allen Regionen der Welt auskennen und überall Positionen vertreten können muss; und wenn es an Konflikten nicht teilnimmt, so müsste es zumindest einen kreativen Ideenbeitrag

In den meisten Ländern
der Welt sammelt der BND
lediglich Artikel

**Geheimdienste, die
alles zu wissen meinen,
verstehen oft nichts**

leisten können. Deutschlands eigene Vorstellung von Außenpolitik beschränkte sich bislang auf Folgendes: „Wir kümmern uns ein bisschen um Europa, das ist der Kontinent, wo wir involviert sind.“ Nun sagen plötzlich die Franzosen und die Briten: „Deutschland muss auch mal in Afrika aktiver werden.“ Aber worin bestehen denn zum Beispiel die deutschen nachrichtendienstlichen Kapazitäten in Afrika? Mit wie vielen Ländern kennen wir uns wirklich aus? Welche Länder außer vielleicht Somalia und Kenia hat sich denn der BND tatsächlich näher angeschaut in den vergangenen Jahren?

Vom Nachteil und Nutzen der Demokratie

Geheimdienste in autoritären Staaten haben es natürlich in gewisser Weise leichter als die in demokratischen Staaten – und eine Karriere in ihnen ist ungleich prestigeträchtiger. Die Geheimdienstler sind mächtige Leute, die zur Elite eines Landes gehören, die die Politik manipulieren und mitbestimmen können und die gefürchtet werden. Als hoher Mukarabat-Beamter in Ägypten sind Sie ein unglaublich wichtiger Mann – überhaupt nicht zu vergleichen mit einem BND-Abteilungsleiter, der noch nicht einmal über seine Arbeit sprechen darf.

Aber ich denke nicht, dass das wirklich ein Wettbewerbsnachteil ist. Denn Staaten, die keine übermächtigen Geheimdienste haben, funktionieren im Großen und Ganzen besser. Zudem schützt es vor Paranoia. Wir wissen ja aus unserer eigenen Geschichte, dass gerade die Geheimdienste, die glauben, alles zu wissen, letztlich nichts verstehen. Das war im Grunde die Geschichte der DDR-Staatssicherheit: Die Stasi hat ja ihre eigene Opposition gesteuert – aber letztlich dann eben doch nicht.

Deutschland braucht dringend leistungsfähigere Geheimdienste. Aber das bedeutet nicht, dass es wünschenswert wäre, dass Geheimdienste in Deutschland übermächtig werden, zu einem Staat im Staate. Da müssen wir immer wachsam bleiben.



Peter Neumann
ist Professor of Security Studies am King's College London und Gründungsdirektor des International Centre for the Study of Radicalisation (ICSR).