Deutsche Sicherheitspolitik, Bundeswehr und CyberWarfare

Siegen, FiFF-Tagung, 26.10. 2013

Gliederung:

- Deutschland und der Krieg gegen den Terror
- NATO-Truppenstatut
- SIGINT-Programm der Bundeswehr
- Neuorganisation des militärischen Nachrichtenwesens
- Bundeswehr und Cyber-Warfare

In der jüngsten Vergangenheit hatten wir es im Zusammenhang mit der NSA-Abhöraffäre insbesondere mit drei Aufregern zu tun:

a) Der Ausspionierung des Handys der Bundeskanzlerin.
b) Der Kooperation deutscher Dienste wie Verfassungsschutz und Bundesnachrichtendienst mit dem US-amerikanischen Geheimdienst NSA, bei der große Datenmengen weitergegeben wurden, was vorgeblich im Rahmen des Anti-Terrorkampfes dringend nötig gewesen sei.
c) Und in diesem Rahmen insbesondere die Weitergabe von Daten, um Drohnenangriffe gegen vermeintliche Terroristen (v.a. in Pakistan) optimieren zu können. Damit war unweigerlich die Frage verknüpft, inwieweit zumindest von einer indirekten Beteiligung deutscher Behörden an extralegalen „gezielten Tötungen“ ausgegangen werden müsse.

Die Aufregung war nachvollziehbar, war aber – sofern von offiziellen Stellen die Rede ist, aber auch von Teilen der Medien – nicht frei von Bigotterie. Dass Deutschland am „Krieg gegen den Terror“, den der damalige US-Präsident George W. Bush nach den Terroranschlägen 2001 ausgerufen hatte, nicht unbeträchtlich beteiligt war, war doch bekannt. Es war die böse aber konsequente Folge des Kanzler-Wortes von der „uneingeschränkten Solidarität“. Dass aus Kreisen der US-Administration lapidar auf Übereinkünfte in diesem Rahmen hingewiesen wurde, war daher nur folgerichtig. Denn man konnte, ja musste davon ausgehen, dass zwischen den sog. Nachrichtendiensten Vereinbarungen getroffen worden waren, die weit über die in diesem Milieu üblichen Deals (Do ut des; Gib´ und dir wird gegeben) hinausgingen.

1. Inwieweit ist Deutschland am Anti-Terror-Krieg beteiligt?

Die Beteiligung an dem von den USA geführten Anti-Terrorkrieg hatte immer verschiedene Seiten: Gesetzgeberisch und damit in der Politik nach innen, wurden die empfindlichen Einschränkungen demokratischer Freiheitsrechte, die in den USA mit dem US Patriot Act vorgemacht wurden, cum grano salis hier übernommen. Nach außen war die Bundesrepublik bereit, sich an bestimmten Formen der Terrorbekämpfung zu beteiligen, z.B. am Krieg in

Afghanistan, auch durch den Einsatz militärischer Spezialkräfte. Insgesamt war man bereit, das militärische und geheimdienstliche Zusammenwirken bei der Bekämpfung der Terroristen (bzw. derjenigen, die man entsprechend zuordnete) intensiv zu betreiben.

Dabei bewegte man sich gerne in Grauzonen und bevorzugte doppelbödiges Agieren: Von manchen Exzessen des War On Terror setzte man sich rhetorisch ab und erklärte im Zweifelsfalle auch, dass man sich nicht überall beteiligen müsse. Aber auf lauteren Widerspruch wurde bewusst verzichtet und das Mitmachen bei den diversen Unternehmungen wollte man nicht aufgeben. Die heutigen Absetzbewegungen von den NSA-Abhöraktionen entbehren daher nicht der Scheinheiligkeit.

Die illegalen Praktiken des „War On Terror", wie die geheimen Verschleppungen (rendition flights) und Folterungen hat man lange Zeit stillschweigend hingenommen, bestenfalls zwischen den Zeilen kritisiert, sich aber auch, wie im Falle des Bremers Murat Kurnaz, direkt in schlimme Dinge verstrickt. Den US-geführten Irak-Krieg hat man offiziell nicht mitgetragen, hinter den Kulissen aber Unterstützungsleistungen erbracht. Während man sich rhetorisch mehr und mehr vom Anti-Terrorkrieg absetzte, hat man sich noch bis ins Jahr 2010 an der völkerrechtlich unhaltbaren Mission „Enduring Freedom" in Afghanistan beteiligt. An der maritimen Anti-Terror-Mission Active Endeavour im Mittelmeer ist man trotz öffentlich immer wieder bekundeten Unbehagens bis heute beteiligt. Bei den Verhandlungen vorm Bundesverfassungsgericht über den Einsatz der Tornado-Aufklärungsflugzeuge, legte die Bundesregierung größten Wert auf die Feststellung, diese Flugzeuge kämen nur im Rahmen des völkerrechtlich gesicherten ISAF-Mandats zum Einsatz, und ISAF und Enduring Freedom blieben streng getrennt. Wie sich eine solche Trennung vor Ort „on the ground" tatsächlich aufrechterhalten ließ, bleibt bis heute ein Buch mit sieben Siegeln.

Vor allem in Afghanistan operierten bestimmte deutsche Militär-Einheiten auch im Grauzonenbereich. Was die speziellen Task Forces im Einzelnen getan haben, worin sie sich beteiligten, woran nicht, ist nicht restlos aufzuklären. Denn diese Spezialeinheiten haben ihrerseits immer eng mit den US-Special Forces agiert. Tatsache ist zum Beispiel, dass sich die Bundesrepublik an der Erstellung von Listen besonders übler und gefährlicher Feinde in Afghanistan beteiligt hat. Diese JPALS-Listen waren die Grundlagen für Militäroperationen, in denen vermeintliche Terroristen gefangengenommen („Capture") oder getötet („Kill") wurden. Bis heute steht die Aussage der politischen und militärischen Führung der Bundeswehr, dass man sich nicht an Aktionen beteiligt habe, bei denen es darum gegangen sei, Terroristenführer vorsätzlich und gewaltsam auszuschalten. Die Bundeswehr nehme nur fest und überstelle die gefangen Genommenen an die afghanischen Autoritäten, so die offizielle Lesart. Diese Version wird hier auch gar nicht bestritten (sofern nicht andere Beweise auftauchen), aber die offene Frage ist, wie weit die Kooperation mit den US-Akteuren reichte und damit die indirekte Verantwortung für illegale Praktiken? Was bedeuten die indirekten Hilfe- und Unterstützungsleistungen, wie die de facto Absicherung eines Operationsraumes, die Weitergabe von Daten über mögliche Gegner und deren Aufenthalte, konkret? Reicht es, dann die Hände in Unschuld zu waschen?

Bis heute ist ungeklärt, ob an der Durchführung von Killeroperationen mittels Kampfdrohnen US-Militärkommandos auf deutschem Boden involviert waren und sind. Es fällt schon auf, dass die verschiedenen Bundesregierungen dieser Art der Kriegführung, insbesondere in

Pakistan, keinen nennenswerten politischen Widerstand entgegengesetzt haben. Immerhin äußerten zu Beginn des Jahres 2013 die Bundestagsfraktionen der SPD und Grünen, neben den bereits früher aktiven LINKEN, schwerste völkerrechtliche Bedenken gegen die „targeted killing"-Operationen und forderten die Regierung auf, sich für die sofortige Beendigung dieser Einsätze zu verwenden.

Dies führt zu Punkt Zwei:

2. Was ist nach dem NATO-Truppenstatut erlaubt?

In der Öffentlichkeit wurde vor einiger Zeit zum Thema, ob die Einsätze mit bewaffneten Drohnen zur gezielten Ausschaltung vermeintlicher oder tatsächlicher Terror-Anführer auch von deutschem Boden aus koordiniert werden und inwieweit eine solche Praxis, so sie denn belegbar ist, mit internationalem und nationalem Recht vereinbar sei.

Was die Sachlage betrifft, ist zumindest davon auszugehen, dass das zur Zeit in Stuttgart angesiedelte Afrika-Kommando der US-Streitkräfte – AFRICOM – an den Drohnen-Einsätzen (Djibouti, Niger) in welcher Form auch immer beteiligt ist. Auch dürften Militärstrukturen im pfälzischen Ramstein bei der Datenübermittlung involviert sein.

Die Bundesregierung hat auf entsprechende Anfragen der Bundestagsfraktion der LINKEN in der vergangenen Legislaturperiode eher ausweichend geantwortet.

Ja, die Einrichtung des entsprechenden Regionalkommandos sei 2007/2008 mit dem Einverständnis der Bundesregierung erfolgt. Die rechtlichen Grundlagen dafür lägen im Vertrag über den Aufenthalt ausländischer Streitkräfte aus dem Jahre 1954; die Rechte und Pflichten der Streitkräfte aus NATO-Staaten ergäben sich aus dem NATO-Truppenstatut aus dem Jahre 1951 bzw. des Zusatzabkommens zum Truppenstatut aus dem Jahre 1959.[1] Im übrigen träfe es zu, dass die Bundeswehr Verbindungskommandos zu den jeweiligen US-Führungsstrukturen unterhalte, so auch zum AFRICOM. Aber Zugang zu klassifizierten US-Informationen habe man darüber nicht. Dieses Eingeständnis, dass man eigentlich keine ausreichende Informationsgrundlage habe, hindert die Bundesregierung nicht daran, festzustellen, dass ihr „*keine Anhaltspunkte*" dafür vorliegen, „*dass sich die Vereinigten Staaten auf deutschem Staatsgebiet völkerrechtswidrig verhalten hätten*."[2] Über diesen Blankoscheck dürfte man sich in Washington freuen.

Nach Darstellung der US-Regierung habe es keinen Einsatz bewaffneter Drohnen von deutschem Boden aus gegeben, sagt die Bundesregierung. Aber genau darum ging es nie. Sondern darum, inwieweit auf deutschem Boden befindliche militärische Infrastruktur der US Army an ungesetzlichen Drohnenangriffen in Angriffe beteiligt war oder nicht. Und der

---

1 Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion Die LINKE, Zur Rolle des in Deutschland stationierten United States Command bei gezielten Tötungen durch US-Streitkräfte in Afrika, Dt. Bundestag, Drs. 17/14401 vom 18.07.2013

2 Ebd., S.4

blauäugige Hinweis der Bundesregierung, dass sich die US-amerikanische Bündnispartner und deren Streitkräfte jederzeit an die bestehenden völkerrechtlichen Normen und Gesetze halten würden, ist vor dem Hintergrund von Guantanamo, „rendition flights“ und „waterboarding“ mehr als überraschend.

Richtig ist zumindest, dass sich das NATO-Truppenstatut auf die strikte Beachtung völkerrechtlicher Normen und Regeln bezieht und sich dem auch die US-Streitkräfte in der Bundesrepublik unterwerfen müssten. Und richtig ist auch, dass die USA im Rahmen des NATO-Truppenstatuts und einschlägiger Zusatzabkommen, militärische Strukturen wie die Kommandozentrale zur Raketenabwehr in Ramstein aufbauen dürfen – solange man sich in der Praxis ans Völkerrecht hält. Noch Fragen? Der offene Punkt bleibt, inwieweit diese Einrichtungen noch im Rahmen des NATO-Verteidigungsauftrages oder ohne entsprechende rechtliche Grundlagen tätig sind.

Leider wurde eine entsprechende Klage von Bürgern aus dem Raum Kaiserslautern jüngst vom Verwaltungsgericht Köln zurückgewiesen, vor allem weil es keine besondere Interessenbetroffenheit des Klägers meinte, erkennen zu können. Immerhin führte das Gericht aus:

„*Dementsprechend sind völkerrechtlich sehr bedenklich wissentliche Unterstützungsleistungen seitens der Bundesrepublik zugunsten der USA durch Gewährung von Überflugrechten und der Nutzung von im Inland gelegenen Militärstützpunkten. Soweit die USA diese nicht innerhalb des NATO-Rahmens und des Völkerrechts, sondern für völkerrechtswidrige Handlungen nutzen sollten*.“[3]

Und demzufolge müssten deutsche Behörden genau prüfen, ob bei solchen Militäreinsätzen von deutschem Boden aus gegen Völkerrecht verstoßen würde. In diesem Fall müsste die Benutzung deutschen Luftraums untersagt werden. Diese möglichst abstrakt gehaltenen und daher windelweichen Formulierungen besagen zumindest eines: Hier ist dringender weiterer (rechtlicher) Klärungsbedarf. Und: Die Auseinandersetzung muss politisch weitergeführt werden, auch weil die Drohnenattacken weitergehen.

Spionage nur Sache der US-Amerikaner?

In der aufgeregten öffentlichen Debatte wurde bisweilen so getan, als seien die Abhör- und Spionageaktionen der NSA ein exklusives US-amerikanisches Betätigungsfeld. Rechtfertigende Stimmen wiesen dagegen lapidar darauf hin, dass Spionage schließlich von nahezu allen Staaten der Welt betrieben würde. Dies gelte für den wirtschaftlichen wie den militärischen Bereich gleichermaßen. Dem ist auch so. Aber man darf dennoch nicht die Augen davor zu verschließen, dass die Abhör- und Spionageaktivitäten der US-Geheimdienste eine eigene Qualität hatten und haben. Schon allein der Umfang der bei der US-Regierung angesiedelten Behörden, die ihnen zur Verfügung stehenden Ressourcen, übersteigen die Möglichkeiten der

---

3 zitiert nach Berliner Umschau vom 25.10. 2013

anderen Industriestaaten zur Spionage um ein Vielfaches – von den Entwicklungsländern ganz abgesehen.

In dem von mir zu behandelnden militärischen Kontext ist wichtig, dass der ganze Bereich des Information Warfare seit über zwanzig Jahren gravierend an Bedeutung gewonnen hat. Spätestens Ende der 90er Jahre entwickelte sich eine intensive Diskussion innerhalb der NATO-Community – Streitkräften, Militärplanern, Sicherheitsstrategen – welchen Stellenwert Informations- und Kommunikationstechnologien in der Zukunft zukommen werde. Dabei geht es um Kriegführung und die Zeit „zwischen den Kriegen" gleichermaßen. „**Informationsüberlegenheit**" ist dabei das Schlüsselwort. Die moderne Informationstechnik wird dabei als entscheidender „Force Multiplier"[4] angesehen. Wer potenziellen Gegnern immer Schritte voraus sei, diesen jederzeit in die Karten schauen und umgekehrt solche Einblicke verweigern könne, der habe maximale Handlungsfreiheit und den strategischen Vorteil auf seiner Seite. Diese Annahme wurde insbesondere vor dem Hintergrund der Thesen von den asymmetrischen Bedrohungen und Kriege durchbuchstabiert. Der Versuch von Terrornetzwerken, übel wollenden Regierungen in der vormaligen Dritten Welt ihre rüstungstechnologischen Nachteile durch unkonventionelle und den völkerrechtlichen Rahmen sprengende Kriegführung (Guerillakrieg, Terrorattacken etc.) auszugleichen, müsse quasi durch die weitere Revolutionierung der Waffentechnik unterlaufen werden. Die Entwicklung unbemannter Waffensysteme und die Forcierung destruktiver Fähigkeiten im Cyber-Raum stehen dabei obenan. In beiden Fällen geht es darum, effizienteste Störungs- bzw. Zerstörungswirkung auf der gegnerischen Seite bei größtmöglicher Schonung eigener Kräfte zu erreichen. Und in beiden Fällen geht es nicht zuletzt um „verdeckte Operationen", mit denen auch Souveränitätsrechte anderer Länder ausgehebelt werden können und sollen!

Für die US-Streitkräfte wurden die entsprechenden Ziele und Vorgaben in einem National Defense Panel unter dem Titel „Transforming Defense. National Security in the 21st Century" ausgearbeitet und 1997 vorgelegt.

Im Bereich der Bundeswehr wurde bereits 1996 eine ausführliche Studie „Streitkräfteeinsatz (SKE) 2020" vorgelegt.[5]

Neue Informationstechnologien werden in der Folgezeit innerhalb der NATO als entscheidend neue Machtressource angesehen, mit der die Führungsüberlegenheit und damit die Durchsetzungsfähigkeit der eigenen Streitkräfte in der Zukunft gesichert werden könne.

Die Bundeswehr war in den neunziger Jahren bereits im Bereich der Satellitenaufklärung aktiv geworden, kooperierte dabei eng mit den französischen Streitkräften (Helios 2), entwickelte aber auch eigenständige Kapazitäten, und verfügt seitdem mit dem Satellitensystem SAR Lupe über die Möglichkeit strategischer Aufklärung mittels Radar. Daneben verfügte man über boden- und seegestützte signalerfassende Aufklärungssysteme (z.B. die Flottendienstboote),

---

4 Ruhmann, Ingo, Cyberterrorismus – Das Internet unter Kriegsrecht? in: S+F 2/2000, S. 144-149

5 Amt für Studien und Übungen (G.W. Meyer), Streitkräfteeinsatz 2020, 1996

die aber nur begrenzte Fähigkeitsprofile aufweisen konnten (tageszeit- und wetterabhängig, unzulängliche Reichweite usw.). In den Erörterungen über Einsätze der Bundeswehr außerhalb des NATO-Gebietes (out of area) wurde daher betont, dass die Truppe bei der Ausrüstung in jeglicher Hinsicht nachlegen müsse. Das Spektrum reichte dabei von Transportflugzeugen mit großer Reichweite, über besser geschützte Panzerfahrzeuge bis zu den neuartigen Informations- und Kommunikationssystemen, die für die Beurteilung der Lage vor Ort und die Führung der Militäroperationen essentiell erschienen.

Eine besondere **Fähigkeitslücke** entdeckte man sehr rasch. Die Bundeswehr würde nach der unumgänglichen Außerdienststellung alter Flugzeuge der Marine (Breguet Atlantic) spätestens 2010 nicht mehr über signalerfassende „Aufklärungssysteme“ (SIGINT) verfügen. Und hier begann die Geschichte von Eurohawk, eines Drohnenflugzeugs, das in einer Höhe von etwa 15 km stationiert werden sollte, und einen großen Radius von ca. 400 km abdecken könnte. Die Superdrohne wäre dort rund um die Uhr (24 Stunden, 7 Tage) aktiv und könnte nahezu ungefährdet alle telefonischen Daten abgreifen (Handy-Telefonate, Mail-Verkehr), die man zu Aufklärungszwecken für nötig erachtet.

In der Beschaffungsplanung wurde kein Hehl daraus gemacht, dass die Eurohawk oder vergleichbare Flugzeuge gedacht waren (und sind), um eine deutsche Beteiligung am militärischen Kriseninterventionismus zu gewährleisten und zu „optimieren“. Eine beliebte Rechtfertigungsformel dafür lautet: „Schutz der eigenen Truppen“ bei ihrem (selbstverständlich) friedensstiftenden Einsatz. Man kann es auch anders, präziser formulieren: Es geht um die Herstellung militärischer Dominanz, die die Freiheit des eigenen Handelns („freedom of action“) garantieren und damit den Gegner in die Knie zwingen soll.

Vor dem Eurohawk-Untersuchungsausschuss des Deutschen Bundestages hat der frühere Generalinspekteur der Bundeswehr, General Schneiderhan, die Anforderung der Streitkräfte an die Aufklärungs- bzw. Spionagesysteme recht exakt benannt:

Es gehe um kontinuierliche, verzugsarme strategische Lageinformation für die politische Leitung und die militärische Führung – im Spektrum von Krisenfrüherkennung, Krisenvorsorge, Krisenmanagement einschließlich der Planung und Vorbereitung von militärischen Einsätzen.[6]

Dass er dabei die Begriffe Krisen- und Interessensgebiete nahezu synonym verwendete, ist kein Zufall. Sein Nachfolger, General Wieker, konnte in der Ausspähung fremder Territorien durch Drohnen/Flugzeuge auch nichts Bedrohliches erkennen. Es scheint so zu sein, dass diejenigen, die sich immer auf der Seite des Guten wähnen, Schwierigkeiten haben, wahrzunehmen, dass solche Spionagehandlungen von den observierten Regierungen bzw. Bevölkerungen zumindest als unfreundlicher Akt empfunden werden könnten.

Umso mehr waren die Herren Generäle, neben den Industrievertretern, im Untersuchungsausschuss Eurohawk darum bemüht, die Drohnen auch als zivil nützliche Instrumente darzustellen. Sie könnten auch bei der Bekämpfung von Umweltkatastrophen

---

6 Wer Näheres wissen will: Deutscher Bundestag, Drucksache 17/14650, oder: EURO HAWK Untersuchungsausschussbericht, Bundesanzeiger Verlag 2013

helfen. (Ob dies für mit optischen- oder Infrarotsensoren ausgerüsteten Systeme zutrifft, könnte diskutiert werden. Aber dass man dafür den Telefon- und Funkverkehr abhören müsse, erscheint wenig plausibel.) Immerhin haben die Untersuchungen des Ausschusses auch zutage gefördert, wofür solch umfassende Datenstaubsauger auch nützlich sein könnten: Die Herstellungsfirma wollte die Drohnen der EU für die Flüchtlingsabwehr FRONTEX andienen. Eurohawk sollte der Bundesregierung „ressortübergreifend" offeriert werden, also auch für die „Innere Sicherheit". Zu denken ist an Ausspähungsmaßnahmen im Vorfeld von Großdemonstrationen, Streiks usw.

Wie wir wissen, wurde die Beschaffung von 5 Trägersystemen Eurohawk gestoppt wurde, die Entwicklung des Aufklärungssystems ISIS allerdings konsequent zu Ende geführt. Diese Apparatur muss jetzt in eine andere Trägerplattform eingebaut werden. Was letzten Endes daraus werden wird, wissen wir zur Zeit noch nicht; feststeht jedoch, dass die Bundeswehr in wenigen Jahren über solche HighTech-Spionageinstrumente verfügen wird. Ob dabei auch schon mal ein Handy einer ausländischen Regierungschefin abgehört werden wird?

Dass diese Entwicklungen – Kampfdrohnen wie ungehinderte Ausspähung durch Spionagesatelliten – strikt abgewiesen werden müssen, versteht sich. Aber machen wir es uns nicht zu einfach: Ist eine umfassende Aufklärung, die nicht zuletzt auch militärische Fakten einbeziehen muss, nicht eine wichtige Grundlage staatlichen Handelns? Brauchen nicht gerade internationale Einrichtungen wie die UNO oder die OSZE solche Aufklärungsmöglichkeiten, um politische und sonstige Entwicklungen überhaupt adäquat beurteilen zu können? Und kann der Hinweis auf Fälle, in denen mit sogenannten Aufklärungs- oder Spionage-Erkenntnissen Kriege bzw. bewaffnete Konflikte ausgelöst wurden, oder auch Krisen verschärft wurden, nicht umgedreht werden? Wenn man genauer wüsste, ob ein abgestürztes Flugzeug abgeschossen wurde und auch noch von wem, wenn man genau wüsste, wer in einem Krieg/Bürgerkrieg bestimmte Waffentypen eingesetzt hat (Bsp.: C-Waffen), hätte man damit nicht eine Handhabe, um Provokationen zu entlarven und damit ins Leere laufen zu lassen? Kann so verstandene Aufklärung auch für Verhandlungsprozesse von Nutzen sein? Das wird man schwerlich pauschal abweisen können.

Das Grundproblem liegt in dem Wort GEHEIM. Wer kontrolliert die sog. Nachrichtendienste? Wie viel Transparenz ist erforderlich, damit eine solche öffentliche, parlamentarisch-demokratische Kontrolle überhaupt möglich erscheint?

Was die Satellitensysteme der EU-Staaten, darunter auch das Beobachtungszentrum in Torrejon, anbetrifft, so schlugen Friedensforscher/-innen schon vor geraumer Zeit vor, dass die Daten, die dort gesammelt werden, „internationalisiert", d.h. zum Beispiel der OSZE zur Verfügung gestellt werden sollten. Damit würden diese Informationen nicht mehr zu Herrschaftszwecken missbraucht werden und könnten von Allen nutzbringend eingesetzt werden. Ob ein solches Herangehen möglich, ob es sinnvoll ist, ob es überhaupt wahrscheinlich ist, und ob man es auf den Bereich der Drohnen-Aufklärung übertragen kann, muss weiter diskutiert werden.

Was die weitere Perspektive der „Dienste" betrifft, wird man mit einer pauschalen Forderung nach deren Auflösung in der heutigen Welt nicht weit kommen. Keine Regierung wird sich auf

Spiegel online, BreakingNews von CNN, al Jazira, oder welchem Medium auch immer, verlassen, um daraus, Schlüsse für Regierungshandeln abzuleiten. Man wird auf Primärinformationen, auf authentischen Quellen bestehen, um sich ein eigenes Lagebild zu verschaffen. Das große Problem beginnt vor allem dort, wo die Nachrichtendienste operative Politik machen und dabei meinen, weil im Verborgenen, auch schlimme, verbotene Dinge tun zu dürfen. Die Überlegungen und Vorschläge sollten sich ergo darauf richten, wie aus Geheimdiensten parlamentarisch zu kontrollierende Nachrichtendienste werden können!

Es wird auch darauf ankommen, sich der unbegrenzten Durchsetzung der Drohnen-Aufrüstungsprogramme entgegen zu stellen und dringliche Forderungen zu deren Regulierung zu entwickeln. Dass die Entwicklung der Drohnentechnologie und damit die Robotisierung des Krieges unaufhaltsam seien, muss man nicht glauben. Noch muss und kann alles dafür getan werden, den Einsatz der Kampfdrohnen durch internationale Abkommen zu ächten und die Verwendung von unbewaffneten Drohnen sehr genau zu regeln und einzuhegen. Hier ist internationale Rüstungskontrolle und Abrüstung gefragt. Und die Bundeswehr kann einseitig auf die Beschaffung der Kampfdrohnen verzichten. Das wäre eine friedensstiftende Maßnahme.

Wie ist das militärische Nachrichtenwesen in Deutschland organisiert?

Der Bedeutungszuwachs der Informationsbeschaffung und –auswertung für das Militär hat dazu geführt, dass der Gesamtbereich des militärischen Nachrichtenwesens 2007/2008 umorganisiert wurde.

Das Zentrum für Nachrichtenwesen der Bundeswehr (ZNBW) wurde am 31.12.2007 aufgelöst. Die „Lagebearbeitung“ für das Bundesministerium der Verteidigung und die Bundeswehr erfolgt seitdem durch den Bundesnachrichtendienst, der seitdem das Monopol für die „Auslandsaufklärung“ hat. Dies machte die Umsetzung hunderter Dienstposten erforderlich. Mitarbeiter der sogenannten Feldnachrichtenkräfte der Truppe wurden in den BND eingegliedert. Sie erfüllen inzwischen die Aufgabe, die Streitkräfte bei den Kriseninterventionen mit den erforderlichen Nachrichten zu versorgen; zugleich soll der BND die politische Führung in die Lage versetzen, angemessen auf die zahlreichen Krisenprozesse zu reagieren.

Der übrig gebliebene „Rest“ ist bei der Bundeswehr geblieben: Dazu zählen die Satelliten-Aufklärung (SAR Lupe, Helios 2) und die signalerfassenden Systeme (wie die Flottendienstboote), die vom Kommando Strategische Aufklärung in Rheinbach bei Bonn geführt werden. Dort laufen dann die Informationen zusammen, die an die zuständigen Regierungsbehörden, den BND und andere weitergeleitet werden. Während der BND über eine MitarbeiterInnen-Zahl von ca. 5.000 Personen verfügt, weist das Kdo Strategische Aufklärung auch einen Beschäftigten-Umfang von 5.300 Menschen (= 4729 militärische und 579 zivile Dienstposten) aus. Das ist schon eine nicht gering zu schätzende Arbeitskapazität, lässt sich mit den Größenordnungen der US-Dienste (allein die NSA soll über 40.000 Mitarbeiter verfügen) allerdings nicht vergleichen.

Die Drohnen, die die Bundeswehr auf den Einsatz-Schauplätzen benutzt werden, werden bisher von den Teilstreitkräften (Heer, Luftwaffe) eingesetzt und geführt. Im Falle der Eurohawk

war die Unterstellung noch nicht festgelegt; die Verschiebung der Beschaffung hat diese Frage bis heute offen gelassen. Von einer künftigen Zentralisierung der Drohnen-Systeme ist jedoch auszugehen.

Steigt auch die Bundeswehr in den CyberWarfare ein?

Das neueste Spielfeld der Informationskriegführung heißt CyberSpace. Hierbei geht es um alles was mit Computern, der Einwirkung auf Computer, Software etc. und dem Internet zu tun hat. Spätestens seit der Einschleusung der Schadsoftware Stuxnet in die iranischen Atomanlagen (über USB-Sticks), um diese zu zerstören oder zu schädigen, um damit den Fortgang des dortigen Atomprogrammes zumindest beträchtlich zurückzuwerfen, ist auch einer größeren Öffentlichkeit bewusst geworden, dass sich hier ein neuer konfliktträchtiger Raum auftut. Stuxnet wird inzwischen eindeutig US-amerikanischen Urhebern zugeschrieben. Paradoxerweise muss dieser Trojaner in NATO-Debatten immer wieder herhalten, um die Dringlichkeit der Abwehr neuer Bedrohungen hervorzuheben.

Die NATO hat in ihrem Strategischen Konzept von 2010 erstmals das Thema Cyber Security prominent erwähnt; im Juni 2011 wurde ein weitreichender Beschluss über eine Cyber Defense Policy gefasst. Ein umfangreicher Maßnahmekatalog wurde verabschiedet.[7]

Natürlich war auch die Bundeswehr schon länger dabei, allerdings – wie wir heute wissen – auf nicht hohem Level.

Einen ersten, wenig aussagekräftigen Bericht übersandte das Bundesministerium der Verteidigung (BMVg) dem Verteidigungsausschuss im Juni 2011, der aber weiter keine Beachtung fand. Als Abgeordneter und Mitglied des Verteidigungsausschusses habe ich nachgefragt, darauf gedrängt, dieses Thema im Ausschuss zu behandeln. Zunächst ohne Wirkung. Im April 2012 folgte ein weiterer, immer noch recht dürftiger Bericht des BMVg., der viele Fragen unbeantwortet ließ. Ich sah mich dadurch herausgefordert und begab mich am 19.9 2012 direkt ins zuständige Kommando nach Rheinbach begeben, um mich vor Ort briefen zu lassen. Auch andere Mitglieder des Ausschusses taten dies.

Der Vg.-Ausschuss befasste sich erstmals eingehender mit dem Cyber-Thema auf seiner Sitzung am 30. Januar.2013. Dort trug ein Vertreter des Bundesministers des Inneren über die Maßnahmen im zivilen Bereich vor und berichtete über den Aufbau eines Nationalen Cyber-Abwehrzentrums. Der Ausschuss erfuhr erstmals durch BMVg-Vertreter Einiges über den Aufbau einer „Cyber-Unit“ beim KStratAufklärung der Bundeswehr.

In einem ausführlicheren Bericht vom 16. April 2013 konnten die Abgeordneten mehr über die im Aufbau befindliche Abteilung ComputerNetzwerk-Operationen beim KSA erfahren. Die Debatte darüber erfolgte am 13.6.2013.

Zum damaligen Zeitpunkt verfügte diese spezielle Abteilung über 59 Dienstposten (die Zahl derer, die sich mit Cyber-Sicherheit beschäftigen, ist natürlich viel größer), ein rapider

---

7 Mehr unter: NATO and Cyber Defense, s. www.nato.int/cps/en/natolive

Aufwuchs war nicht vorgesehen, die Ausstattung wirkte eher bescheiden. Man habe eine „Anfangsbefähigung zum Wirken in gegnerischen Netzen“ inzwischen erreicht, lautete die Botschaft des Berichts an den Ausschuss und des Briefings vor Ort. Was dies im Einzelnen bedeutet, blieb zunächst unklar. Die Simulation bestätigte nur, dass man im Prinzip mittels auf dem Markt vorfindlicher Werkzeuge in der Lage ist, die Luftabwehr eines potentiell gegnerischen Landes empfindlich lahm zu legen. Ob man aber auch tatsächlich schon in „gegnerischen Netzen“ operiert, oder sich nur die Option verschafft hat, bleibt weiter offen.

Zumindest wissen wir jetzt mehr über die Cyber-Philosophie der deutschen Streitkräfte:

- Man vermeidet den Ausdruck Cyber-Krieg, sondern spricht stattdessen von Cyber-Verteidigung.
- Der Cyber-Raum wird - neben Luft, Land, See – schlicht als neue Dimension möglicher Auseinandersetzungen angesehen. Daher sei dieser Raum eine eigenständige operative Domäne, aber in der Sache gehe es „nur“ um die Fortsetzung früherer militärischer Kampfoptionen mit neuen Mitteln (wenn man so will, als ELoKa 2.0). Im Bericht vom 13.4.2013 heißt es daher lapidar, bei den Aktivitäten im Cyber-Raum handele es sich um ein „weiteres Wirkmittel der Streitkräfte“.
- Dass in diesem Bereich Defensive und Offensive nicht strikt zu trennen sind, wird nicht völlig in Abrede gestellt. Offensive Operationen werden als probates Mittel betrachtet, um Cyber-Attacken auf die eigenen Netze abzuschrecken. Die Grenzen sind zudem fließend: Schon bei der Vorfeldaufklärung über mögliche Cyber-Attacken kann es passieren, dass man in gegnerisches Systeme „eindringt“. Schließlich und am wichtigsten: Immer geht es bei der sog. Cyber-Abwehr auch um Aktionsspielräume der eigenen militärischen Kräfte bei Kriseninterventionen. Und ob es dabei immer um legitime Selbstverteidigung geht, darf bezweifelt werden.
- Die Bundeswehr zeichnet ein, wir kennen es auch aus der grundsätzlichen Bedrohungsanalyse der Streitkräfte, ziemliches diffuses Bild einer gegebenen Bedrohungslage. Aus dem eigenen „Lager“ hervorgebrachte Bedrohungen, wie die Angriffe durch Stuxnet, werden umstandslos als Beleg aufgeführt; die Gesamtsumme der Angriffe im Netz, also auch und gerade im zivilen Bereich, muss als Beweis dafür herhalten, dass man die eigenen Anstrengungen erheblich steigern müsse. Und dazu gehört es eben auch (s.o.), die eigenen Fähigkeiten zum Eindringen in fremde Netze voranzutreiben.
- Dass nicht alle rechtlichen Fragen geklärt, wird eingeräumt. Eine der zu beantwortenden Fragen: Wann muss eine Cyber-Attacke auf Einrichtungen eines NATO-Mitgliedslandes als Angriff gewertet werden, der den Bündnisfall mit entsprechenden Beistandsverpflichtungen auslöst? Klärungsbedürftig auch Fragen im Zusammenhang des Parlamentsvorbehalts bei bewaffneten Einsätzen: Bedürfen aggressive Operationen in gegnerischen Netzen der Zustimmung des Parlaments? Muss darüber nicht zumindest im Vorfeld informiert werden? Muss das Parlamentsbeteiligungsgesetz hier weiterentwickelt werden? Immerhin scheint sich die Bundesregierung im internationalen Rahmen daran zu beteiligen, einen Verhaltenskodex für den Umgang mit empfindlichen Daten in den jeweiligen Netzwerken entwickeln zu wollen. In der entsprechenden Arbeitsgruppe der OSZE ist man aktiv.

Natürlich spielte in jüngster Zeit auch die Frage eine Rolle, welche Kooperationsbeziehungen die Bundesrepublik auf diesem Gebiet mit den USA oder anderen NATO-Staaten eingegangen ist und wie diese Zusammenarbeit künftig gestaltet werden sollte.

Die alte Bundesregierung hat dazu lediglich mitgeteilt, dass man sich in puncto Risikomanagement und Bedrohungsanalyse selbstverständlich mit den Bündnispartnern austausche (zuständig dafür ist auf deutscher Seite das Computer Emergency Response Team der Bundeswehr (CERTBw)). Aber das hätte man gerne genauer gewusst.

Fazit: Auch auf diesem Feld gilt es unter kritischen Vorzeichen weiterführende Vorschläge zur Einhegung, Kontrolle usw. zu erarbeiten. Zumindest kann gesagt werden.

- Gegen Cyberterror hilft nicht zuletzt die Beseitigung der Sicherheitsmängel bestehender IT-Systeme. Da ist gewiss Einiges in der jüngeren Vergangenheit geschehen, aber es kann noch mehr getan werden.
- Für den Gesamtbereich der „Netzpolitik“ - ob es sich da um kommerzielle Nutzer, um Privatpersonen oder Regierungseinrichtungen handelt - gilt, dass der Grundwert „Schutz der Privatsphäre jedes Einzelnen/jeder Einzelnen“ neu bekräftigt und durchgesetzt werden muss. Weder die ungehemmte Ausspähung Anderer, noch das verdeckte Eindringen in „fremde Netze“ sind statthaft.
- Eine neue Art Rüstungswettlauf im Bereich Cyber(Warfare) ist der falsche Weg; stattdessen muss auch hier der Weg in internationalen Regimen der Rüstungskontrolle und der Abrüstung gesucht werden:
- Da es innerhalb der NATO einen unabweisbaren Nexus zwischen Militäreinsätzen „out of area“ und der Informations-/Cyber-Kriegsführung gibt, müssen diese Kriseninterventionen immer wieder kritisch hinterfragt werden. Die Stärkung der Friedens- und Konfliktforschung und der weitere Ausbau der zivilen Konfliktbearbeitung wären da eine prima Alternative.