

23. Nov. 2010

von jjunk

in Cyber Security,  
Militär,  
Sicherheitskultur,  
Strategie

Kommentare ( 7 )

## Neue Software, alte Hardware? Die NATO 3.0 als Risikomanager

von Gabi Schlag und Julian Junk

Auf dem NATO-Gipfel in Lissabon wurde soeben eine neue Sicherheitsstrategie beschlossen. Die Allianz werde nun „more effective, more engaged, and more efficient“ [[Quelle](#)], so NATO-Generalsekretär Anders Fogh Rasmussen. Ohne die Folgen dieser neuen Strategie bereits jetzt evaluieren zu können, so kann man doch festhalten, dass mit dieser Strategie tatsächlich ein sich seit geraumer Zeit abzeichnender Paradigmenwechsel seinen vorläufigen Höhepunkt gefunden hat: Die NATO 3.0 als Risikomanager.

3.0 – dies liest sich wie ein grundlegendes Software-Update. Und in der Tat: Während die NATO 1.0 in Zeiten des Kalten Krieges in erster Linie ein Verteidigungsbündnis war, rekurrierte die NATO 2.0 in den 1990er Jahren zunehmend auf einen erweiterten Sicherheitsbegriff. Die strategischen Konzepte aus den Jahren 1991 und 1999 wiesen über eine enge Definition von Artikel 5, dem Bündnisfall, hinaus: das transatlantische Bündnis stand nun exemplarisch für eine Sicherheitsgemeinschaft im Sinne von Karl W. Deutsch, die nicht nur gewaltfreie Beziehungen zwischen ihren Mitgliedern dauerhaft institutionalisierte, sondern im Notfall auch für den Schutz von Demokratie und Menschenrechten international militärisch aktiv wurde.

Anstatt klar umrissener Bedrohungen sieht sich die NATO spätestens seit den terroristischen Anschlägen am 11. September 2001 der Abschätzung diffuser Risiken gegenüber, wie Mikkel Rasmussen dies vor einigen Jahren bereits mit dem Begriff der „reflexive security“ andeutete. Zeigt sich schon seit 1991 eine stetige Erweiterung des Aufgabengebiets des Bündnisses vor dem Hintergrund von „out-of-area“-Einsätzen, so scheint die NATO 3.0 nun vollends die Rolle eines Risikomanagers zu übernehmen. Ein Themenfeld steht hierfür exemplarisch: Cyber Security, die Sicherheit im virtuellen Netz. Attacken auf Banken und Ministerien in Estland, angebliche chinesische Trojaner auf Rechnern von Bundesministerien und der Zusammenbruch von Steuerungscomputern westeuropäischer Stromnetze im Jahr 2007, Hackerangriffe von Nordkorea auf südkoreanische Regierungsserver und verseuchte georgische Regierungsrechner während des Kaukasuskrieges im Jahr 2009 und in diesem Jahr dann der StuxNet-Angriff auf iranische Atomanlagen haben die Wahrnehmung dieses Problems entscheidend verändert. Die Expertengruppe für das neue strategische Konzept unter der Leitung von Madelaine Albright kommt angesichts dieser sich häufenden Einschlüge zu dem Schluss: “The next significant attack on the Alliance may

### SOCIAL MEDIA



### SUCHE

### TWITTER FEED

In den nächsten Wochen bei uns: Eine Beitragsreihe zu #Cyberpeace. Großartige Autoren, spannende Posts! [@fiff\\_de](http://t.co/z54MUpBFNc) ungefähr 21 Stunden her von &s

Ein kleiner Konferenzbericht zur #doeff14 von @seditioni und ein großes Lob an die Organisator\_innen! <http://t.co/tUtscX4Vdg> 1. Dezember 2014, 10:08 von &s

### TAGS

well come down a fibre optic cable” [Quelle]. Dass solche Beschreibungen von Gefahren und Risiken nicht ohne Folgen bleiben, zeigt die Formalisierung einer “Cyber Defence Management Authority”, die Institutionalisierung eines “Cooperative Cyber Defence Centre of Excellence” und die Entscheidung, eine “Computer Incident Response Capability” aufzubauen. Trotzdem bleiben Fragen offen: Würde eine Cyber-Attacke den Bündnisfall auslösen? NATO-Generalsekretär Rasmussen möchte dies offen halten, der politischen Bewertung im Einzelfall überlassen und spricht hinsichtlich der Auslegung des Artikels 5 von einer “konstruktiven Ambiguität” [Quelle].

Was bedeutet das? Diese Ambiguitäten sind jeder Art des Risikomanagements inhärent. Die Allianz wird in Zukunft ein vollkommen neues Spektrum an Instrumenten der Sicherheitsmaximierung und Risikominimierung entwickeln, um diese Gefahren gemeinsam zu bewältigen. Bedrohungen werden diffuser, neue Risiken entstehen, die nach flexibleren und schnelleren Entscheidungs- und Konsultationsstrukturen verlangen. Geht also mit dem strategischen Software-Update auch die Anschaffung einer neuen Hardware, d.h. neuer Organisationsstrukturen, gar neuer ziviler und militärischer Fähigkeiten einher? Dies bleibt abzuwarten. Ein Software-Update baut in erster Linie auf bestehenden Bausteinen auf, aktualisiert diese im Kontext rasanter Entwicklungen. Verteidigungsfall und Sicherheitsprojektion, die Kernelemente von NATO 1.0 und NATO 2.0, bleiben als Aufgaben bestehen und werden auch weiterhin den Zusammenhalt der Alliierten bestimmen. Vor dem Hintergrund eines entterritorialisierten, inhaltlich erweiterten Sicherheitsbegriffes wird die Gewährleistung von Sicherheit in Zukunft aber zusätzlich eine Aufgabe der Risikoabschätzung und –minimierung erfordern. Ein Vorschlag, wie im Bericht der Expertenkommission angeführt, dem Generalsekretär und/oder dem Oberkommandierenden der Streitkräfte Entscheidungskompetenzen im Falle eines Cyber-Angriffs zu geben als auch die Mitte November stattfindende (dritte) „Cyber Coalition 2010 Exercise“, d.h. die Simulation eines Cyber-Angriffes gegen die NATO und ihre Mitgliedsstaaten, könnten jedoch eine Dynamik in Gang setzen, die das strukturelle Gefüge der Allianz – ihre Hardware – langfristig verändern werden. Mit dem Problem der Risikoabschätzung und -minimierung wird vor allem eine neue Organisationskultur einhergehen, die auf Kommunikation, Öffentlichkeit und Transparenz stärkeren Wert legen muss. Darauf scheint sich die Allianz bislang nicht ausreichend eingestellt zu haben. Ohne passende Hardware bleibt eine neue, anspruchsvolle Software jedoch wirkungslos.

Wie neu – und effektiv, engagiert und effizient – diese NATO 3.0 sein wird, bleibt also abzuwarten. Eine institutionelle Ausdifferenzierung und Flexibilisierung scheint unverzichtbar, wenn die NATO in Zukunft nicht nur Sicherheit in und für Europa, sondern global verwirklichen will. Institutionalisten wie Robert Keohane und Celeste Wallander mögen schlussendlich Recht behalten, dass die NATO als eine hybride Sicherheitsinstitution, seit ihrer Gründung zwischen Verteidigungsallianz und Sicherheitsmanager navigierend, die besten Voraussetzungen mitbringt,

BELIEBT KOMMENTARE NEU

Hell yeah, it's Political Science!  
Wissenschaftliche Podcasts

Das Internet darf ein cyberfreier  
Raum sein

Deutschlands Irak -Politik –  
Verantwortung nach außen,  
Intransparenz nach innen.

Wir haben Geburtstag!

„Mit Sicherheit nicht!“ Sexuelle  
Gewalt als politisches Mittel

## KATEGORIEN

Außenpolitik (59)

Bürgerkriege (16)

Cyber Security (40)

Demokratisierung (9)

Drohnen (15)

Humanitäre Interventionen (15)

Innere Sicherheit (24)

Interviews (10)

Katastrophen (4)

Konferenz (20)

Militär (27)

Pandemien (2)

Podcast (7)

Popkultur (20)

Sanktionen (8)

Security Culture (13)

Sicherheits-Kommunikation (14)

Sicherheitskultur (204)

Sozialwissenschaft Online (56)

um die neuen Risiken und Gefahren erfolgreich zu bewältigen. Im Lichte rückläufiger Verteidigungsetats der Mitgliedsstaaten, einer finanziell bedingten Verkleinerung der bürokratischen Strukturen der Allianz und einer kritischen Öffentlichkeit, die dem Einsatz in Afghanistan skeptisch bis ablehnend gegenüber steht, wird die NATO jedenfalls auch weiterhin an der Software ihres strategischen Konzeptes feilen müssen.

 Tags: [NATO](#), [Risikomanager](#), [Transparenz](#), [„out-of-area“-Einsätze](#)

[« Willkommen! »](#)

[Krieg im Internet? »](#)

[Stellenangebote \(41\)](#)

[Strategie \(10\)](#)

[Terrorismus \(14\)](#)

[Theorie \(2\)](#)

[Umwelt \(1\)](#)

[Versicherheitslichung \(21\)](#)

[Visualisierung \(5\)](#)

[Whistleblowing \(8\)](#)

[WikiLeaks \(17\)](#)

[WMD \(10\)](#)

[Zivilgesellschaft \(48\)](#)

## BLOGROLL

 [Arbeitskreis soziale Bewegungen](#)

 [Augen geradaus](#)

 [Dan Drezner](#)

 [Dart-Throwing Chimp](#)

 [David Campbell](#)

 [de.hypotheses.org](#)

 [Demokratieforschung Göttingen](#)

 [Duck Of Minerva](#)

 [Future and Politics](#)

[Hylaeon Flow](#)

 [Internet und Politik](#)

 [IR Blog](#)

 [Just Security Blog](#)

 [justsecurity.org](#)

 [Killer Apps](#)

 [Kings Of War](#)

 [netzpolitik.org](#)

 [shabka.org](#)

 [Terrorismus in Deutschland](#)

## 7 Kommentare zu “Neue Software, alte Hardware? Die NATO 3.0 als Risikomanager”

Christian Tuschhoff | 25. Nov. 2010 um 15:17 |

**#1**

Das ist ein interessanter und herausfordernder Beitrag! Allerdings sind die analytischen Kernbegriffe (z.B. NATO 3.0 = Risikomanager) mindestens genauso vage und ambivalent wie die politischen Formulierungen der neuen NATO-Strategie selbst. Damit lässt sich m.E. nicht begründen, dass NATO 3.0 eine neue/andere Qualität eingenommen hat als NATO 1.0 oder 2.0. Eine Wesensveränderung der Organisation liegt schon deshalb nicht vor, weil der Kern der NATO nach wie vor die Beistandsgarantie nach Artikel 5 ist. Der Umgang mit neuen Herausforderungen/Bedrohungen ist ein Randphänomen, keine Wesensveränderung. Der zweite Grund dafür, dass keine Wesensveränderung vorliegt, ist darin zu sehen, dass auch NATO 1.0 oder 2.0 sich mit allerlei Randphänomen beschäftigt hat wie es der cyber war heute ist. Insofern war die NATO immer auch ein Risikomanager. Das leuchtende Beispiel dafür ist der Harmel Bericht und die damit einhergehenden institutionellen Veränderungen/Erneuerungen. Hier lassen sich sicherlich dieselben “wesensverändernden” Mechanismen beobachten. Ich selbst komme jedoch zu einer ganz anderen Schlussfolgerung: Das Wesen der Institution NATO war und ist seit jeher sehr viel komplexer und vielschichtiger. Nur sind diese Schichten nicht für jedermann und jederzeit sichtbar. Deshalb mag es sein, dass die NATO 3.0 nur neu erscheint, jedoch im Kern die NATO 1.0 ist. Nicht jede neue Softwareversion enthält auch wirklich neue Features!

ANTWORTEN

Matthias Dembinski | 25. Nov. 2010 um 15:23 |

**#2**

Auf dem Weg ins Phantasieland: Die NATO und das neue strategische Konzept Entgegen den Verkaufsbemühungen ihres Generalsekretärs weist das neue Strategische Konzept der NATO nicht die Richtung, sondern ist ein Manifest der Orientierungslosigkeit. Die Lebensdauer von NATO 3.0 dürfte daher deutlich kürzer sein als die entsprechenden Produkte aus dem Hause MS; die Gefahr eines Absturzes aufgrund von Programmierungsfehlern umso höher. Die Orientierungslosigkeit ist zum Teil der Tatsache geschuldet, dass die Interessen der

Mitglieder auseinanderdriften, zum Teil ist sie der Suche eines aktivistischen Generalsekretärs nach neue, öffentlichkeitswirksamen Aufgaben für seinen Verein zuzuschreiben. Um das an wenigen Beispielen zu demonstrieren.

(1) Im Verhältnis zu Russland verkündet der Generalsekretär, meines Erachtens zu recht, das Land sei keine Bedrohung, sondern ein strategischer Partner und künftiger Bundesgenosse. Einige der neuen Mitglieder sahen im Kaukasus-Krieg den Beginn eines neuen und aggressiven russischen Revisionismus und brachen eine Debatte über die Unterfütterung des Artikel 5 durch zusätzliche militärische Maßnahmen vom Zaun. Das strategische Konzept stellt einfach beides nebeneinander. Russland ist Partner, und die territoriale Verteidigung einschließlich contingency planning, Übungen und mobile Verstärkungen ist plötzlich wieder in aller Munde. Und diese Vorsorgemaßnahmen richten sich natürlich nicht gegen Marokko oder Österreich.

(2) Neben der kollektiven Verteidigung gegen Bedrohungen, die es nicht gibt, soll das Krisenmanagement wie seit den 1990er Jahren das zweite große Betätigungsfeld bleiben. Die NATO lernt (scheinbar) und hat entdeckt, dass sich Krisenmanagement nicht allein mit militärischen Instrumenten machen läßt, sondern hierfür in erster Linie zivile und polizeiliche Mittel von Nöten sind. Also kündigt sie ihren großangelegten Wandel in diese Richtung an. Dieses Zukunftsmodell der NATO als multidimensionaler Krisenmanager übersieht allerdings, dass die politischen Grundlagen für das out-of-area Engagement mit rapider Geschwindigkeit erodieren. Der Krieg der USA (und in ihrem Schlepptau der NATO) in Afghanistan dauert nun schon neun Jahre. An diesem Samstag werden die USA die Verweildauer der UdSSR am Hindukusch, das zum sowjetischen Vietnam wurde, überschreiten. Und ein Ende, geschweige denn ein irgendwie als Erfolg verkaufbarer Ausgang, ist nicht in Sicht. Wer glaubt, die Mitgliedsländer der NATO würden sich noch einmal auf ein derartiges Abenteuer einlassen, und die NATO solle sich mit comprehensive approaches und ähnlichem darauf einstellen, lebt in einer Scheinwelt.

(3) Entgültig ins Phantasieland gerät die NATO mit der Raketenabwehr. Nicht nur die Bedrohung und die technische Leistungsfähigkeit der Abwehrsysteme sind imaginiert; auch die Planungen der NATO selbst sind auf Sand gebaut. Die von Rasmussen wie das Kaninchen aus dem Hut gezauberte Zahl von 200 Mio. Euro, verteilt über zehn Jahre, zum Aufbau einer vernetzten Infrastruktur der nationalen Abwehrsysteme verschleiert, dass es bei den europäischen NATO-Mitgliedern außer ein paar Patriots mit zweifelhaften Fähigkeiten nichts zu vernetzen gibt. Die Systeme, die die USA im Rahmen des phased adaptive approaches anbieten, wären zwar sehr viel leistungsfähiger, aber auch teurer. Diese Sache hat damit ebenfalls einen Haken. Das von Bush in Polen und Tschechien geplante System sollte Teil der nationalen amerikanischen Abwehr zur Verteidigung von iranischen Raketen mit langen Reichweiten sein. Obamas System soll die Europäer gegen die wahrscheinlichere Gefahr schützen, dass es dem Iran gelingt, funktionsfähige Mittelstreckenraketen zu bauen. Und wer jetzt glaubt, der US-Kongress werde mit amerikanischen Steuergeldern ein Raketenabwehrsystem finanzieren, das exklusiv die Europäer schützt, hat die Rechnung ohne die Tea-Party gemacht. Real bewirkt wird das ganze Gerede über Raketenabwehr nur eines: nämlich die fragile Annäherung an Russland gefährden.

Matthias Dembinski siehe auch den HSFK-Standpunkt [Auf der Suche nach Orientierung](#)

ANTWORTEN

 theorieblog.de

 Verfassungsblog

 Vom Bohren harter Bretter

 whistleblower-net.de

## ARCHIV

Wähle den Monat

Leinad Resiak | 26. Nov. 2010 um 0:31 |

**#3**

Das Programm-Update beseitigt die selbst geschaffenen Bugs!

Äußerst interessant bei dieser ganzen Diskussion ist es, dass die Bedrohungen, denen sich das Militärbündnis ausgesetzt sieht, als neue, von außen hereingetragene Risiken und das gesamte System bedrohende "Viren" gesehen werden. Selbstverständlich bedarf es zur

Abwehr dieser Gefahren eines regelmäßigen Updates. Dabei sollte jedoch nicht vergessen werden, dass sich das Programm durch seine eigene Programmierung und dieser immanenten, penetranten Ausbreitung seine eigenen Probleme schafft. Ist nicht die digitale Welt, in welcher nun adäquate Antworten auf terroristische und staatliche Cyber-Angriffe gefunden werden müssen, nicht gerade im Herzen des Verteidigungsbündnisses entworfen worden? Und wurde und wird das selbst entworfene System nicht auch aus Herzenslust für eigene "strategische Sicherheitsmaßnahmen" instrumentalisiert? Das gleiche gilt für den "gefährlichen" und "unheimlichen" Nahen Osten und die sogenannte arabische Welt. Hat nicht das "Verteidigungs-"programm NATO, sei es in seiner Beta-Version oder später in seiner ganzen Pracht und Macht, nicht auch eine Gegenreaktion provoziert? Letztendlich soll dieser Beitrag jedoch nicht pure Polemik sein, vielmehr würde ich mir eine konstruktive Diskussion innerhalb der NATO und um sie herum wünschen, die einen weniger imperialistischen und eurozentristischen Sicherheitsbegriff zumindest kurz reflektierte. Die (nicht nur) auf dieser Plattform stattfindende Diskussion dreht sich in meinen Augen doch zu sehr um marginale Anpassungen von Programm-Features, anstatt einmal über eine innovative Neuausrichtung oder gar ein völlig neues, den aktuellen Herausforderungen einer globalisierten und größtenteils marginalisierten Welt entsprechendes Programm nachzudenken!  
Ganz abgesehen davon, dass die Systemanforderungen (zum Glück) nicht auf der Verpackung stehen...

ANTWORTEN

Tobias Bunde | 26. Nov. 2010 um 19:08 |

**#4**

— Zunächst vielen Dank an die Initiatoren des Blogs – eine sehr gute Idee! —  
Die NATO aus dem Blickwinkel der These der "Risiko-Gesellschaft" zu betrachten, ist in der Tat interessant. Allerdings würde ich Christian Tuschhoff insofern zustimmen, als es mir ebenfalls eher fraglich erscheint, gerade das Ergebnis des Lissabon-Gipfel als Manifestation der Risiko-NATO zu begreifen. Auch die Sprache der beiden anderen Strategischen Konzepte nach dem Ende des Ost-West-Konflikte ist schon sehr deutlich vom Risiko-Gedanken geprägt.  
Besonders spannend finde ich jedoch die Frage, wie das Denken in Risikokategorien den Zusammenhalt und die Anpassungsfähigkeit der Allianz beeinflusst. Man könnte argumentieren, dass der Übergang von "Bedrohung" zu "Risiko" hier nachhaltige Veränderungen in Gang gesetzt hat, weil es den Mitgliedstaaten angesichts diffuser Risiken immer schwerer fällt, eine gemeinsame Position zu entwickeln. In gewisser Weise kann man ja auch die Raketenabwehrpläne kritisch als Versuch verstehen, neue Unklarheiten durch eine alle vereinende Bedrohung zu ersetzen, die das Bündnis zusammenhalten könnte.  
Kritisch an den Strukturierungen nach NATO 1.0 etc. oder auch NATO I bis IV, wie man sie ab und an in der Literatur findet, finde ich vor allem, dass sie nicht zuletzt insofern zu stark vereinfachen, als damit (wie von Christian Tuschhoff angesprochen) Kontinuitäten verschleiert werden und – in meinen Augen noch wichtiger – Ungleichzeitigkeiten überdeckt werden. Vielleicht ließe sich die NATO viel besser verstehen, wenn man sie als Institution betrachtete, die nicht nur selbst in verschiedenen "Versionen" existiert, sondern deren Mitglieder auch gerne unterschiedliche Versionen benutzen möchten (vgl. Schwerpunkt der mittel- und osteuropäischen Staaten auf "reassurance" etc.). Im Übrigen ein gutes Beispiel für unterschiedliche "Sicherheitskulturen"...

ANTWORTEN

Florian Roth | 30. Nov. 2010 um 16:22 |

#5

Nachdem das Thema ‚Risiko‘ jahrzehntelang ein Schattendasein in der sicherheitspolitischen Forschung gefristet hat und primär die Risiken von Atomenergie, Chemieindustrie und genveränderten Lebensmitteln (u.ä.) betrachtet wurden, erscheint eine Rückführung auf das sicherheitspolitische Feld angesichts der Komplexität der gegenwärtigen Probleme und der Unsicherheiten der Lösungswege überfällig; schließlich gibt es mehr als genügend Anknüpfungspunkte im Forschungsfeld, von Machiavellis ‚Fortuna‘ bis zu von Clausewitz’ ‚Nebel des Krieges‘. Kritisch sehe ich die Versuche, die Veränderungen in der globalen Sicherheitsarchitektur als eine Ablösung von Bedrohungen durch Risiken zu deuten (in diesem Punkt ist die LSE-Schule aus meiner Sicht zu sehr dem Narrativ ihres Mentors Beck gefolgt). Mögen sie auch in jüngerer Zeit verstärkte Aufmerksamkeit erhalten haben, präventive und präemptive Strategien sind ebenso wenig neu wie global interdependente Sicherheitsprobleme oder die ‚unintended consequences‘ von Sicherheitsmanagement. Die eigentliche Veränderung findet weniger im realen Bedrohungsspektrum als vielmehr in der Risikoperzeption, aber insbesondere auch in der Risikoakzeptanz der zentralen Akteure statt. Wie die Afghanistan-Mission eindrücklich zeigt lassen sich Risiken kaum minimieren, sie lassen sich lediglich gegeneinander abwägen, priorisieren und im besten Fall auf Dritte transferieren, wie Martin Shaw treffend beschrieben hat. Kennzeichen der jüngeren westlichen Militärinterventionen ist ein komplexes Geflecht, das sich u.a. aus strategischen, operativen, ökonomischen, innenpolitischen und moralischen Risiken zusammensetzt – wobei aus meiner Sicht die beiden letztgenannten Risikotypen die größten Herausforderungen für den Zusammenhalt der NATO darstellen.

Die Probleme der NATO-Entwicklungsabteilung eine Software zu entwickeln, die den unterschiedlichen Nutzeranforderungen gerecht wird, sind offensichtlich. Ein Ausweg könnte in einer transparenten und partizipativen Organisationskultur – im Sinne einer ‚Open-Source-NATO‘ – liegen.

ANTWORTEN

Gabi Schlag | 1. Dez. 2010 um 16:15 |

#6

Die Hybridität der NATO:

In der Tat erscheint es allzu verkürzt, eine klare Trennlinie zwischen der NATO 1.0 bis 3.0 zu ziehen, wie Christian Tuschhoff dies treffend angemerkt hat. So besteht ein Erfolg der Allianz darin, nicht nur unterschiedliche Aufgaben zu erfüllen sondern auch unterschiedliche Sicherheitsinteressen der Mitgliedsstaaten zu kanalisieren, wie Tobias Bunde andeutet. In der politischen und akademischen Diskussion dominiert jedoch oftmals die Frage, ob die NATO ein Verteidigungsbündnis oder ein Risikomanager ist, anstatt davon auszugehen, dass die westliche Allianz sowohl der Verteidigung&nbsp;als auch des Risikomanagements dient. In diesem Sinne weist Florian Roth darauf hin, dass es nicht um eine Ablösung, sondern vielmehr Verschränkung von Bedrohungen und Risiken geht.

Seit ihrer Gründung vereint die Allianz nicht nur den Gedanken kollektiver Verteidigung wie er in Artikel 5 beschrieben ist, sondern das Prinzip gegenseitiger Konsultationen nach Artikel 4. Gerade diese Formen des Austauschs sind grundlegend für das zukünftige Risikomanagement als Gefahrenabwägung. Diese Hybridität der NATO könnte wesentlich dazu beitragen, dass die Orientierungslosigkeit des neuen Strategischen Konzeptes – wie Matthias Dembinski es nennt – kein Nachteil, sondern vielmehr Grundvoraussetzung für den Fortbestand der Allianz ist. Denn diese Uneindeutigkeit von gemeinsamen Zielen und Mitteln eröffnet mitunter auch die Möglichkeit, eine politische Diskussion des Für und Wider und somit eine demokratische Streitkultur innerhalb der NATO zu stärken.

&nbsp;

ANTWORTEN

Christian Tuschhoff | 6. Dez. 2010 um 17:39 |

#7

Ich stimme Gabi Schlag ausdrücklich zu, dass die "Orientierungslosigkeit" eine Streitkultur begünstigen kann. Viele andere Beobachter, z.B. Karl-Heinz Kamp, haben ja darauf hingewiesen, dass die Konsensfindung durch Kompromissformulierungen gestärkt worden sei. Insoweit wurde der politische Zusammenhalt der Allianz gestärkt und der Streitprozess hat durchaus das Potential, diesen Zusammenhalt dauerhaft zu festigen. Probleme sind jedoch dann zu erwarten, wenn Kompromissformeln in gegenseitige Verhaltenserwartungen umschlagen. Hier geht es darum, Beiträge zur kollektiven Verteidigung/Risikomanagement zu leisten. Die große Frage ist, ob es gelingt, kooperative Verfahren für Krisen und Konflikte zu entwickeln, die wechselseitige Verhaltenserwartungen stabilisieren. Wenn solche Verfahren für bestimmte Situationen existieren, kann es nur darum gehen, in Entscheidungen deren Bestand festzustellen, damit die vorbereiteten Maßnahmen eingeleitet werden können. Wenn diese Verfahren fehlen, müssen sie situativ geschaffen werden. Dies ist ein sehr ineffektiver Weg, der kaum geeignet ist, den Zusammenhalt der Allianz zu festigen.

ANTWORTEN

## Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Geben Sie den Text ein.





Icons for refresh and headphones.

Datenschutz - Nutzungsbedingungen

Benachrichtige mich über nachfolgende Kommentare per E-Mail.



Impressum | 

Dieses Werk bzw. Inhalt steht unter einer Creative Commons Namensnennung-NichtKommerziell-KeineBearbeitung 3.0 Unported Lizenz.  
Über diese Lizenz hinausgehende Erlaubnisse können Sie unter [redaktion@sicherheitspolitik-blog.de](mailto:redaktion@sicherheitspolitik-blog.de) erhalten