Verlegen und verlogen

Die Nato versucht krampfhaft, am Ideal einer harmonischen Zusammenarbeit mit Russland festzuhalten. Die jüngsten Entwicklungen mahnen zur Vorsicht. ***Von Jürg Dedial***

Im 62. Jahr seit ihrer Gründung erweckt die Nato immer mehr den Eindruck, dass ihr der tiefere Daseinszweck abhandenzukommen droht. Ihr ursprünglicher atlantischer Gemeinsinn im Kampf gegen eine reale sowjetische Bedrohung ist längst erodiert; die politische Stossrichtung ist verwässert, die Ressourcen sind überdehnt. Hinzu kommen immer grössere Finanzierungsprobleme. So ist längst nicht mehr nur die Rede vom «Warum» und «Gegen wen», sondern immer mehr vom «Wie». Die finanzielle Auszehrung ist jetzt in vollem Umfange sichtbar, da die Amerikaner ihr enormes Engagement nicht mehr aufrechterhalten können. Der abtretende Verteidigungsminister Gates hat dies unlängst mit drastischen Worten festgehalten. Ein leichtes, kurzes Schaudern ging damals durch die Reihen der europäischen Partnerländer, mehr nicht. Es fehlen einfach der tiefere Zweck und die gemeinsame Überzeugung, dass die Sicherheitserfordernisse vielleicht anders definiert werden müssen, dass sie aber keineswegs obsolet sind.

Die Crux der Gleichberechtigung

Dies ist in den letzten Wochen bei den beiden Hauptthemen, mit denen sich die Nato konfrontiert sieht, der Raketenabwehr und Libyen, wieder deutlich geworden. Schon seit längerem geistert das Problem einer potenziellen Bedrohung durch Mittel- und Langstreckenraketen aus Schwellenländern durch die Korridore der verschiedenen Nato-Gremien. Die Frage lautet ganz einfach, ob man das Risiko in Kauf nehmen könne, dass irgendein Hirnloser in einem verrückten Staat («rogue state») auf den Knopf drückt und ein oder mehrere Missile auf einen europäischen Staat loslässt. Keineswegs überraschend meldete Russland sogleich seine Opposition gegen konkrete Pläne an, und in der Nato, der Russland bekanntlich nicht angehört, stieg der Puls beträchtlich.

Die Sache wurde dadurch kompliziert, dass die Hardware, nämlich einsatzfähige Abfangraketen, vorderhand nur in den Arsenalen der Amerikaner zu finden sind. Dies war der Nährboden für die Verlegenheit, die jetzt unter europäischen Nato-Mitgliedern herrscht, wenn es um die Frage geht, wie man eine Raketenabwehr des Bündnisses in die Realität umsetzen könnte. Die russische Diplomatie, unterstützt von freizügig polternden Militärs, nützt die latent amerikafeindlichen und -skeptischen Ressentiments weidlich aus, was die Verunsicherung in einigen westlichen Ländern wie zum Beispiel Deutschland noch erheblich steigerte. So kam man auf die ebenso trügerische wie verlogene Formel, dass eine Raketenabwehr der Nato nur in engster Kooperation mit Russland entwickelt werden könne – womit man fast schon den Bock zum Gärtner im eigenen Äckerchen machte.

Der Lauf der Dinge hat dies immer wieder bestätigt. Längst ist klar, dass es Russlands vorrangiges Ziel ist, eine Nato-Raketenabwehr zu verhindern. Da dies kaum zu erreichen sein wird, versucht es, mit der Forderung nach einer gleichwertigen Beteiligung an der Aufstellung von Abfangmissilen in die Kommandostruktur eingebunden zu werden. Moskau verspricht sich dabei nicht zuletzt eine Veto-Position und den Transfer von fortgeschrittener Technologie. Dies wiederum werden die Amerikaner nie zulassen. Sie wollen der Nato hochmoderne Systeme zur Verfügung stellen, deren Geheimnisse sie nicht mit den Russen teilen werden. Damit aber wird der Eiertanz um eine «vollwertige» russische Partnerschaft endgültig absurd.

In den letzten Tagen hat man sich in Sotschi einmal mehr zu einem der westöstlichen Rituale scharf kalkulierter Unnahbarkeit getroffen. Der dänische Nato-Generalsekretär Rasmussen wand sich förmlich um eine Antwort auf die Frage, warum man die Zusammenarbeit mit den schwierigen Russen nicht revidiere. Er musste zugeben, dass es zahlreiche Hindernisse gebe und dass die Verhandlungen mit Moskau «kompliziert» seien.

Salven aus Sotschi

Dies ist kaum übertrieben, wenn man die Salven betrachtet, die am Schwarzen Meer auf die Bündnismitglieder losgelassen wurden. Da wurde die Drohung mit dem Aufbau eines eigenen Raketenabwehrsystems aufgewärmt, wenn die Nato nicht spure, ferner werde man sich überlegen, aus dem Abkommen über die Reduktion der strategischen Waffen (Start) auszusteigen, und schliesslich folgte noch der eher rüde Hinweis, man könnte die Aufstellung neuer Kurzstreckenraketen entlang der östlichen Nato-Grenzen ins Auge fassen. Dass diese Drohungen mit einem Rundumschlag gegen die Nato-Luftangriffe in Libyen unterfüttert wurden, erstaunt kaum, obwohl man sich fragt, weshalb die Russen weiland die Sicherheitsratsresolution 1973 gegen Ghadhafi möglich machten. Niemand wird ernsthaft erwägen, nicht mit Russland zusammenzuarbeiten. Aber angesichts immer schwierigerer interner Probleme wäre es für die Allianz schon ein Fortschritt, wenigstens nach aussen mit geschlossenen Reihen und weniger blauen Augen aufzutreten.

Die Buchpreisbindung als rostige Abwehrwaffe

Das Referendum gegen die Buchpreisbindung wird zu einer breiten Debatte über Handelsbeschränkungen und die Rolle grosser deutscher Verlage führen. ***Von Beat Gygi***

Das Thema Buchpreisbindung wird in der Schweiz bald auch in die breite Diskussion gelangen, nachdem soeben das Referendum gegen das Gesetz zu deren Wiedereinführung zustande gekommen ist. Was das Parlament im März mit der Verabschiedung des «Gesetzes über die Buchpreisbindung» als branchenspezifische Abwehreinrichtung konstruiert hat, wird nächstens vor einem breiteren Hintergrund zu diskutieren und gründlich zu überprüfen sein. Es ist zu erwarten, dass sich die Debatte unter Beteiligung des «grossen Publikums» anders entwickeln wird als die bisherige, eher von gut organisierten Interessengruppen geprägte Diskussion unter Bundespolitikern. Diese haben zwar auch immer wieder von vermuteten Bedürfnissen des Publikums gesprochen, dieses kam aber bisher im politischen Prozess nicht selber zu Wort – sondern nur im Markt, aber der Markt zählt für die «Buchpreisbinder» ja nicht als Orientierungshilfe.

Was soll man mit alten Kanonen tun?

Jedenfalls wirkt die von den Politikern nach einer parlamentarischen Initiative entworfene Konstruktion zur Abwehr von Wettbewerb und Vertragsfreiheit in der Buchbranche wie ein Versuch, die Zeit aufzuhalten, mit altmodischem Gerät gegen moderne Entwicklungen anzukämpfen und jüngst erweiterte unternehmerische und kreative Spielräume von Lesern, Autoren, Verlegern und Händlern wieder einzuschränken. In gewisser Hinsicht weckt dies unwillkürlich Gedanken an Anachronismen im Militär, etwa an Situationen, in denen man vor der Frage steht, was man mit grossen und teuren Festungskanonen anfangen soll, die zwar imposant aussehen, aber gegenüber neuer Technik machtlos sind. In der Schweizer Armee kam es jüngst immerhin so weit, dass die Experten selber zum Schluss gelangten, solche Kanonen seien von geringem Nutzen und aus dem Dienst zu nehmen.

In der Bundespolitik und Teilen der Buch- und Medienbranche dagegen haben sich die traditionellen Defensiv-Experten und -Interessenvertreter nochmals durchgesetzt und den Versuch unternommen, die bereits früher einmal eingesetzte und dann abgeschaffte Abwehrwaffe Buchpreisbindung so weit zu modernisieren, dass sie auch im Internet-Zeitalter ihre Wirkung entfalten möge. Dass man dabei Altmodisches ziemlich behelfsmässig zu modernisieren suchte, zeigt etwa die Regelung, wonach nicht nur der traditionelle Vertrieb von Büchern, sondern auch der Internet-Buchhandel in die Buchpreisbindung einbezogen werden soll. Richtig unter Kontrolle bringen lässt sich aber die elektronische Welt doch nicht: Als «Buch» gilt laut verabschiedetem Gesetzestext nämlich «jedes Verlagserzeugnis in gedruckter Form und jedes kombinierte Erzeugnis, bei dem das Verlagserzeugnis in gedruckter Form die Hauptsache bildet».

In der Print-Welt verhaftet

Die Buchpreisbindung – so, wie sie vorgeschlagen ist – bleibt also im Gedruckten verhaftet und wird beim Übergang in die elektronische Welt wohl kaum richtig mithalten können. Texte und andere Inhalte, die primär in elektronischer Form, auf Lesegeräten oder Computern, in den Markt gelangen, erscheinen bereits nicht mehr so einfach hoheitlich «einfangbar». Dies ist immerhin eine gute Nachricht für viele Konsumenten bzw. Leser sowie für Befürworter einer etwas freieren Ordnung, zumal man mit fortschreitender Entwicklung der Technik mehr oder weniger automatisch näher zu Marktordnungen gelangen dürfte.

Dies bedeutet allerdings nicht, dass man die bisherigen Argumente gegen die Buchpreisbindung aus dem Blick verlieren darf. Die früher erarbeiteten Analysen und Entscheidungen etwa von Wettbewerbskommission und Rekursinstanzen haben weiterhin ihre Gültigkeit. So ist im Gedächtnis zu behalten, dass die Buchpreisbindung als Einengung des Wettbewerbs eher grossen Akteuren der Branche zugutekommt als kleineren, wendigeren und innovativeren Verlagen oder Autoren, die in jüngerer Zeit die neue Freiheit schätzen gelernt haben. Primär sind es allem Anschein nach deutsche Grossverlage, denen das neue Gesetz zur Stabilisierung ihrer Preissetzungspolitik und zu Mischrechnungen zulasten der Schweizer Leser dient.

Pikant daran ist, dass dies im Nationalrat mit «Kulturförderung» sowie «Strukturerhaltung bedrohter Wirtschaftszweige» begründet wurde, während der Ständerat nur die «Strukturerhaltung» und der Bundesrat weder das eine noch das andere als Anknüpfungspunkt sah. Wahrscheinlich werden die Konsumenten bzw. Leser den Interessenvertretern und den im Namen von Kultur und Vielfalt auftretenden Politikern zu verstehen geben, dass sie diesen Fall ähnlich sehen wie der Bundesrat.

Ein internationaler Kodex für Cyber-Konflikte ist überfällig

Die neuen Bedrohungen im Internet wie Cyber-Spionage und Cyber-Konflikte lassen sich mit traditionellen Instrumenten der Sicherheitspolitik kaum abwehren. Erforderlich ist ein internationales Regelwerk, das Standards setzt für das Verhalten von Staaten im Cyberspace. ***Von Daniel Stauffacher, Riccardo Sibilia und Barbara Weekes***

Zu den Sorgen, die sich Nationen rund um den Globus zur Umwelt machen, zur Finanzkrise, zu Armut und Naturkatastrophen, kommt eine Herausforderung dazu: eine invasive, mehrschichtige Bedrohung in Form eines modernen Wettrüstens. Doch Akteure und Waffen sind unsichtbar. Charakteristisch für diese Gefahr ist eine ansteigende Anzahl von Attacken. Die Stabilität unserer globalen Computer-Netzwerke sowie das einwandfreie Funktionieren unserer Länder, Städte und täglichen Aktivitäten hängen vom Internet ab. Wichtige Infrastrukturen – wie zum Beispiel das Verkehrswesen, die Nuklearanlagen, Elektrizitäts- und Kommunikationsnetzwerke, Ölpipelines sowie Finanzinstitute – sind zu Zielen von Computer-Attacken geworden. Angriffe dieser Art könnten verheerende Auswirkungen für die Menschheit haben. Die internationale Gemeinschaft tut nicht genug, um dem gegenwärtigen Anstieg der Cyber-Attacken zuvorzukommen.

Offensive und defensive Komponenten

Das Internet ist ein globales und allgemeines Gut, das geradezu eine Explosion der Innovation, des Unternehmergeistes, der Kommunikation und des Ideenaustauschs bewirkt hat. Um Angriffe auf diesen Kernbereich unserer modernen Gesellschaft abzuwehren, sind vereinte Kräfte nötig – ein gemeinschaftlicher und offener Dialog, um eine gemeinsame Basis und Lösungen zu finden. Die Natur der Bedrohung erschwert das Finden von wirksamen Abwehrstrategien. Cyber-Attacken erfolgen anonym und stammen oft von nichtstaatlichen Akteuren. Es ist beinahe unmöglich, jemandem die Attacke in rechtlich einwandfreier Form nachzuweisen. Auch ist es schwierig, Attacken zu erkennen. Sie können jahrelang unentdeckt bleiben und geben dem Angreifer die Möglichkeit, den Angriff einem Dritten in die Schuhe zu schieben. Cyber-Angriffe erfolgen unmittelbar und weltweit. Datenmengen erreichen die ganze Welt in weniger als einer halben Sekunde. Wir stehen vor einer neuen Art von Konflikt, in dem es einfacher ist zu attackieren, als sich zu verteidigen. Wie können wir mit dieser Asymmetrie umgehen? Was bedeutet dies für die hergebrachten sicherheitspolitischen Konzepte wie Abschreckung und das Gleichgewicht der Kräfte?

Wir müssen uns die Frage stellen, ob die internationale Gemeinschaft Verhandlungen über «Cyber-Abrüstung» nach dem Muster der traditionellen Rüstungskontrolle beginnen sollte. Doch diese traditionelle Herangehensweise funktioniert im Internet nicht. So haben nahezu alle Instrumente, die man als «Waffen» im Cyber-Konflikt bezeichnen könnte, auch eine defensive und zivile Seite. «Waffen» wie zum Beispiel Malware (bösartige Software)und Backdoors (von den Programmierern absichtlich geschaffene Schwachstellen) können unter dem Deckmantel einer legitimen zivilen Nutzung entwickelt werden, taugen dann aber für das ganze Spektrum an Cyber-Angriffen von der Kriminalität über die Spionage bis hin zu unmittelbar militärischen Anwendungen.

Gestützt auf den World Summit on the Information Society und mit der United Nations Millennium Declaration on peace, security and disarmament im Hinterkopf sollte die globale Gemeinschaft stattdessen einen nicht bindenden Verhaltenskodex für den Cyberspace entwickeln. Dieses Regelwerk würde die internationalen Dos and Don'ts für das Verhalten im Cyberspace in Friedens- wie in Kriegszeiten beschreiben. Der Verhaltenskodex müsste vor allem das Prinzip verbindlich machen, wonach eine Cyber-Attacke gegen einen anderen Staat einen Verstoss gegen internationales Recht darstellt.

Diese Selbstverpflichtungen müssten festhalten, was die Staaten dürfen und was sie unterlassen müssen – und zwar sowohl, wenn sie Beteiligte eines Cyber-Konfliktes sind, als auch, wenn sie nur mittelbar in die Auseinandersetzung involviert sind. So können sich in einem Staat Server befinden, auf denen Inhalte einer Konfliktpartei verwaltet werden, oder eine Regierung gerät in die Situation, dass sie auf Servern in ihrem Hoheitsgebiet bestimmte aggressive Inhalte aus Drittstaaten blockieren will. Der Kodex würde ebenfalls die Rolle von privatwirtschaftlichen Firmen in Cyber-Konflikten regeln. Er wäre zugleich eine Referenzgrösse für internationale Definitionen und Rechtsnormen in allen Bereichen der Cyber-Sicherheit.

Die Staaten müssen dem Thema Computer-Sicherheit Priorität einräumen und Cyber-Diplomatie auf bilateraler wie internationaler Ebene betreiben. Neben dem erwähnten Verhaltenskodex sollten bilaterale Vereinbarungen zur Einschränkung von Cyber-Attacken abgeschlossen werden. Weil niemand genau weiss, wie gross die Fähigkeiten bestimmter Staaten im Bereich der Cyber-Kriegführung sind, erodiert das zwischenstaatliche Vertrauen. Dem muss durch mehr Transparenz und Vertrauensbildung entgegengewirkt werden. Cyber-Kooperation und Cyber-Diplomatie sollten zur Regel werden und nicht mehr die Ausnahme sein.

Die Freiheit steht an erster Stelle

Entscheidend für einen internationalen Effort zur Förderung des Cyber-Friedens sind die Fähigkeit sowie die Ressourcen, um die Aktivitäten der Staaten zu verifizieren, die dem Verhaltenskodex zugestimmt haben. Eine internationale und unabhängige Institution sollte ins Leben gerufen werden – oder in eine bereits bestehende Organisation integriert werden –, um tatsächliche oder vermutete Verstösse gegen den Verhaltenskodex zu überprüfen. Bei allen Anstrengungen muss aber eines berücksichtigt werden: Cyber-Sicherheit ist zwar von grosser Bedeutung, auch haben die Bürger das Recht, ihre Computer unter sicheren Bedingungen zu nutzen. Aber alle Lösungen dürfen unter keinen Umständen die Freiheit im Netz einschränken oder das aus unserem Leben nicht mehr wegzudenkende Internet in seiner Bedeutung beschneiden.

Daniel Stauffacher ist Vorsitzender der ICT4Peace Foundation und früherer Schweizer Botschafter. **Riccardo Sibilia** ist Chef Cyber-Bedrohungsanalyse im VBS in Bern. **Barbara Weekes** ist Leiterin des Geneva Security Forum.