VEREIN SICHERHEITSPOLITIK
UND WEHRWISSENSCHAFT

POSTFACH 65, 8024 ZÜRICH

Sicherheitspolitische Information

Herausgegeben vom Verein Sicherheitspolitik und Wehrwissenschaft (VSWW)
Postfach 65, 8024 Zürich (PC 80–500-4)

www.Chinfo.ch/vsww

Präsident: Dr. Günter Heuberger
Redaktion: Dr. Daniel Heller, Ivan Jäggi

Juli 2005

Vernetzte Sicherheit

Aspekte der Zusammenarbeit von Sicherheitsorganisationen – eine Analyse nach den Anschlägen von London

Ob national oder international, ob technisch oder führungsmässig: Die Zusammenarbeit von Sicherheitsorganisationen bietet oft unüberwindbare Probleme.

Inhalt

Vorwort

Ausgehend von den modernen Streitkräften, die heute komplexe elektronische Netzwerke bilden, lassen sich die entsprechenden Technologien über den eigentlichen klassischen Kriegsfall hinaus in einer Vielzahl von Krisenlagen auch für den Bereich der Inneren Sicherheit nutzbar machen.

Es ist auch für die Schweiz entscheidend, bei der Suche nach einer angemessenen Antwort auf aktuelle Herausforderungen für den Bereich der Inneren Sicherheit Begriffe wie «Vernetzte Sicherheit» und «Netcentric Organisations» in den Mittelpunkt ihrer Aufmerksamkeit zu stellen. Die Notwendigkeit zur Zusammenarbeit zeigt sich technisch, aber auch bezogen auf die Einsatzführung, die Kompetenzordnung und die Rollenspezifizierung. Es fehlt in der Schweiz ein überzeugendes Konzept der Inneren Sicherheit.

Die Schweiz wird sich gegenüber dieser Entwicklung zur Vernetzung der Sicherheitsorgane nicht länger verschliessen können, will sie auf die aktuelle Bedrohungslage angemessen reagieren können.

Dr. Günter Heuberger, Präsident VSWW

1 Vernetzte Sicherheit

Organisationen, die im Bereich der Nationalen oder der Inneren Sicherheit tätig sind, sehen sich heute vor *immer komplexere Aufgaben* gestellt. Das Spektrum der Bedrohungen erweitert sich nicht nur, es ändert sich vor allem ständig. Einer der Schlüssel der Zukunft liegt im *erfolgreichen Zusammenwirken* der verschiedenen Sicherheitsorganisationen.

Wie man auf Herausforderungen aller Art angemessen reagiert, machen moderne Streitkräfte international vor: Sie orientieren sich am Konzept der netzwerkzentrierten Operationsführung und erschliessen durch das *Teilen von Informationen* neue Wertschöpfungsquellen. Eine Wertschöpfung, die sich konkret messen lässt anhand von Faktoren wie Kosten, Funktionalität und Transparenz. Bei Militär, Polizei und Rettungskräften kommen darüber hinaus die Faktoren *Überlebensfähigkeit, Geschwindigkeit, Effizienz,* zeitliche *Synchronisation und Reaktionsfähigkeit* hinzu.

In den Fokus der Sicherheitspolitik sind in den letzten Jahren zunehmend der *Terror und seine Bekämpfung,* und damit die Wechselwirkung zwischen Innerer und Äusserer Sicherheit geraten. Als Reaktion auf die Terroranschläge vom 11. September kündigte die Regierung der USA im Jahr 2001 an, einen weltweiten Krieg gegen den Terrorismus («War on Terrorism» oder häufiger «War on Terror») führen zu wollen – einen langwierigen Kampf gegen Terroristen und jede Regierung, die sie unterstützt. Der Begriff knüpft einerseits an ähnliche, von früheren US-Regierungen geprägte Begriffe wie Krieg gegen Armut («War on Poverty») oder Krieg gegen Drogen («War on Drugs») an, und spiegelt andererseits das Empfinden vieler Menschen wider, die die Anschläge in ihrer Dimension als *Kriegserklärung an die Zivilisation* empfanden.

Der Begriff setzte sich international schnell durch für *alle Arten von Massnahmen,* die – zu Recht oder zu Unrecht – als Terrorismusbekämpfung verstanden werden sollten. So wurden auch einige bestehende Konflikte wie (von den USA selbst) der Irak-Konflikt, aber auch der Tschetschenien-Konflikt und der Nahostkonflikt in diesem Sinne neu interpretiert. In der Schweiz kam es in diesem Zusammenhang zu *intensiven Diskussionen* zum Einsatz der Polizei, der Armee und der Rettungskräfte. Mit den Nullentscheiden im Zusammenhang mit USIS 3 gelangte die Schweiz schnell an den Punkt, wo *Improvisation und politisches Versagen* die Diskussion über eine wirksame Zusammenarbeit von Sicherheitsorganisationen zum Zwecke der Wahrung der Inneren Sicherheit dominierte. Die vorliegende Studie macht – kurz nach den jüngsten *Anschlägen in London* – eine Auslegeordnung zu diesem zentralen Thema moderner Sicherheitspolitik.

Chronik des Terrors: Schwere Terroranschläge seit dem 11. September 2001

11. September 2001: In New York und Washington werden fast 3000 Menschen getötet, nachdem Attentäter drei Flugzeuge in das World Trade Center und das Pentagon gesteuert haben. Eine vierte entführte Maschine stürzt über Pennsylvania ab.

11. April 2002: Auf der tunesischen Ferieninsel Djerba kommen bei einem Anschlag vor einer Synagoge 21 Menschen ums Leben.

14. Juni 2002: Ein Selbstmordattentäter reißt vor dem US-Konsulat in der pakistanischen Hafenstadt Karachi 14 Menschen mit in den Tod. Die Behörden machen die Organisation Harkat-ul-Mujahedeen verantwortlich, die mit der Al Qaida in Verbindung gebracht wird.

12. Oktober 2002: Bei Bombenanschlägen auf Nachtclubs der indonesischen Insel Bali werden 202 Menschen getötet, vor allem ausländische Touristen. Als Drahtzieher gilt die Jemaah Islamiyah, die Kontakt zur Al Qaida haben soll.

28. November 2002: Drei Selbstmordattentäter töten in Kenia 13 weitere Menschen in einem Hotel bei Mombasa. Zugleich wird ein israelisches Charterflugzeug nach dem Start in Mombasa mit Raketen beschossen, die ihr Ziel jedoch verfehlen.

12. Mai 2003: Bei Anschlägen auf überwiegend von Ausländern bewohnte Gebäude in der saudiarabischen Hauptstadt Riad kommen 35 Menschen ums Leben, darunter neun Attentäter.

16. Mai 2003: Bei einer Anschlagsserie in Marokko werden mehr als 40 Menschen getötet, darunter zwölf Attentäter, und mehr als 100 verletzt. Einigen Verdächtigen wird Mitgliedschaft in der marokkanischen Extremistenorganisation Salafia Jihadia vorgeworfen, die Verbindungen zur El Kaida haben soll.

5. August 2003: In einem Hotel der indonesischen Hauptstadt Jakarta reißt ein Selbstmordattentäter zwölf Menschen mit in den Tod. Rund 150 Menschen werden verletzt. Hinter dem Anschlag wird erneut die Jemaah Islamiyah vermutet.

8. November 2003: Bei drei vermutlich von Selbstmordattentätern ausgelösten Explosionen in einer Wohnanlage in Riad werden neben den Angreifern mindestens zehn Menschen getötet, darunter zwei kleine Kinder. Mehr als 80 Bewohner des Wohnviertels werden verletzt.

12. November 2003: Zwei Sebstmordattentäter reissen bei Anschlägen auf zwei Synagogen in Istanbul 23 Personen mit sich in den Tod.

20. November 2003: Bei Bombenanschlägen auf das britische Konsulat und eine britische Bank in Istanbul werden 30 Personen getötet und 400 weitere verletzt.

11. März 2004: Bei einer Serie von Bombenanschlägen in Madrid kommen 191 Personen ums Leben, rund 1'500 weitere werden verletzt.

3. September 2004: Das dreitägige Geiseldrama in der Schule von Beslam (Kaukasus) endet mit Dutzenden von Toten und Verletzten.

6. Juli 2005: Zum G-8-Gipfel explodieren in London vier Sprengsätze – es kommt zu zahlreichen Toten und etwa 700 Verletzten.

2 Die Entwicklung vom Netcentric Warfare zu den Netcentric Operations

Eine moderne Armee, wofür sie denn auch immer eingesetzt wird, muss *alle Grundfunktionen einer Streitkraft des 21. Jahrhunderts* – zumindest in einem beschränkten Umfang, aber in höchster Qualität mit dem Ziel, bei Bedarf auf diesen Fähigkeiten aufzubauen – erfüllen können. In diesem Sinne sind moderne Streitkräfte oder zumindest solche, die es bleiben wollen, einem beständigen *Prozess der Anpassung und Wandlung* unterworfen.

Zu diesen Grundfunktionen auch unserer Streitkräfte im Verbund mit anderen Sicherheitsorganisationen gehört ein *integriertes, krisenfestes Führungssystem,* welches die Behörden von Bund, Kantonen und Kommunen sowie alle sicherheitspolitischen Institutionen verbinden kann. Es ermöglicht im Ereignisfall eine laufende Lageanalyse sowie die fristgerechte Anordnung und Kontrolle aller notwendigen Massnahmen, die zur Aufrechterhaltung der Inneren oder der Äusseren Sicherheit notwendig sind.

2.1 Das Konzept des Netcentric Warfare

Treiber dieser Entwicklung ist auch im 21. Jahrhundert die *eigentliche Kriegführung*. Seit den von US-amerikanischen Truppen angeführten Militäroperationen im Irak 2003 wurde für alle Beobachter deutlich, auf welchen *herausragenden Ausbaustand* die Vernetzung dieser Streitkräfte mittels Kommunikationsmitteln gebracht wurden. Der Zuwachs gegenüber dem Golfkrieg von 1990 ist evident und enorm. Die alliierten Kräfte erreichten 2003 mit dem Konzept des Netcentric Warfare eine bis dahin *unerreichte Geschwindigkeit* in ihrer Situationsanalyse. Die Zeitspanne von der Informationsaufnahme bis hin zur Aktion oder zur Schussabgabe wurde noch einmal erheblich beschleunigt und die Wirkung ihrer Waffen in beträchtlichem Masse gesteigert.

Unter Netcentric Warfare (NCW) oder Network-based Warfare wird generell ein auf *Informationsvorteil beruhendes Operationskonzept* verstanden. Charakteristika eines NCW sind nach David S. Alberts[1] die Vernetzung von Sensoren mit Entscheidungsträgern und Waffensystemen, wodurch die Befehlsausgabe beschleunigt, das Operationstempo erhöht, die Wirkung auf das Ziel gesteigert, die Überlebensfähigkeit der eigenen Truppen erhöht und ein gewisser Grad an Selbstsynchronisation der Kräfte erreicht werden kann. Insgesamt wird damit für die eigenen Streitkräfte ein gesteigerter Kampfwert generiert.

Im Gegensatz zum NCW wird die traditionelle Kriegführung als *Platform-centric Warfare* betrachtet. Der Unterschied zwischen diesen beiden Typen der Kriegführung besteht darin, dass jedes Waffensystem im Platform-centric Warfare unabhängig handelt, so dass Kräfte konzentriert werden müssen, um die Kampfwirkung zu steigern, während gemäss NCW die Wirkung und nicht die eigentlichen Kräfte gesteigert wird.

[1] Alberts, D. S., Information Age Transformation: Getting to a 21st Century Military, rev. ed., Washington, D.C.: Command and Control Research Program (CCRP), 2002.

2.2 Das Konzept der Netcentric Operations

Das Konzept des NCW ist eher auf den konventionellen Kriegsfall ausgerichtet. Die neuen Konfliktformen verlangen aber nach einer Vernetzung dreier Arten von Einsätzen, wobei die Fähigkeit für Netcentric Operations (NCO) weiterhin im Zentrum steht:

- Eingreifoperationen mit schwerer Ausrüstung,
- stabilisierende Aktionen,
- Grundbetrieb von Streitkräften.

Informationstransfer und gemeinsame Verfügbarkeit von Informationen bilden auch bei den NCO die zentralen Merkmale. Im Gegensatz zum NCW sind die NCO aber nicht mehr nur allein für den eigentlichen Kriegsfall, sondern für eine breitere Einsatzpalette konzipiert. Die Streitkräfte bilden dabei nur noch *ein Element im Gesamtkontext*.

Die Auf- und Ausrüstung für NCO ziehen zwar einen grossen Investitionsbedarf nach sich, aber durch die damit gewonnene Möglichkeit des Teilens von Informationen erschliessen sich neue Wertschöpfungsquellen. So ist heute die deutsche Bundeswehr in der Lage, rasch ein *rollendefiniertes Lagebild* bereitzustellen, um eine vernetzte Operation gewährleisten zu können. Damit dies überhaupt möglich ist, müssen sowohl die Voice-Kommunikation wie auch die Datentransfers derart gestaltet sein, dass ein gemeinsames Lagebild erzeugt werden kann.

Wenn für das Eintreten ausserordentlicher Lagen kein Super-«Homeland-Security»-Ministerium geschaffen werden soll, muss es möglich sein, ein *politisch-zivil geführtes ad hoc-Führungszentrum* zu betreiben, welches die Einsätze aller involvierter Sicherheitsorganisationen führt und koordiniert. Dies ist aber nur möglich, wenn ein solches Führungsgremium in ein Netzwerk eingebunden ist, das über die Fähigkeit für NCO verfügt.

Die Elbe-Flutbewältigung im Jahr 2002 in Deutschland hat in der Koordination des Informationsflusses gravierende Schwächen offen gelegt: Informationen waren zwar vorhanden, aber der Transfer und die Vernetzung gelangen nur mangelhaft, so dass entsprechend höhere Koordinationskosten und demzufolge höhere Schäden wegen zu spät getroffener Vorkehrungen entstanden sind. Die Situation in der Schweiz wäre nach allen Aussagen von Experten *zumindest nicht besser* als jene in Deutschland. Hier würde NCO Abhilfe schaffen.

3 Die Auswirkungen auf die Schweizer Armee

Dem zu beobachtenden Transformationsprozess moderner westlicher Streitkräfte hin zur *Integration in elektronische Netzwerke*, welche den Informationsfluss sicherstellen, kann sich auch die Schweizer Armee nicht entziehen.

Im Falle unserer Streitkräfte müsste sichergestellt sein, dass sich sowohl modular zusammenstellbare militärische Kräfte als auch Waffensysteme bzw. Teile davon zu einem Ganzen zusammenfügen, um je nach Lage Einsätze in der Schweiz – im Verteidigungsfall oder im Rahmen eines *koordinierten Einsatzes* mit zivilen Partnern – oder Einsätze im Ausland im Rahmen eines multinationalen Einsatzes erfolgreich durchführen zu können. Diese Notwendigkeit erfordert eine *vernetzte Operationsführung*, welche die Einbindung von Sensoren, Effektoren, Entscheidungsträgern und Leistungserbringern zulässt und innerhalb eines Führungssystems als eigentlicher Force-Multiplikator wirkt.

3.1 Auf dem Weg zu Network Enabled Operations

Die Schweiz ist daran, sich die Fähigkeiten für NCO aufzubauen, wobei das VBS den Begriff Network Enabled Operations (NEO) verwendet. Der Leitgedanke hinter dem Aufbau eigener Fähigkeiten für NEO ist es, die Aufträge effizient erfüllen zu können, indem die relevanten Informationen stufen- und zeitgerecht zu einem umfassenden und einheitlichen Lagebild gebündelt werden.

Network Enabled Operations

Unter dem Begriff Network Enabled Operations (NEO) versteht der Planungsstab der Schweizer Armee eine Konzeption, welche durch die Einbindung von Sensoren, Effektoren, Entscheidungsträgern und Leistungserbringern in einem Netzwerk Mehrwert generiert, um entscheidende Wirkungen zu erzeugen.

Quelle: http://www.vbs-ddps.ch/internet/groupgst/de/home/planung.Par.0004.DownloadFile.tmp/02_Faltblatt_d_050608.pdf

In einer ersten Phase (2004–2008) soll ein erster Führungsverbund aufgebaut werden, um den stufen- und zeitgerechten Informationsaustausch

innerhalb des Bereiches Verteidigung sicherzustellen. In einer 2. Phase (2008–2011) geht es um den Aufbau von C4ISTAR.

C4 ISTAR

C4 ISTAR steht für Command, Control, Computers, Communication, Information / Intelligence, Surveillance, Target Acquisition, Reconnaissance. C4 ISTAR beschreibt die Gesamtheit der Instrumente und Massnahmen, die als Plattform für die Führung angewendet werden. C4 ISTAR teilt sich in zwei Hauptbereiche:

- Einerseits beschreibt C4I die notwendigen Grundlagen für die Aufbereitung von Informationen im Hinblick auf die situationsgerechte Entschlussfassung und die Führung,
- Andererseits deckt ISTAR alle Bereiche ab, die zur Beschaffung entschlussrelevanter Informationen dienen.

Quelle: http://www.vbs-ddps.ch/internet/groupgst/de/home/planung.Par.0004.DownloadFile.tmp/02_Faltblatt_d_050608.pdf

3.2 Die konkrete Umsetzung

Die Armee soll damit zur stufen- und zeitgerechten Generierung eines «Joint Recognised Picture» und zu dessen Verbreitung befähigt werden. Dies ist einzig mit der Beschaffung fehlender Sensoren, der Kampfwertsteigerung bzw. -erhaltung bestehender Sensoren und Effektoren sowie deren Integration in den Führungsverbund zu erreichen. Parallel dazu sollen die Kompetenzen zur netzwerkgestützten Aktionsplanung und -führung auf allen Stufen mit einem *evolutionären Ausbau des Führungsverbundes* geschaffen und die Interoperabilität sichergestellt werden.

Im Rüstungsprogramm 2006 sind 600–800 Mio. CHF für die Beschaffung des Joint FIS – des Teilstreitkräfte übergreifenden Führungs- und Informationssystems der Schweizer Armee – vorgesehen. Dieses wird die technologische Plattform zur Sicherstellung der vernetzten Operationsführung der unterstellten Kräfte des Chefs der Armee bzw. des Oberbefehlshabers der Armee. Gemäss heutigem Planungsstand werden zwischen 2008 und 2012 *weitere ISTAR-Komponenten* beschafft werden.

4 Innere Sicherheit: Die technische Seite

Die sicherheitspolitischen Megatrends lassen mittelfristig eher eine Verschlechterung der Sicherheitslage erwarten: *Migration, Ressourcendisparitäten, Wohlstandsgefälle, soziale Unrast und Zunahme der Verletzlichkeit technologischer Gesellschaften* lauten nur einige der Gefahrenpotentiale. Es besteht dabei kaum Beurteilungssicherheit über die Eintretenswahrscheinlichkeit der einzelnen Szenarien.

4.1 System der Inneren Sicherheit als Verbundsystem

Die Gefährdung durch nicht näher zu definierende Krisen ist umso bedrohlicher, als sie auf die zersplitterten Kompetenzen von Kantone und Bund sowie ein *teures und eher ineffizientes System* der Inneren Sicherheit trifft. Bei einer tiefen pro Kopf-Polizeidichte haben wir eines der teuersten Polizeikorps: 25 Mio. EUR pro Jahr auf 100’000 Einwohner ist ein Spitzenrang.

Um auf eine eher als diffus beschriebene und empfundene, aber durchaus reale Bedrohungslage reagieren zu können, müssen die Vorkehrungen zur Inneren Sicherheit *als Verbundssystem* zwischen den verschiedenen Akteuren aufgebaut sein.

So wie die militärische Sicherheit in den nächsten Jahren zielstrebig vernetzt wird, muss auch für den Bereich der Inneren Sicherheit in naher Zukunft ein *modernes Kommunikationsnetzwerk* geschaffen werden, das den Informations- und Datenfluss sowie den Zugriff der verschiedenen involvierten Stellen beschleunigt und auch für Krisenlagen sicherstellt. Ohne ein solches Kommunikationsnetz ist an eine effiziente Koordination der verschiedenen Einsatzkräfte im Krisenfall nicht zu denken.

4.2 Heutiger Zustand

Nach Eingang eines Grossalarms rücken Feuerwehr, Sanität und Kantonspolizei aus. Die Alarmierung der Rettungskräfte funktioniert heute tadellos. Doch bei der Kommunikation zwischen den verschiedenen Einsatzkräften treten die *Schwierigkeiten* auf, denn jeder Dienst funkt auf einem anderen Kanal. Um alle Informationen mitzukriegen, müssen die verschiedenen Einsatz-

kräfte teilweise bis zu drei Funkgeräte im Einsatz mit dabei haben. Bisweilen existieren zwar gemeinsame Kanäle, doch wie sagt man einem Gesprächspartner, dass er im richtigen Moment auf diesen Koordinationskanal umschalten soll? Bei Grossereignissen tauschen heute die Einsatzstäbe deshalb als Erstes Handynummern (!) aus.

Die Kantonspolizeien Basel-Stadt und Baselland benutzen beispielsweise je ihre eigenen Systeme. Wegen der unterschiedlichen Codierung sind sie nicht kompatibel. Will ein Baselbieter Gesetzeshüter mit einem Kollegen aus der Stadt Kontakt aufnehmen, muss er über die Einsatzzentrale gehen. Andere Dienste wie etwa die Sanität funken immer noch über offene Kanäle, wo jedermann mithören kann und selbst der Koordinationskanal ist *nicht verschlüsselt*.

4.3 Bundesrätlicher Entscheid für Polycom

Der Bundesrat gab bereits 2001 grünes Licht für das nationale *Sicherheitsfunknetz Polycom* zu Gunsten aller Behörden und Organisationen für Rettung und Sicherheit (BORS). Einmal in Betrieb wird es den Funkkontakt unter den verschiedenen Partnerorganisationen wie Grenzwachtkorps, Polizei und den Rettungsorganisationen ermöglichen. Zum Einsatz kommt das digitale *Bündelfunksystem Tetrapol*.

Digitale Bündelfunksysteme stellen global gesehen den aktuellsten Stand der Entwicklung von Kommunikationssystemen für den professionellen Mobilfunk dar. Sie kombinieren frequenzökonomische Bündelfunktechnologie mit moderner Digitaltechnik welche durch geeignete Algorithmen nicht nur die Sprachqualität erhöht, sondern auch eine zuverlässigere (weniger Übertragungsfehler) und abhörsichere Übertragung erlaubt.

Breites Anwendungsspektrum von Tetrapol
Ein professionelles Mobilfunknetz welches von mehreren Organisationen geteilt werden kann, muss sämtliche Bedürfnisse aller Organisationen vollumfänglich abdecken. Dabei muss im Bedarfsfall auch organisationsübergreifende Kommunikation möglich sein. Der Standard Tetrapol vermag ein breites Anwendungsspektrum abzudecken:

- vollautomatische Zuordnung eines Betriebskanals und Verwaltung der Frequenzressourcen,
- Ende-zu-Ende-Verschlüsselung im Regelbetrieb,
- robuster Direktmodus ohne Netzinfrastruktur,
- Sprach- und Datenfunk im gleichen Netz mit gleicher Abdeckung,
- Durchwahlmöglichkeit von/in andere Netze (Sprache und Daten),
- offener Kanal, «Jeder-hört-Jeden» Funktion,
- Interoperabilität zwischen verschiedenen Organisationen,
- dynamische Gruppenbildung durch Leitstelle,
- ständige Überwachung des Netzes im Direkt-Betrieb (Dual-Watch Mode),
- Ferndeaktivierung von Terminals (temporär/endgültig) im Falle von Diebstahl oder Verlust,
- parametrisierbarer Notruf,
- Steuerung der Gespräche nach Prioritätsgesichtspunkten,
- Koppelbarkeit mit GPS-Systemen für Flottenmanagement.

Tetrapol wurde speziell für die *Kommunikationsanforderungen von Behörden und Organisationen mit Sicherheitsaufgaben* wie Grenzschutz, Polizei, Feuerwehr, Rettungs- und Sicherheitsorganisationen (Sanität, Energieversorgung, Autobahndienste) sowie für die Armee konzipiert. Aufgrund seiner Modularität kann Tetrapol einfach erweitert werden und so einzelne Regionen oder ganze Länder mit Funkdiensten versorgen. Dank dem geringen Bandbreitenbedarf (12,5 kHz) lässt sich das System in heute analog genutzte Frequenzbänder integrieren und ermöglicht damit eine sanfte Migration von der bisherigen Analog- zur Digitaltechnik. Durch die Kompatibilität, Interoperabilität und das *automatische Mobility Management* können regionale Netze in nationale Netze integriert werden. Tetrapol beweist durch operativen Einsatz mit 49 Netzen in 26 Ländern seine Tauglichkeit zur Zufriedenheit von Multiuser-Organisationen.

4.4 Umsetzung in weite Ferne gerückt

Die Umsetzung des bundesrätlichen Entscheides zu Polycom liegt immer noch in *weiter Ferne*. Zwar fiel der Entscheid des Bundesrats 2001, trotzdem ist man bis heute nicht über Diskussionen hinausgekommen. Nur einige wenige Organe und Stellen haben Polycom eingeführt. Bis März 2005 haben einzig Teile des Grenzwachtkorps und die Kantone Aargau, Glarus, Neuenburg und Thurgau Regional- und Teilnetze von Polycom in Betrieb genommen.

Die Industrie wäre bereit, den Entscheid des Bundesrates umzusetzen, hat investiert und nun feiert der Föderalismus Urstände. Dass der Bund in der Umsetzung seines Entscheides zu Polycom den Lead preisgegeben hat, entpuppt sich heute *als Fehler*. Es wird wohl ein Grossereignis brauchen, um hier Abhilfe zu schaffen. Man kann nur hoffen, dass es sich dabei um ein gutes handelt, wie es die EM 2008 darstellt, und nicht um eine Katastrophe oder ein Ereignis, wie es London dieser Tage erleben musste.

5 Innere Sicherheit: Die Einsatzseite

Gravierende Defizite in der Ausgestaltung der Inneren Sicherheit bestehen aber auch einsatzseitig, wenn «Soll» und «Ist» miteinander verglichen werden. So sollen Lageveränderungen rechtzeitig erfasst, eine rasche Reaktionsfähigkeit gewährleistet, adäquate Mittel bereitgestellt und eine Vernetzung *zwecks Kooperation* angestrebt werden.

Tatsächlich werden aber neue Phänomene zu spät erkannt und die Kompetenzen und Mittel divergieren. Zudem gibt die öffentliche Hand ihr knappes Geld zunehmend für Soziales aus, weshalb in allen anderen Bereichen Geld fehlt. Die Kernprobleme der Inneren Sicherheit sind zwar erkannt, aber es *fehlt am politischen Willen*, sie zu lösen.

5.1 Es fehlt ein Konzept für die Innere Sicherheit

Um diese Defizite zu beheben, ist die Politik gefordert. Prioritär wird die *Koordination* und die *Fähigkeit zur Vernetzung* zwischen den einzelnen Sicherheitsorganen verbessert werden müssen. Sekundär ist ein *brauchbares Konzept zur Gewährleistung* der inneren Sicherheit bereitzustellen. Wie weit Raumsicherung und subsidiäre Sicherungseinsätze von Milizsoldaten Teile einer modern verstandenen Sicherheitsstrategie bilden, ist hoch umstritten. Immer wieder steht die Frage im Raum, ob für die Sicherstellung der Inneren Sicherheit die Armee tatsächlich im neuerdings vorgesehenen Ausmass gebraucht werde. So hat etwa der Zürcher Regierungsrat Ruedi Jeker diesen Mai zu bedenken gegeben, dass ihm Truppeneinheiten nur dann etwas nützten, wenn sie innert *48 Stunden eingesetzt* werden könnten und die entsprechende Mission – Überwachung, Sicherung und Kontrollen – über einen *längeren Zeitraum* hinweg zu erfüllen in der Lage seien.

Wirft man einen Blick auf die neuesten Anschläge in London vom 6. Juli 2005 im Lichte unserer nationalen sicherheitspolitischen Diskussion, so beleuchten diese dramatisch ein wiederholt vorgebrachtes Argument für den vorgeschlagenen Umbau der Armee: Das Ziel eines verbesserten Schutzes gegen terroristische Bedrohungen.

Seit Wochen waren die britischen Sicherheitskräfte in höchst möglicher Alarmbereitschaft. Grossbritannien ist der wichtigste Partner der USA im Irak. Einen Tag vor dem Anschlag begann der G8-Gipfel. Es ist davon auszugehen, dass von Seiten Grossbritanniens in dieser Situation alle *erdenklichen präventiven Massnahmen* ergriffen wurden, um terroristische Anschläge zu verhindern. Trotzdem führten die Terroristen erfolgreich eine offensichtlich koordinierte und von langer Hand geplante Anschlagsserie gegen das öffentliche Verkehrsnetz der britischen Hauptstadt durch, töteten Dutzende, verletzten Hunderte und legten den öffentlichen Verkehr der Metropole für Tage lahm.

Es muss stark hinterfragt werden, ob eine *Neuausrichtung der Schweizer Milizarmee* gegen diese Art Bedrohung Sinn macht. Sicher kann und muss sie im Bereich des Konferenzschutzes ihre Dienste anbieten. Und sicher wird sie im Bereich der Nachsorge der Terroranschläge ihre Aufgaben finden (Absperren, Aufräumen, Absichern, etc.). Nur im Falle einer *ausreichend früh wahrnehmbaren Zuspitzung der Situation*, beispielsweise im Falle konkreter Anzeichen für Attentate, könnten aber Einsätze einer Milizarmee zur Unterstützung der Polizei überhaupt rechtzeitig organisiert werden. Wäre man schliesslich tatsächlich mit einem Terroranschlag konfrontiert, müsste dieses Zusammenspiel zwischen der Truppe und der Polizei möglichst rasch fugenlos vonstatten gehen. Weiss man, dass *diese Vernetzung und Koordination eben gerade nicht gegeben ist*, verwundert es nicht, dass es Polizeikommandanten gibt, welche der Verwendung von Truppenteilen für subsidiäre Sicherungseinsätze sehr kritisch gegenüberstehen.

Insgesamt ist aber die Miliz-Armee *kein Instrument gegen Terror*. Damit ist die Frage nicht beantwortet, was gegen diese Bedrohung unternommen werden muss: Hierzu fehlt ein Gesamtkonzept. Dass aber die Terrorbedrohung als Argument für den Armee-Umbau her halten muss,

erscheint nicht erst im Licht der Londoner Ereignisse *mehr als fragwürdig. Die Armee ist hier gezwungen, Lücken zu füllen, die sie eigentlich nicht füllen kann.*

5.2 Nationale und internationale Vernetzung

Die Ausarbeitung des integrierten Lagebildes liegt seit einigen Jahren beim Dienst für Analyse und Prävention (DAP) des Bundesamts für Polizei. Eine verstärkte Zusammenarbeit mit ausländischen Nachrichtendienst-Partnern und der *Abschluss internationaler Kooperationen* (Polizeiabkommen, Schengen etc.) bilden eine Massnahme, um den Kampf gegen die internationale Kriminalität zu verstärken. Die sicherheitspolitische Führung sollte mit einem permanenten Krisenstab in Form eines Kernstabes verstärkt werden. Auf die Schaffung eines Sicherheitsdepartements wurde seitens des Bundesrats und des Parlaments hingegen *zu Recht verzichtet*. Weitere Verbesserungsmassnahmen wurden jüngst vom Bundesrat beschlossen.

Die Verbesserung der internationalen Vernetzung der schweizerischen Sicherheitsorgane ist zu begrüssen; sie allein wird aber den Stand der Inneren Sicherheit nicht verbessern können, wenn diese nicht selbst auf eine leistungsfähige und verlässliche Vernetzung aufbauen wird. Zudem sind die gravierenden Lücken in den kantonalen Polizeikorps, welche die Armee provisorisch überbrücken muss, *dauerhaft zu schliessen*. Sicherheit ist auch standortwirksam: Die Schweiz darf kein Hort für internationale Terroristen oder Kriminelle werden. Zu viel steht auf dem Spiel, man denke nur an den Finanzplatz und seine Erfolgsbedingungen.

5.3 Kantonale und interkantonale Vernetzung

Die Kantone sehen sich mit einer veränderten Lage konfrontiert, die durch eine steigende Gefahr von extremistischen Aktionen und Tätigkeiten, Verkehrs- und Umweltkatastrophen gekennzeichnet ist. Die aktuellen Gefährdungen sind dabei als kaum verhinderbar, überraschend, schwierig vorhersehbar und mit hohem Schadenspotential behaftet zu charakterisieren.

Interkantonal arbeiten die Kantone seit einigen Jahren über regionale *Polizeikonkordate* zusammen. Sämtliche kantonalen Polizeikorps sind – mit Ausnahme von Zürich und Tessin – einen der vier Konkordaten der Zentralschweiz, der Ostschweiz, der Nordwestschweiz und der Westschweiz angeschlossen. Für grössere Einsätze als solche im Rahmen dieser Konkordate gibt es die Zusammenarbeit im *Rahmen der GIP* (Gesamtschweizerische Interkantonale-Zusammenarbeit bei besonderen Ereignissen), die Ende 2003 nach den Erfahrungen des G-8 Einsatzes in Evian geschaffen wurde. Dazu gibt es je ein *operatives und ein strategisches* Führungsorgan. Dies alles sind dem *Föderalismus abgerungene Hilfskonstruktionen*, die zwecks einer «politisch korrekten» Einbindung aller relevanten Stellen auch *überaus kompliziert* und *damit unzweckmässig* aufgebaut sind.

Bei den *präventiven Sicherungseinsätzen* bestehen nach wie vor ungelöste Probleme: Das Anforderungsprozedere für Armeeunterstützung ist unhaltbar lang und kompliziert. Aus Sicht der Kantone wird dieser Fall kaum je eintreffen. Präventive Raumsicherung wird als neuer Begriff eingeführt, aber *einsatzmässig nicht klar umschrieben*. Sie unterscheidet sich von subsidiären Sicherungseinsätzen im Wesentlichen durch die auf *Seiten der Armee liegende Einsatzkompetenz*, was aber nur mit Notrecht möglich ist. Deshalb fehlt es den Kantonen ebenfalls an diesbezüglichen Einsatzvorstellungen. Während im Rahmen der dynamischen Raumsicherung eine Gegenkonzentration gebildet wird, um einen symmetrischen Gegner abzuhalten, bleibt die präventive Raumsicherung unscharf. Das erstere ist klar eine militärische Aufgabe, die Einsatzverantwortung liegt beim Militär. Zur präventiven Raumsicherung bestehen grosse Fragezeichen: Welchen Sinn macht eine präventive Raumsicherung mit Militär, das von der Ausbildung und von der Ausrüstung her nur zum Polizeidienst geeignet ist? Wird je ein Kanton dem Militär für diese Einsatzform die Kompetenz übertragen? Die Frage stellen, heisst sie beantworten.

Die Armee kann sich beim präventiven Raumsicherungseinsatz auch «gemischte Zustände» vorstellen: entweder subsidiär oder mit der Einsatzführung betraut. Die Frage der Kompetenzen – wer kann entscheiden – ist aber bis heute ungelöst, ebenso die Frage des Kräfteeinsatzes. Die Kantone lehnen sich seit dem Entscheid des Bundesrates zu USIS 3 zurück und vertrauen einzig darauf, dass die Armee dann schon helfe. Die Behörden aller Stufen müssen sich heute ernsthaft Gedanken machen, wie ein bedrohter Raum im Einsatzfall «möbliert» wird. Geübt wurden derartige Situationen in den vergangenen Jahren immer weniger, so dass heute ein plötzlicher kon-

kreter Einsatz wohl im Chaos enden würde. So fehlen heute die strategischen Führungsübungen, die Krisen- und Stabsübungen auf Stufe Bund und Kantone, um die verantwortlichen Behörden aller Stufen auszubilden und zu schulen. In den Gesamtverteidigungsübungen auf Stufe Bund und Kantonen erhielten die Verantwortlichen seinerzeit einen 1:1-Eindruck der Realität und wurden sensibilisiert, dies natürlich vor einem anderen Bedrohungshintergrund. Der Stab Operative Schulung ist heute in der Schweiz erst wieder im Aufbau begriffen.

Bei den Rettungsdiensten fehlen Vernetzung und Koordination noch fast vollständig. Hier herrscht *dringender Handlungsbedarf*. Gerade im Bereich der zivilen Katastrophen könnten viele Menschenleben gerettet werden, wenn Vernetzung und Koordination vereinfacht und verbessert würden. Obwohl die Rettungsdienste als erste auf dem Schadenplatz sind, sind sie beispielsweise oftmals nicht in der Lage, ein brauchbares Lagebild weiterzugeben.

5.4 Ohne netzwerkzentrierte Ansätze nur Scheinlösungen

Man gewinnt den Eindruck, dass zwar alle involvierten Stellen an der *Inneren Sicherheit herumwerkeln aber niemand die Koordination wirklich übernimmt*. Es bleibt uns daher nichts anderes übrig, als an konkreten Ereignissen zu lernen. Die EM 2008 könnte ein derartiges Ereignis sein.

Solange die Experten es nicht schaffen, die Probleme einer breiten Öffentlichkeit zu vermitteln, ist es nicht verwunderlich, dass auch die *Politiker nicht angemessen reagieren*. Scheinlösungen, beispielsweise in Deutschland die Schaffung eines «Bundesamts für Flutkatastrophen» nach der Elbeflut, bewirken wenig Entscheidendes, solange die Kompetenzordnung nicht hinterfragt wird, die Rollenteilung unklar bleibt und vor allem keine Vernetzung hergestellt wird.

6 Fazit: London zeigt – die Politik ist gefordert!

Die heutige Bedrohungslage ist vielfältig und schwierig vorhersehbar, die Gefahren sind heterogen und vielfältig.

Die politischen Realitäten und die polarisierte Blockade führen dazu, dass zu *wenig adäquat gehandelt* und geführt wird. Erste Schritte dieser Bedrohungslage zu begegnen sind zwar eingeleitet, aber sie scheitern zunächst noch an den *politischen Realitäten*. Die fehlenden Finanzen und die unklare Kompetenzordnung bilden die grössten Hindernisse auf dem Weg zu einer Vernetzung der verschiedenen involvierten Stellen der Inneren Sicherheit. Eine gewisse Vermengung von Innerer und Äusserer Sicherheit bereitet Probleme bei der Wahl der Einsatzmittel. Verheerend war der Entscheid von USIS 3 auf den Verzicht, die kantonalen Polizeikorps aufzustocken und stattdessen auf die Armee zurückzugreifen. Dieser Entscheid hat die *Schweiz um Jahre zurückgeworfen.*

Es fehlt allgemein an politischem *Leadership im Bereich Sicherheitspolitik*. Die Prioritäten werden daher falsch gesetzt. *Das billige Konzept, einfach das Gros der Armee als Lückenbüsser vor die Botschaften zu stellen, und zu hoffen, es passiere nichts, ist falsch.* Die Armee ist im Bereich der Inneren *Sicherheit Ultima Ratio* und nicht das *Mittel der ersten Stunde* und *des täglichen Gebrauchs*. Die Strukturen zu ändern wird eine herkulische Aufgabe sein – die neue Zürcher Verfassung zum Beispiel stärkt die dritte Staatsebene unter dem Titel Gemeindeautonomie gerade auch im Polizeibereich. Eine Einheitspolizei wurde in Zürich mit einer 2/3-Mehrheit abgelehnt. Das Resultat bleibt sicherheitsmässig ein *unbefriedigender Flickenteppich*.

Fortschritte sind scheinbar unendlich zäh zu erzielen, weshalb eine politisch geführte Vernetzung der Sicherheitsorgane des Staates, zwischen Bund, Kantonen und Gemeinden, dringlich wäre. Es darf nicht sein, dass bei uns auch zuerst eine Katastrophe nach dem Muster von London oder Madrid passieren muss, bevor echte Fortschritte erzielt werden.

Verein Sicherheitspolitik und Wehrwissenschaft VSWW

Unsere Ziele
Der Verein Sicherheitspolitik und Wehrwissenschaft und seine Mitglieder wollen
- bekräftigen, dass die Schweiz auch in Zukunft ein militärisch ausreichend geschützter Raum bleiben soll,
- erklären, dass ein wirksamer Schweizer Beitrag an die Stabilisierung primär des europäischen Umfeldes eine glaubwürdige, kalkulierbare und umfassende Schweizer Sicherheitspolitik benötigt,
- herausarbeiten, dass die Schweiz nicht nur als Staat, sondern auch als Wirtschaftsstandort, Denk-, Werk- und Finanzplatz sicherheitspolitisch stabil bleiben muss, um weiterhin erfolgreich existieren zu können,
- darlegen, dass eine sichere Schweiz angemessene Mittel für ihre Sicherheitspolitik benötigt,
- aufzeigen, was für eine effiziente und glaubwürdige Armee im Rahmen des integralen Selbstbehauptungsapparates an Führungscharakter und Kompetenz, an Ausbildung, Ausrüstung und Organisation nötig ist,
- sich dafür einsetzen, dass künftige Reformen der Milizarmee und ihrer Einsatzdoktrin diesen Postulaten entsprechen.

Unsere Leistungen
Der Verein und seine Mitglieder verfolgen diese Ziele seit 1956 durch Informationsarbeit in Form von Studien, Fachbeiträgen, Publizität und Stellungnahmen (vgl. www.vsww.ch), Vorträgen, Interviews und Gesprächsbeiträgen.

So hat er wesentlich geholfen,
- gegen eine moderne Schweizer Sicherheitspolitik gerichtete Volksinitiativen und Referenden zu bekämpfen sowie
- Expertenbeiträge zu einer neuen Sicherheitspolitik und zu einer glaubwürdig ausgebildeten und ausgerüsteten Armee zu leisten.

Unsere Zukunftsvision
Wir wollen mit unserer Arbeit dazu beitragen,
- dass die Schaffung eines breit abgestützten inneren Konsenses im Bereich der militärischen Selbstbehauptung in der Schweiz gelingt und
- die gesellschaftliche, wirtschaftliche und politische Integration unserer Milizarmee auch in Zukunft intakt bleibt.

Unsere Finanzierung
Wir finanzieren uns durch Mitgliederbeiträge, Gönnerbeiträge, Spenden sowie Legate.

Unsere Publikationen
Finden Sie unter: www.vsww.ch

Sie erreichen uns unter:
Verein Sicherheitspolitik und Wehrwissenschaft, Postfach 65, 8024 Zürich
Internet: www.vsww.ch, Telefon: 01-266 67 67 oder Fax: 01-266 67 00

PC-Konto 80-500-4, Credit Suisse Zürich, Konto-Nr. 468809-01
Herzlichen Dank für Ihre Unterstützung!