INHALT

Seite

I. EINFÜHRUNG

1. In den Monaten seit dem 11. September hat sich allgemein die Erkenntnis durchgesetzt, dass die Netzwerke, über die Terroristen ihre Angriffe planen, ein hohes Maß an Komplexität erreicht haben. Vor kurzem wies Thomas Homer Dixon von der Universität Toronto in einem Artikel auf das „grausame Paradoxon" moderner Gesellschaften hin: Während technologische Innovationen einigen zu schnellem Reichtum und Wohlstand verhelfen können, macht diese neuartige vernetzte Welt die hoch entwickelten Staaten für potenzielle Angreifer überaus verwundbar. Da die entscheidenden Einrichtungen in unseren stark vernetzten Gesellschaften an bestimmten Standorten dicht an dicht liegen, kann ein unerwarteter Angriff besonders schwere Folgen haben. Darüber hinaus ist mit der technischen Entwicklung das Zerstörungspotenzial für kleine Gruppen und für Einzelne stetig gewachsen. Kurz gesagt: Die Technologie ist ein zweischneidiges Schwert.

2. In seinem letztjährigen Bericht [AU 221 STC/MT (01) 5 rev. 1] umriss Michael Mates, der damalige Berichterstatter dieses Unterausschusses, die sich ändernden Beweggründe, Mittel und Strukturen terroristischer Organisationen. Er verwies auf das Auftreten einer „neuen" Form des Terrorismus, die sich aus religiösen oder anderen ideologischen Quellen speist, aber keine klaren politischen Ziele verfolgt. Ein Grundmerkmal dieses „neuen" Terrorismus sind die tödlicheren Folgen seiner Angriffe, die nicht mehr – wie bei „herkömmlichen" Terroristen – darauf abzielen, gerade soviel Gewalt anzuwenden, wie nötig ist, um Aufmerksamkeit für die eigene Sache zu wecken, sondern die jeweiligen Feinde strafen und möglichst viele von ihnen töten sollen.

3. Die veränderten Beweggründe haben auch Änderungen der Organisation und der Struktur der Terrorgruppen mit sich gebracht. Herr Mates beschrieb ihren Organisationsaufbau als segmentiertes, polyzentrisches und ideologisch integriertes Netzwerk (SPIN), eine Definition, die ursprünglich für die Sozialbewegungen der 1960er Jahre geprägt worden war. Diese lose miteinander verbundenen Gruppierungen verfügen über eine Vielzahl von Finanz- und Informationsquellen, Waffen und unerlaubten Materialien. Da die Mitglieder dieser Netzwerke in bestimmten Gesellschaften unter Umständen als „Schläfer" leben, lässt sich nur schwer eine konkrete Struktur ermitteln. Dieses dezentralisierte Vorgehen erhöht die Ungewissheit im Hinblick auf künftige Terrorangriffe und macht Strategien und letztlich auch Technologien erforderlich, die diese Bedrohung anders angehen als in der Vergangenheit.

4. In dem vorangegangenen Bericht wurden mehrere Waffentechnologien analysiert, die bei Terroranschlägen verwendet werden könnten und eine Reihe von Empfehlungen ausgesprochen, um unsere Antwort auf den Terrorismus zu verbessern – nicht nur durch Abschreckung und Verhütung, sondern auch durch Verbesserung der öffentlichen Sicherheit. Im Lichte der internationalen Entwicklungen nach dem 11. September und der über das Al-Qaida-Netzwerk gewonnenen Erkenntnisse werden in diesem Bericht einige der in den letzten Monaten erörterten Bedrohungen untersucht, die in dem vorangegangenen Bericht gar nicht oder nur zum Teil angesprochen wurden. Außerdem werden einige der technischen Hilfsmittel und Innovationen beschrieben, die uns bei der Bekämpfung des Terrorismus helfen könnten.

5. In Kapitel II dieses Berichts wird versucht, eine Reihe von Bedrohungen, die sich aus der denkbaren terroristischen Nutzung chemischer, biologischer, radiologischer oder nuklearer Waffen (CBRN) ergeben könnten sowie Anschläge auf Kernenergieanlagen wie z.B. Kernkraftwerke zu bewerten. Darüber hinaus wird die bereits umfassende Behandlung des Cyberterrorismus im letztjährigen Bericht kurz aktualisiert. Kapitel III geht darauf ein, wie innovative Technologie politisch Verantwortlichen und Militärplanern beim Umgang mit komplexen terroristischen Bedrohungen helfen kann. Noch ist nicht bekannt, welches Ausmaß der Kampf gegen den Terrorismus haben, wie lange er dauern oder welche Folgewirkungen das neue Sicherheitsumfeld haben wird, doch ist sicher, dass die Technologie bei diesem neuen Kampf eine Rolle spielen wird. Abschließend geht

Kapitel IV auf den Gesamtrahmen der multilateralen Nichtverbreitungs- und Rüstungskontrollvereinbarungen ein und macht Vorschläge für eine verbesserte Behandlung der neuen terroristischen Bedrohung in internationalen Regelungen und Übereinkommen. Ihr Berichterstatter ist der festen Überzeugung, dass ein verbesserter Rahmen multilateraler Übereinkommen einen entscheidenden Beitrag zu der erfolgreichen Abwehr der Bedrohungen im aktuellen Sicherheitsumfeld darstellt.

Der vorliegende Bericht geht weder detailliert auf die nationalen Verteidigungsmaßnahmen und -strategien der NATO-Staaten (oder den „Heimatschutz“) gegen den Terrorismus noch auf die Zivilschutzaspekte der Terrorbekämpfung ein, da diese Themenfelder in den Berichten des Ausschusses für Verteidigung und Sicherheit und des Ausschusses für die zivile Dimension der Sicherheit behandelt werden.

II. BEDROHUNGSEINSCHÄTZUNG

A. NUKLEARSCHMUGGEL

6. Nach dem 11. September wurde ein Terroranschlag mit einer Kernwaffe oder einer „schmutzigen“ Bombe ernsthaft als denkbar betrachtet. Wie der Gesamtbericht des Ausschusses für 2001 [AU 220 STC (01) 7] deutlich machte, ist Russland wegen der immer noch unzureichenden Sicherheit seines gewaltigen Kernwaffenbestands die wahrscheinlichste Quelle, aus der Terroristen eine Kernwaffe oder Spaltmaterial beziehen könnten. Ungeachtet alarmistischer Analysen aus jüngster Zeit betrachten die meisten Studien (einschließlich eines im Januar 2001 von einer überparteilich zusammengesetzten Gruppe von Abgeordneten und Experten erstellten Berichts) den Diebstahl eines Kernsprengkopfs und sein Herausschaffen aus Russland als sehr unwahrscheinlich. Dem Jahresbericht 2002 des National Intelligence Council für den Kongress der Vereinigten Staaten zufolge ist eine solche Möglichkeit jedoch wegen des überalterten russischen Sprengkopf-Sicherungssystems nicht ganz auszuschließen, das „nicht unbedingt ausreicht, um dem heutigen Hauptproblem eines kenntnisreichen Insiders zu begegnen, der mit einer kriminellen oder terroristischen Gruppe zusammenarbeitet.“ Kleine taktische Kernwaffen, von denen in vielen Ländern noch Tausende vorhanden sind, geben wegen ihrer Diebstahlanfälligkeit Anlass zu besonderer Besorgnis.

7. Deutlich größer ist die Gefahr, dass waffenfähige Spaltstoffe (d.h. Plutonium und hoch angereichertes Uran [HAU]) Terroristen in die Hände fallen. Der Erwerb von Spaltmaterial ist das größte Hindernis für die Waffenherstellung, denn Kenntnisse über den Bau solcher Waffen sind recht weit verbreitet. Den Standards der Internationalen Atomenergie-Agentur (IAEA) zufolge reichen 8 kg Plutonium oder 25 kg HAU für die Herstellung eines Kernsprengsatzes aus.

8. Seit 1991 wurden von der IAEA 18 bestätigte proliferationsrelevante Fälle eines vollzogenen oder versuchten Diebstahls von Spaltmaterial aus Kernenergieanlagen in den Staaten der ehemaligen Sowjetunion (NIS) ermittelt. Nur in einem Fall wurde, amerikanischen Nachrichtendienstinformationen wie dem russischen Atomenergieministerium zufolge, für die Herstellung einer Bombe ausreichendes Material gestohlen und nicht wiedergefunden. Scott Parrish, einem erfahrenen Experten des Monterey Center for Nonproliferation Studies (CNS), zufolge „(gibt) es ... keine signifikanten Mengen an HAU oder Plutonium, die aus den NIS zu potenziellen Endabnehmern geschmuggelt wurden, ob es sich nun um Terrororganisationen oder Staaten handelt.“ Andere Experten warnen jedoch, der von diesen bekannten Fällen verkörperte „sichtbare“ nukleare Schwarzmarkt sei möglicherweise nur die Spitze des Eisbergs, und ein größerer „unsichtbarer“ Markt sei der Entdeckung entgangen.

9. Während Anfang der 1990er Jahre Beschlagnahmen vor allem in Europa erfolgten, lassen Vorkommnisse im Kaukasus in jüngster Zeit vermuten, dass Spaltstoffe jetzt nach Süden gehen könnten – zu potenziellen Käufern im Nahen Osten und in Zentralasien. Wie Ihr Unterausschuss schon 2001 in seinem Bericht angegeben hatte, haben sich islamistische Terrorgruppen wie Osama bin Ladens Al-Qaida wiederholt am Erwerb von Nuklearmaterial interessiert gezeigt. Von US-Vertretern vor kurzem in Afghanistan gefundene Unterlagen bestätigen, dass diese Terroristen sich in der einen oder anderen Form nukleare Fähigkeiten zulegen wollen.

10. Trotz dieser beunruhigenden Tendenzen haben Russland und andere NIS seit 1991 mit Hilfe der internationalen Gemeinschaft die Sicherheit der in mehr als 50 Anlagen gelagerten Spaltstoffe deutlich verbessert. Kooperative Sicherheitsvereinbarungen zwischen den Vereinigten Staaten und Russland haben besonders erfolgreich zu einer Verbesserung der Sicherheit der rund 600 Tonnen waffenfähigen Nuklearmaterials in den NIS beigetragen. Wie jedoch die Entschließung 313 deutlich macht, die von diesem Ausschuss eingebracht und im Oktober 2001 in Ottawa angenommen wurde, „(bleibt) viel ... zu tun, um in den Staaten der ehemaligen Sowjetunion Waffen und waffenfähiges Material zu schützen, zu sichern und zu beseitigen." Vor allem kommt es darauf an, die Spaltstoffe Russlands und anderer NIS an weniger und sichereren Standorten zu konzentrieren. Gleichzeitig muss diesen Staaten dabei geholfen werden, die bestehenden Programme auszubauen und die sozialen Bedingungen und die Zuverlässigkeit der Beschäftigten von Kernenergieanlagen zu verbessern.

11. Die Besorgnisse über waffenfähige Nuklearmaterialien beschränken sich nicht auf Russland und Osteuropa. Mindestens 180 000 kg abgetrenntes, ziviles und waffenfähiges Plutonium befinden sich in 11 anderen Ländern: Belgien, China, Deutschland, Frankreich, Indien, Italien, Japan, den Niederlanden, der Schweiz, dem Vereinigten Königreich und den Vereinigten Staaten. Außerdem enthalten nach Schätzungen der IAEA 170 in Betrieb befindliche Forschungsreaktoren in 43 Ländern über 2 772 kg HAU. Ein Teil davon ist noch nicht bestrahlt, was Terroristen den Umgang damit zusätzlich erleichtern würde. Experten der IAEA und des Center for International Security and Cooperation (CISAC) der Stanford University haben wiederholt darauf hingewiesen, dass die Sicherheit in vielen westeuropäischen und US-amerikanischen Forschungsreaktoren unzulänglich ist und verbessert werden muss.

12. Bei Initiativen führender Mitglieder des US-Kongresses ergaben sich vor kurzem nach Unterlagen des Energieministeriums und einer Studie der Beobachtungsgruppe Project on Government Oversight bei 10 großen Kernwaffenkomplexen der Vereinigten Staaten Sicherheitsprobleme. Bundesbedienstete, die bei Scheinübungen als „Kommandotruppen" auftraten, konnten in mehr als der Hälfte der Fälle die Sicherheitsschranken der Kernwaffenlaboratorien durchbrechen. Das Personal der Anlagen war sogar vor den bevorstehenden Scheinangriffen gewarnt worden und konnte sie trotzdem nicht zurückschlagen. Bei einem weiteren Test in einer wichtigen militärischen Kernwaffen-Produktionsanlage konnten Kommandotruppen der US-Marine genug Material für den Bau mehrerer Kernwaffen „stehlen".

B. ANGRIFFE MIT „SCHMUTZIGEN" BOMBEN

13. Trotz der weit verbreiteten Kenntnisse über die Physik eines einfachen Kernsprengkopfs und der relativen Verfügbarkeit von waffenfähigem Material ist es für eine Terroristengruppe technisch immer noch schwierig, eine Kernwaffe zu bauen. Selbst wenn man annimmt, dass sich jemand aus einer solchen Gruppe die Grundlagen der Kerntechnik angeeignet hat, wären eine Zeitlang (einigen Experten zufolge mindestens zwei Jahre lang) ein Testgelände und Laboratorien erforderlich, was den Schutz durch einen Staat voraussetzen würde. Da nur wenige Terroristengruppen diese Voraussetzungen erfüllen dürften, könnten andere auf einfachere Lösungen verfallen und

zum Beispiel radioaktive Materialien in Verbindung mit konventionellen Sprengstoffen verwenden, um eine so genannte radiologische (oder „schmutzige“) Bombe herzustellen.

14. Dr. Henry Kelly, der Präsident der Federation of American Scientists, erläuterte in einer Aussage vor dem Außenpolitischen Ausschuss des US-Senats, Angriffe mit „schmutzigen“ Bomben könnten zu Todesfällen führen, aber „nicht in einer Größenordnung von Hunderttausenden von Opfern wie bei einer einfachen Atombombe. Die Angriffe könnten große Teile eines Stadtgebiets mit Strahlungen kontaminieren, die über den Leitlinien der (US-Umweltbehörde) EPA für Gesundheitsgrenzwerte und toxische Stoffe liegen würden.“ Eine „schmutzige“ Bombe könnte schwer wiegende gesundheitliche, wirtschaftliche und psychische Wirkungen nach sich ziehen. Sie könnte Dutzende städtischer Wohnblöcke kontaminieren, die umgehende Evakuierung nötig machen und große Wohngemeinden in Angst und Schrecken versetzen, auch wenn es nur wenige Strahlentote geben sollte.

15. Das Nuklearmaterial, das zur Herstellung einer „schmutzigen“ Bombe verwendet werden kann, braucht nicht waffenfähig zu sein. Für die Strahlentherapie, Röntgenaufnahmen, in industriellen Bestrahlungsgeräten und Wärmekraftaggregaten verwendete radioaktive Materialien sowie Nuklearabfälle reichen für die Herstellung eines solchen Sprengsatzes aus. Die Beschaffung solcher Stoffe, darunter Kobalt-6, Strontium-90, Cäsium-137 und Iridium 192, ist nicht schwierig. Nach Aussage von Abel Gonzalez, des IAEA-Direktors für Strahlen- und Abfallsicherheit, werden bei Ausrüstungen für die Strahlentherapie normalerweise nur wenige Vorsichtsmaßnahmen ergriffen, und eine große Strahlenquelle könnte recht leicht entwendet werden, insbesondere wenn die Täter auf ihre eigene Gesundheit keine Rücksicht nehmen. Wie Professor Michael Clarke, der Direktor des Centre for Defence Studies am Londoner King's College diesem Unterausschuss gegenüber im März erklärte, wurden „schmutzige“ Bomben früher im Allgemeinen wegen der mit ihrer Herstellung und ihrem Transport verbundenen hohen persönlichen Risiken als unwahrscheinliche Bedrohung angesehen, während wir heute eine andere Bewertung vornähmen, da wir Terroristen gegenüberstünden, die bereit seien, bei einem Angriff ihr Leben zu opfern.

16. Außerdem gibt es Belege dafür, dass Al-Qaida-Mitglieder versucht haben könnten, in Afghanistan eine schmutzige Bombe zu entwickeln. Einer Meldung von Associated Press zufolge legte eine amerikanische Rakete, die einen Taliban-Komplex traf und aufriss, mehrere Räume frei, die mit Papieren und Formeln gefüllt waren, von denen einige beschrieben, wie eine Explosion von TNT mit Plutonium kombiniert werden kann. Ob die in Afghanistan gefundenen Dokumente zutreffend waren und zu dem angestrebten Ziel geführt hätten, müsste wahrscheinlich wissenschaftlich untersucht werden, doch ein Szenario mit einer „schmutzigen“ Bombe in den Händen von Terroristen ist auf jeden Fall sehr ernst zu nehmen.

In einem IAEA-Bericht vom Mai 2002 über das Schmuggelproblem wurden für den Zeitraum 1993 bis 2001 über 200 Fälle genannt, in denen zu medizinischen und industriellen Zwecken verwendete radioaktive Materialien beschlagnahmt worden waren. Die Türkei, ein NATO-Mitglied, das an verbreitungsrelevante Staaten wie den Irak, Syrien und den Iran grenzt und in der Nähe potenzieller Schmuggelrouten in den Kaukasus und nach Osteuropa liegt, wies kürzlich auf eine Zunahme des Schmuggels von radioaktivem Material über seine Grenzen hin. Türkischen Polizeikräften zufolge ist es zumeist in großen Industriehäfen, jedoch auch an den Landgrenzen zum Irak und zu Bulgarien zur Beschlagnahme von Materialien aus Russland und Kasachstan gekommen. Die türkischen Bemühungen zur Bekämpfung des Schmuggels und zur Erhöhung der Sicherheit an den Grenzen sind in letzter Zeit verstärkt worden.

17. Auch aufgegebene Materialien könnten als Quelle für schmutzige Bomben dienen. Im Februar 2002 fanden Nuklearexperten in Georgien in den Bergen nahe der abtrünnigen Provinz Abchasien Kanister mit tödlichem radioaktivem Material. Die Kanister enthielten Strontium-90, ein Abfallprodukt von Kernreaktionen, und dienten als Energiequelle für einen sowjetischen Funk-

sender. In vielen Teilen der ehemaligen Sowjetunion gibt es noch Hunderte ähnlicher Kanister zur Stromversorgung bei Bauvorhaben in entlegenen Gegenden.

18. In Brasilien macht ein Unfall mit Nuklearmaterial die möglichen Auswirklungen einer „schmutzigen" Bombe deutlich. 1987 fanden Plünderer in der Stadt Goiania, als sie eine aufgegebene Krebsklinik durchsuchten, Cäsium-137, das sie später an Freunde weitergaben, wobei 249 Menschen der Strahlung ausgesetzt wurden und vier daran starben. Diese Privatklinik war aufgegeben worden, nachdem sie geschlossen worden war und das radioaktive Material war einfach zurückgelassen worden. Die Gesundheitsbehörden untersuchten mehrere Monate lang über 100 000 Einwohner, rissen 85 Häuser ab und mussten kontaminierte Kleidung, persönliche Habseligkeiten und Mobiliar wegschaffen – insgesamt über 3 500 Kubikmeter Abfall.

19. Das Problem reicht bis in die Vereinigten Staaten. Befürchtungen vor einem Szenario wie in Goiania kamen im März 1998 auf, als 19 Ampullen mit Cäsium-137 aus einem Krankenhaus in Greensboro, North Carolina, verschwanden und nie wieder auftauchten. In jüngerer Zeit wurde außerdem in einem Bericht des Generalinspekteurs des US-Energieministeriums (DOE) eingeräumt, dass „beträchtliche Mengen" an Nuklearmaterial, die sich in zwei zur Verwendung berechtigten Einrichtungen befanden, nicht mehr vorhanden sind. Allein in den US gibt es an Universitäten, in Krankenhäusern und in gewerblichen Einrichtungen rund 2 Millionen Geräte, die radioaktive Materialien verwenden.

C. ANGRIFFE AUF KERNENERGIEANLAGEN

20. Nach dem 11. September wurden Kernenergieanlagen als wahrscheinliche Ziele terroristischer Anschläge genannt. Neuere Analysen großer Kernkraftwerke deuten darauf hin, dass die Sicherheitsvorkehrungen womöglich nicht ausreichen, um entschlossene Terroristen abzuwehren.

21. In mehreren Medienberichten wurde der Schwerpunkt auf die Verwundbarkeit der Reaktorhülle für Angriffe aus der Luft gelegt. Hierzu vertreten die verschiedenen Experten unterschiedliche Ansichten. IAEA-Sprecher David Kyd erklärte am 19. September, die meisten in den 60er und 70er Jahren des 20. Jahrhunderts gebauten Kernkraftwerke seien nur für versehentliche Aufschläge der damals eingesetzten kleineren Flugzeuge ausgelegt. „Wenn man das Risiko eines vollgetankten Jumbo-Jets annimmt, so ist klar, dass sie von ihrer Konzeption her nicht für einen solchen Aufprall ausgelegt wurden." Der Nuclear Regulatory Commission (NRC) zufolge, der US-amerikanischen Bundesbehörde für die Überwachung der in Betrieb befindlichen Kernkraftwerke des Landes, sind die Kernenergieanlagen in den USA dafür ausgelegt, Erdbeben und anderen Naturkatastrophen zu widerstehen, doch die Bedrohung durch ein Großraumflugzeug war bei der ursprünglichen Konstruktion und den damaligen Sicherheitsbetrachtungen nicht berücksichtigt worden. John B. Ritch, früher US-Botschafter bei der IAEA und jetzt Generaldirektor der World Nuclear Association (WNA), einer die internationale Kernenergiewirtschaft vertretenden Organisation, erklärte gegenüber Mitgliedern dieses Ausschusses, „westliche Kernkraftwerke (seien) so gebaut, dass sie den meisten Terroranschlägen (widerstünden). Fast alle Reaktorkonstruktionen", so Ritch, „würden selbst bei einem unwahrscheinlichen Worst-Case-Szenario ein Freiwerden von Radioaktivität verhindern."

22. In einem Artikel aus einer neueren Ausgabe des WNA-Newsletter wurde jedoch eingeräumt, dass „andere mit dem nuklearen Brennstoffzyklus zusammenhängende Anlagen möglicherweise verwundbarer sind." Experten weisen darauf hin, dass Abklingbecken für verbrauchte Brennstäbe, die mit die höchsten Radioaktivitätskonzentrationen aufweisen, sich bisweilen in Gebäuden befinden, die Risse und Korrosionsschäden aufweisen können. Der Grund liegt darin, dass nicht alle Abklingbecken Stahlbetonwände und Auskleidungen aus Edelstahl besitzen. Die größte Gefahr besteht in einem Verlust des Beckenwassers, das den hoch radioaktiven abgearbeiteten

Brennstoff abkühlt und abschirmt, was zu einer Brandkatastrophe mit möglicherweise schlimmeren Folgen als eine Reaktorkernschmelze führen könnte. Neuere US-amerikanische, russische, französische und britische Studien stimmen darin überein, dass ein Angriff auf ein Abklingbecken – ob nun mit einem Flugzeug oder herkömmlichem Sprengstoff – zu einem Kühlwasserverlust und zum Freisetzen von Radioaktivität führen könnte. Eine Studie des Brookhaven National Laboratory zeigte, dass der Brand eines Abklingbeckens eine Fläche von über 470 Quadratkilometern verseuchen und annähernd 30 000 Krebstote sowie Schäden in Höhe von 59 Milliarden US-Dollar verursachen könnte.

23. Eine noch größere Bedrohung ziviler Kernenergieanlagen kann ein Angriff am Boden oder ein Sabotageakt bedeuten – ob nun mit oder ohne Unterstützung durch Insider. Experten des CISAC der Stanford University wiesen darauf hin, dass angesichts der Zunahme der Attentate mit Autobomben im letzten Jahrzehnt Terroranschläge mit konventionellem Sprengstoff auf Kernkraftwerke, Abklingbecken oder Atommülltransporte Anlass zu großer Sorge geben. Vielen unabhängigen Quellen zufolge sind die Sicherheitsbestimmungen für sämtliche Kernkraftwerke in den USA schon seit langem unzureichend. Bis vor kurzem brauchten sich die Betreiber nach den NRC-Vorschriften nur vor einem angreifenden Insider und/oder drei externen Angreifern zu schützen. Es sind nur mindestens 5 Wachleute vorgeschrieben, doch Quellen aus der Kernenergiewirtschaft zufolge sind in den Kernenergieanlagen der USA rund 5 000 Wachleute beschäftigt – im Durchschnitt 80 je Anlage. Gegenwärtig kann der Sicherheitsdienst von privaten Sicherheitsunternehmen gestellt werden, die nach Ansicht einiger Kongressabgeordneter laxe Einstellungsverfahren anwenden. Außerdem wurden erst nach dem Bombenanschlag von 1993 auf das World Trade Center Schutzmaßnahmen gegen Autobomben ergriffen.

24. Als die Vereinigten Staaten die Verwundbarkeit von Kernenergieanlagen erkannten, erließen sie neue Vorschriften. Im November 2001 wurde im US-Senat ein Gesetzentwurf eingebracht, durch den die Sicherheitsdienste im Nuklearbereich der Bundesebene unterstellt und Aktionspläne zur Vorbereitung auf eventuelle künftige Angriffe erarbeitet wurden. Im Februar wies die US-Regierung die Kernkraftwerke des Landes an, ihre Mitarbeiter strenger zu überprüfen. Die Zugangsrechte der Mitarbeiter innerhalb der Anlagen sind jetzt eingeschränkt, und Autos, die sich den Anlagen nähern, müssen nun in größerer Entfernung von den Eingängen anhalten. Die Küstenwache hat im Umkreis von Kernenergieanlagen Sperrgebiete eingerichtet, und die US-Luftfahrtbehörde (Federal Aviation Administration) hat in einer 12-Meilen-Zone um die meisten Anlagen herum Flüge verboten.

25. Andere Staaten haben ebenfalls Maßnahmen zum Schutz ihrer Kernkraftwerke ergriffen. Nach dem 11. September brachte die französische Regierung in der Nähe ihrer Nukleareinrichtungen von La Hague Boden-Luft-Raketen und Radargeräte in Stellung. Außerdem stehen innerhalb von 2 Minuten startklare Kampfflugzeuge bereit, um mögliche Angriffe aus der Luft auf Kernenergieanlagen abzufangen. Die kanadische Regierung erwog ähnliche Schritte. Das Britische Atomforum (BNIF) erklärt, die Betreiber hätten die Sicherheitssysteme überprüft und ergriffen zurzeit mit den Behörden abgestimmte Maßnahmen, um sicherzustellen, dass die getroffenen Vorkehrungen „belastbar“ sind. Die deutsche Bundesregierung gab einen Bericht über Reaktorsicherheit in Auftrag und unterstrich die Bedeutung einer Neubewertung der Sicherheitsvorkehrungen.

D. BIOTERRORISMUS

26. Ihr Unterausschuss hat sich schon früher vielfach mit der Bedrohung durch den Bioterrorismus auseinandergesetzt. In dem letztjährigen Bericht wurde darauf hingewiesen, dass einige der größten moralischen Hemmschwellen im Hinblick auf den Einsatz von Biowaffen angesichts der zunehmenden Ausbreitung des fanatischen religiösen Terrorismus und von Weltuntergangssekten

sinken. Auch wenn die Milzbrandanschläge im letzten Herbst in den Vereinigten Staaten (mit 5 Toten und 17 Erkrankten) relativ geringfügig waren, können sie wohl als Signal dafür dienen, dass für uns eine neue, gefährliche Ära des Bioterrorismus begonnen hat.

27. Vor allem aus drei entscheidenden Gründen steht die internationale Gemeinschaft im Hinblick auf den Bioterrorismus an „einer Wasserscheide“, wie Michael Moodie, der Präsident des Washingtoner Chemical and Biological Arms Control Institute (CBACI), es nannte. Der erste Grund ist einfach zu erkennen: Die Milzbrandanschläge letztes Jahr in den Vereinigten Staaten (und die breite Medienberichterstattung darüber) können Nachahmer finden. Der zweite Grund hängt mit dem veränderten Wesen des Terrorismus zusammen. In dem Maße, wie an die Stelle der herkömmlichen politischen Beweggründe religiöser Fanatismus, Weltuntergangsvorstellungen oder bloße Rachsucht (wegen tatsächlich oder nur in der Einbildung erlittenen Unrechts) getreten sind, haben die Terroristen alle moralische Hemmungen aufgegeben und versuchen, ihren Feinden gewaltige Verluste zuzufügen.

28. Der dritte Grund ist technologischer Art: Angesichts der Fortschritte in der Biologie und der Biotechnologie fällt es Terroristen heute vermutlich leichter, die bestehenden Hürden für den Erwerb biologischer Waffen zu überwinden. Die Weltgesundheitsorganisation (WHO) nennt 50 Bakterien (wie Milzbrand), Viren (wie Pocken) und Toxine (wie Ricin, ein aus Rizinussamen gewonnener Stoff), die wohl am ehesten für die biologische Kriegführung verwendet werden dürften. Auf der Biowaffenliste der NATO stehen 30 verschiedene Bakterien, Viren und Pilze. Die Erreger lassen sich unter Umständen recht leicht beschaffen, doch ist es, wie Dr. Moodie es formulierte, „nicht das Gleiche, ob man einen Erreger besitzt oder über eine Waffe verfügt. Er muss in waffenfähiger Form vorliegen, und es ist ein wirksamer Träger zu entwickeln.“ Wie Michael Mates in dem letztjährigen Bericht erläuterte, werden wissenschaftliche Fortschritte uns noch besser in die Lage versetzen, an der Funktionsweise lebender Systeme gezielt genau berechnete Änderungen vorzunehmen. Damit erhält die Menschheit ein gewaltiges, neues Potenzial für segensreiche medizinische Entwicklungen, aber auch für den Missbrauch in Form von Waffensystemen.

Von einer Dienststelle des Pentagons finanzierte Wissenschaftler an der State University of New York erzeugten vor kurzem erstmals ein „künstliches“ Polio-Virus. Dazu verwendeten sie öffentlich zugängliche genetische Informationen und beschafften sich Teile der Erbgutsequenz bei Firmen, die DNA-Bestandteile jeder Art auf Bestellung produzieren. Die gleiche Technik könnte auch zur Erzeugung anderer Viren und zur deutlichen Erhöhung der Virulenz existierender Krankheitserreger verwendet werden. Es genügt, die genetische Sequenz zu kennen und über ausreichenden wissenschaftlichen Sachverstand zu verfügen. Diese Fortschritte der Wissenschaft, warnt Jakob Kellenberger, der Präsident des Internationalen Komitees vom Roten Kreuz, „werden die Entwicklung und den Einsatz von Biowaffen erleichtern und die vorsätzliche Verbreitung von Krankheiten und Veränderung der chemischen Abläufe im Körper einfacher, tödlicher, billiger und schwerer nachweisbar machen“. In der von diesem neuen Experiment entfachten Diskussion vertraten viele die Ansicht, der Zugang zu der genetischen Sequenz tödlicher Krankheiten müsse Einschränkungen unterworfen werden.

29. Wir sollten auf jeden Fall, wie der Mates-Bericht hervorhebt, auch dafür gerüstet sein, diesen künftigen Bedrohungen wirksam zu begegnen. Vor allem aber müssen wir zuerst einmal das Wesen der aktuellen Bedrohung durch den Bioterrorismus verstehen. Die Experten scheinen sich darüber einig zu sein, dass die einfachsten Formen des Bioterrorismus – wie z.B. eine Lebensmittelvergiftung – nur geringen technischen Sachverstand erfordern und von einer recht großen Zahl von Terrorgruppen ausgeführt werden könnten. 1984 verseuchte die Rajneeshee-Sekte, um das Kommunalwahlergebnis in einer Kleinstadt in Oregon zu beeinflussen, das Salatbuffet in einem Restaurant mit Salmonellen, worauf 45 Menschen ins Krankenhaus kamen. Die Bakterien waren bei einer Firma für Medizinbedarf in Seattle im Bundesstaat Washington gekauft worden.

30. Sollen bioterroristische Anschläge massenhaft Opfer fordern, müssen beim Umgang mit tödlicheren Erregern weitaus höhere technische Anforderungen erfüllt werden. Jonathan Tucker, einem Experten des Büros des Monterey CNS in der Bundeshauptstadt Washington, zufolge müssen Terroristen, die ein verheerendes Blutbad anrichten wollen, über technischen Sachverstand, organisatorische Disziplin und die Motivation verfügen, wahllos unzählige Menschen zu töten. Die Terroristen des 11. Septembers erfüllten sicherlich die beiden letztgenannten Kriterien, besassen sie aber auch genügend technischen Sachverstand? Es liegen Beweise vor, wonach Al-Qaida Massenvernichtungswaffen erwerben wollte und Osama bin Laden soll eine solche Beschaffung als religiöse Pflicht betrachtet haben. Die Vereinigten Staaten entdeckten in der Nähe des afghanischen Kandahar ein im Bau befindliches Labor, in dem angeblich Milzbranderreger gezüchtet werden sollten. Es ist jedoch nicht belegt, dass es Al-Qaida jemals gelungen ist, biologische Kampfstoffe herzustellen.

31. Das überrascht nicht, denn schon die Erfahrungen der japanischen Sekte Aum Shinrikyo machten deutlich, dass selbst über viel Geld verfügende Gruppen mit Zugang zu wissenschaftlichem Sachverstand mit dem Versuch kläglich scheitern können, biologische Waffen einzusetzen. Madeline Drexler, die Verfasserin von *Secret Agents: The Menace of Emerging Infections*, erklärte dazu vor kurzem in einem Artikel: „Biologische Kampfstoffe breiten sich am leichtesten in Form trockener Partikel von 1-5 Mikrometer Durchmesser aus. In dieser Form wirken sie wie Gase, sinken in der Luft langsam nach unten und dringen tief in die Lungen und damit in die Blutbahn ein. Das Kunststück ist die Entwicklung von Formulierungen, die zu verhindern vermögen, dass diese Lebewesen nicht absterben, austrocknen, zerfallen, sich verklumpen oder ihre Virulenz verlieren, wenn sie an die Luft gelangen."

32. Für Terroristen wäre es leichter, sich biologische Agenzien wie auch die für ihren Einsatz als Kampfstoffe erforderlichen Kenntnisse bei den Überresten des „Biowaffen-Archipels" der ehemaligen Sowjetunion zu beschaffen. Kurz nach der Unterzeichnung des Biowaffenübereinkommens von 1972 begann Moskau insgeheim mit dem größten Programm für biologische Kriegführung der Geschichte. Kanatjan Alibekov (auch als Kenneth Alibek bekannt), der ehemalige stellvertretende Leiter des Biopreparat genannten Programms, behauptete 1992, nachdem er sich in die Vereinigten Staaten abgesetzt hatte, Ende der 1980er Jahre hätten 65 000 Forscher und Techniker dafür gearbeitet. Die über das ganze Gebiet der riesigen Sowjetunion verstreuten Anlagen von Biopreparat produzierten große Mengen von Erregern nicht infektiöser Krankheiten wie Milzbrand und Tularämie, aber auch hoch ansteckender Seuchen wie Pocken- und Pesterreger. Einige dieser Agenzien konnten als Kampfstoffe verwendet werden.

33. Nach dem Zerfall der Sowjetunion verpflichtete sich Russland, dieses gefährliche Erbe zu vernichten oder für zivile Zwecke umzuwidmen. Es hat außerdem mehrere alte Biopreparat-Forschungs- und Entwicklungszentren für die internationale wissenschaftliche Zusammenarbeit geöffnet. Einige Forschungs- und Produktionsanlagen in Jekaterinburg, Sergijew Possad und Kirow sind jedoch immer noch für Ausländer geschlossen. Obwohl alle diese Anlagen westlichen Experten zufolge relativ gut gesichert sind, ist die Lage durchaus beunruhigend. Darüber hinaus geht die Bedrohung, wie Alibek kürzlich betonte, nicht von der russischen Regierung, sondern von früheren Beschäftigten mit Biowaffenerfahrung aus. Einigen Quellen zufolge sind bereits sowjetische Bioingenieure aus ihrer postsowjetischen Arbeitslosigkeit in Staaten wie den Iran, den Irak und China gelockt worden. Die Lage wäre jedoch noch schwerwiegender ohne die großen Investitionen in Programme wie das International Science and Technology Center (ISTC), eine intergouvernementale Organisation, die 1992 von der Europäischen Union, Japan, Russland und den Vereinigten Staaten gegründet wurde, um sowjetische Waffenentwickler und -experten in nichtmilitärischen Forschungsprojekten unterzubringen.

34. Wissenschaftler sind vor allem wegen eines möglichen Diebstahls von Pockenviren besorgt. Die einzigen offiziellen Verwahrungsorte für dieses 1997 ausgerottete Virus sind zwei Einrichtungen in den Vereinigten Staaten und Russland. Dem *Scientific American* zufolge könnten jedoch auch andere Einrichtungen in Russland darüber verfügen. Wenn ein Zugriff auf die vorhandenen Bestände möglich sein sollte und diese als Biowaffe genutzt werden sollten, könnte sich die Krankheit schnell ausbreiten, da die Bevölkerung seit der Ausrottung der Krankheit nicht mehr routinemäßig dagegen geimpft worden ist.

E. CHEMIEWAFFENTERRORISMUS

35. Chemiewaffen machen sich die toxischen Eigenschaften chemischer Stoffe, nicht ihre Sprengkraft zunutze, um physische oder physiologische Wirkungen auf Menschen auszuüben. Wie bei biologischen Agenzien wurde für eine Vielzahl von chemischen Stoffen eine Verwendung durch Terroristen als denkbar ermittelt. Dazu gehören zum Beispiel Insektizide wie Nicotinsulfat, Herbizide wie Dioxin und Benzidin, „Atemgifte mit blutschädigender Wirkung“ wie Cyanwasserstoff und Cyanogenchlorid, „Erstickung herbeiführende Substanzen“ wie Chlor, „Vesikantien“ wie Senfgas und Stickstoff-Lost sowie „Nervengase“ wie Sarin, VX und Soman.

36. Die Toxizität von Chemikalien liegt im Allgemeinen zwischen der der tödlicheren Biowaffen und der konventioneller Waffen. Wie die Biowaffen unterscheiden sich auch die Chemiewaffen sehr in ihrer Tödlichkeit. Die meisten Experten sind sich einig, dass Chemiewaffen billiger, leichter herzustellen und wahrscheinlich auch einfacher ins Ziel zu bringen sind als Biowaffen, auch wenn ein Angriff auf eine ausgewählte Zielbevölkerung im Freien äußerst stark von den Umgebungsbedingungen, der Art des Kampfstoffs und der verwendeten Angriffsform abhängt.

37. Trotz der in jüngster Zeit gestiegenen Beachtung für Biowaffen sollten wir die Möglichkeit eines Chemiewaffenangriffs durch Terroristen nicht unterschätzen. Schließlich wurde einer der erfolgreichsten Terrorangriffe der letzten Jahre – der Anschlag der Aum Shinrikyo-Sekte in der Tokioter U-Bahn, bei dem 12 Menschen getötet und über 5500 verletzt wurden – mit einer Chemiewaffe, dem Giftgas Sarin, durchgeführt. Wie oben angegeben hatte die Sekte erfolglos mit Biowaffen experimentiert, war aber in der Lage, mehrere Formen von Chemiewaffen zu synthetisieren. Nichtsdestoweniger war der Anschlag von Aum Shinrikyo ein „politischer“ Erfolg, aber ein technischer Fehlschlag: Es wären viel mehr Menschen getötet worden, wenn das Giftgas-Verteilungssystem richtig funktioniert hätte.

Im August 2002 erbrachten in Afghanistan entdeckte Videobänder den Beweis, dass Al-Qaida chemische Kampfstoffe entwickelte und testete. Insbesondere ein anscheinend vor dem 11. September aufgenommenes Band zeigt den qualvollen Tod dreier Hunde, die einer Chemikalie ausgesetzt worden waren. Experten zufolge könnte es sich bei dem Kampfstoff entweder um Sarin oder um Cyanidgas gehandelt haben.

38. Wissenschaftler haben in jüngster Zeit darauf hingewiesen, dass es in vielen Ländern bemerkenswert einfach (und preiswert) ist, sich ganz legal alle für die Waffenproduktion benötigten Chemikalien zu beschaffen. So gelang es James M. Tour, Chemieprofessor an der Rice University (Vereinigte Staaten), sich im Postversand alle Ingredienzien für die Sarinherstellung zu besorgen. „Tausende von Menschen“, schrieb er später, „sind talentiert genug, um den detaillierten Syntheseprotokollen zu folgen, die seit Jahrzehnten in der Primärliteratur verfügbar sind und auf die jetzt problemlos über das Internet zugegriffen werden kann.“ Trotz des internationalen Verbots der Entwicklung, der Herstellung und des Erwerbs chemischer Waffen, wie es im Chemiewaffenübereinkommen (CWÜ) verankert ist, gibt es in vielen Ländern (insbesondere in den Vereinigten Staaten) keine Bestimmungen zur Regulierung des Erwerbs kleiner (für Terroristen aber ausreichender) Mengen zahlreicher Grundstoffe für Chemiewaffen.

F. CYBERTERRORISMUS

39. Im Internet zeigten sich nach dem 11. September zwei scheinbar widersprüchliche Tendenzen. Zum einen waren die Administratoren von Computersystemen in höchster Alarmstimmung, während die Aktivitäten der Hacker in den Vereinigten Staaten zurückgingen. Möglicherweise erklärt sich diese Abnahme damit, dass niemand mit den Terroranschlägen in Verbindung gebracht werden wollte. Zum anderen waren einzelne Hacker und Hackergruppen aus den USA und einigen muslimischen Staaten an einer wahren Flut von Cyberattacken beteiligt. Amerikanische Hacker attackierten und veränderten Hunderte muslimischer Websites und starteten Denial-of-Service-Angriffe, um „offizielle Ziele“, wie z.B. iranische Ministerien, arabische Banken mit Verbindungen zu Al-Qaida oder palästinensische Internet Service Provider (ISP) lahm zu legen. Muslimische Hacker veränderten westliche Websites und drohten mit Schlägen gegen wichtige US-amerikanische und britische militärische Websites, wobei sie eine „Al-Qaida-Online-Allianz“ ausriefen.

40. Diese beiden Tendenzen spiegeln auf verschiedene Weise die zunehmende politische Nutzung des Internets wieder. Einige Experten theoretisierten sogar über die Nutzung des Internets als „digitales Schlachtfeld“. Dorothy E. Denning, Professor für Informatik an der Georgetown University (USA), schrieb vor kurzem: „Es ist überhaupt nicht ungewöhnlich, dass ein regionaler Konflikt eine Cyberdimension aufweist, in der selbsternannte Hacker nach eigenen Regeln ihre Kämpfe austragen.“ Die Zunahme computergestützter politischer Angriffe wurde schon im letztjährigen Bericht hervorgehoben. Die Experten sind sich allerdings nicht darüber einig, ob diese Aktivitäten als Cyberterrorismus bezeichnet werden können oder nicht.

41. Obwohl viele einräumen, dass Terroristengruppen regelmäßig traditionelle Formen subversiver Tätigkeiten mit Computerhilfe unterstützen und fördern, wird unter Cyberterrorismus im Allgemeinen ein computergestützter Angriff verstanden, durch den Staaten oder Gesellschaften zur Verfolgung politischer, religiöser oder anderer ideologischer Ziele eingeschüchtert oder unter Druck gesetzt werden sollen. Bei diesen Angriffen sollten in der Regel konkrete Schäden verursacht werden: größere Störungen öffentlicher Einrichtungen, Unfälle mit Todesfolge und/oder Verletzungen oder schwere wirtschaftliche Verluste. Damit Angriffe unter die Definition des Cyberterrorismus fallen können, sollten sie Computer und/oder IT-Systeme als Ziel und/oder Waffe einbeziehen.

42. Mehrere Studien haben deutlich gemacht, wie verwundbar viele Teile der entscheidenden Infrastruktur unserer Gesellschaften für Cyberattacken sind. Darüber hinaus macht es die steigende Komplexität unserer hoch vernetzten Gesellschaften, worauf Professor Homer Dixon hinwies, effektiv unmöglich, alle Schwächen zu beseitigen. Trotz der Einführung neuer Technologien und der Verbesserung der Cyberabwehr sind unsere Systeme so konfiguriert oder werden so verwendet, dass sie Angriffen eine offene Flanke bieten. Wenn wir diese grundlegende Verwundbarkeit akzeptieren, stellt sich die entscheidende Frage, ob es Terroristen gibt, die geschickt und motiviert genug sind, um extrem folgenschwere Operationen durchzuführen.

43. In dem letztjährigen Bericht fasste Herr Mates die Ergebnisse einer Studie von 1999 des Center for the Study of Terrorism and Irregular Warfare der Naval Postgraduate School (NPS) im kalifornischen Monterey zusammen. Ein extrem schädlicher Cyberterrorismus sei nach der wichtigsten Schlussfolgerung der Autoren noch Zukunftsmusik, doch könnten bestimmte (religiöse oder chiliastische) Gruppierungen Cyberanschläge im Rahmen ihrer Strategie einsetzen. Im Oktober 2000 veröffentlichte das NPS Center einen zweiten Bericht im Anschluss an eine Tagung über Entscheidungsprozesse in bewaffneten Widerstand leistenden substaatlichen Gruppen. An der Konferenz nahmen auch Hacker und frühere Aktivisten gewalttätiger substaatlicher Gruppen teil.

Der Bericht bestätigte weitgehend die Schlussfolgerungen der früheren Studie und machte deutlich, dass 1. Terroristen Cyberattacken noch nicht in ihre Taktik eingeschlossen haben, 2. substaatliche Gruppen Cyberattacken als „nichttödliche Waffe" verwenden können und 3. eine deutliche Distanz zwischen Hackern und Terroristen ihrem Zusammenschluss zu einiger einzigen Gruppe entgegenstanden.

Neue Erkenntnisse widersprechen diesen Schlussfolgerungen jedoch möglicherweise. In vor kurzem aufgefundenen Al-Qaida-Computern waren Informationen über öffentliche wie private Computersysteme zur Steuerung von Infrastruktureinrichtungen in den USA gespeichert. Insbesondere untersuchten – der *Washington Post* zufolge – unbekannte „Browser" aus dem Nahen Osten und Asien die digitalen Notfallsysteme für das Telefonnetz, die Stromerzeugung und -weiterleitung, die Wasserspeicherung und -verteilung, für Kernkraftwerke und Gasversorgungseinrichtungen. Nach Warnungen des FBI besteht die Gefahr dabei in einem physischen Angriff von Terroristen mit konventionellen Waffen in Verbindung mit einer Cyberattacke auf lebenswichtige Infrastruktureinrichtungen. Die verschiedenen Sicherheitsbehörden und Nachrichtendienste der USA, räumt die *Post* ein, „sind sich über das Ausmaß und den Zeithorizont dieser Bedrohung nicht einig". Einige Verantwortliche erklärten, die Fähigkeit von Al-Qaida zur Durchführung solcher Angriffe werde überschätzt und sie machten sich über denkbare physische Terroranschläge weitaus größere Sorgen.

44. Nichtsdestoweniger könnte es gefährlich sein, Cyberterrorismus als reine Zukunftsmusik zu betrachten. Wie Professor Denning schrieb, kommt es darauf an, „über die herkömmlichen Terrorgruppen hinauszublicken und an die Computerfreaks zu denken, die bereits über beachtliche Fertigkeiten als Hacker verfügen." Wie die Ereignisse nach dem 11. September gezeigt haben, könnten sich einige Hacker ernsthaft mit Terroristen zusammentun und den Cyberterrorismus zur Realität werden lassen. Diese Gefahr könnte mit der nächsten Generation von Terroristen, die in einer digitalen Welt groß geworden sind, weiter zunehmen.

III. TECHNOLOGIE GEGEN DEN TERRORISMUS

45. Verschiedene bisweilen kreativ eingesetzte Technologien könnten sehr hilfreich sein, um den in dem vorigen Kapitel genannten Bedrohungen vorzubeugen und sie zurückzuschlagen. Wie schon in der Einführung unterstrichen wurde, haben die Anschläge vom 11. September die Aufmerksamkeit auf die Verwundbarkeit der großen, komplexen Systeme gelenkt, von denen unsere Existenz abhängt. Natürlich kann Spitzentechnologie allein uns keine völlige Sicherheit bringen, und in vielen Bereichen ist der „menschliche Faktor" immer noch von grundlegender Bedeutung. Allerdings kann die Technologie zur Aufdeckung von Terroranschlägen jeder Art beitragen, unsere Systeme stabiler und unsere Abwehrmaßnahmen effektiver machen. Leider reicht die Technologie noch nicht aus, um uns vor Anschlägen zu warnen, *bevor* sie stattfinden und uns dabei zu helfen, sie zu verhindern.

A. TECHNISCHE HILFSMITTEL ZUR BEKÄMPFUNG DES NUKLEAR-TERRORISMUS (KERNWAFFEN UND „SCHMUTZIGE" BOMBEN)

Die erste Verteidigungslinie gegen Terroranschläge mit Kern- oder Strahlenwaffen sind robuste Systeme für den Schutz, die Kontrolle und die Bilanzierung von Kernwaffen und Kernmaterial an der Quelle. Eine Reihe von Technologien können die Sicherheit von Kernenergieanlagen erhöhen, darunter (von Computern, Überwachungskameras, Sensoren und Zugangskontrolleinrichtungen erstellte) automatische Erfassungsprotokolle und Aufzeichnungen, externe und interne Alarm- und Überwachungsanlagen, eine Zugangseinschränkung für Personal und Fahrzeuge sowie Biometriedaten (siehe unten, Kapitel D) nutzende Identitätsüberprüfungssysteme, ferner physische Barrie-

ren (Zäune, Mauern, ferngesteuerte Tore, Schleusen, Fahrzeugsperren) und sicherere Computersysteme und Softwarelösungen.

46. Auch der Einsatz von Systemen zur Erkennung unerlaubt mitgeführter Waffen und Materialien könnte sich als effektiv erweisen. Nach den Angriffen auf das World Trade Center musste die US-Regierung einige Male ihr Nuclear Emergency Search Team (NEST) einsetzen, um an verschiedenen Standorten in den Vereinigten Staaten nach möglicherweise vorhandenen Nuklearmaterialien oder „schmutzigen" Bomben zu suchen. Diese Aufgabe mag sich einfach anhören, da diese Materialien ja leicht nachweisbare Strahlungen – Gammastrahlen – aussenden. Das ist im Allgemeinen bei den aus dem Gesundheitssektor oder der Industrie herrührenden Materialien der Fall, die für die Herstellung einer „schmutzigen" Bombe verwendet werden können. Ein sachkundiger Terrorist könnte allerdings ein Strahlen abschirmendes Material wie Blei verwenden, um seine Waffe effektiv zu verbergen. Überraschenderweise sind einige der gefährlichsten Kernmaterialien wie Uran oder Plutonium nur recht schwache Gammastrahler und darum schwerer nachzuweisen. Darüber hinaus können schwach radioaktive Stoffe aufgrund der natürlichen Hintergrundstrahlung der Erde unter Umständen einem Nachweis entgehen.

47. Gammastrahlendetektoren, die mit dem strahlungsempfindlichen Element Germanium arbeiten, sind in der Regel sperrige Laborgeräte. Im März 2002 stellten jedoch drei dem US-Energieministerium (US DOE) unterstellte nationale Laboratorien einen neu entwickelten extrem empfindlichen Handheld-Detektor namens Cryo-3 vor, der Gammastrahlen-„Fingerabdrücke" radioaktiver Materialien nachzuweisen vermag. Er kann außerdem ihre genaue Energie ermitteln, da jede Art von radioaktivem Material andere Gammastrahlen aussendet. Dieses neue System könnte von Sondereinheiten der Polizei und Einsatzgruppen wie NEST verwendet werden.

48. Um Uran oder Plutonium zu finden, müssen die Detektoren nach Neutronen suchen, subatomaren Teilchen ohne elektrische Ladung, die nur sehr schwer nachzuweisen sind. Die US DOE-Laboratorien haben ein kleines, tragbares Gerät entwickelt, das von Spaltstoffen für Kernwaffen ausgesandte Neutronen nachweisen kann. Der Detektor ist so groß wie ein Kartenspiel und könnte internationalen Inspektoren helfen, die Terroristen am Einschmuggeln oder dem Einsatz von Kernwaffen und Kernmaterialien hindern sollen.

B. TECHNISCHE HILFSMITTEL ZUR BEKÄMPFUNG DES BIO- UND CHEMIEWAFFENTERRORISMUS

49. Die Möglichkeit von Angriffen mit Bio- oder Chemiewaffen und die unzähligen denkbaren Erreger, die in Waffen gegen unschuldige Opfer verwandelt werden könnten, haben die Besorgnisse der politisch Verantwortlichen deutlich gesteigert. In drei großen Bereichen kann die Technik weiterhelfen: 1. bei der Verhütung von Angriffen und Infektionen mit biologischen oder chemischen Substanzen; 2. bei der Erkennung biologischer und chemischer Kampfstoffe und 3. bei der Behandlung einzelner Patienten nach einem Einsatz dieser Stoffe. Die neuesten Forschungsarbeiten haben wissenschaftliche Entdeckungen erbracht, von denen einige noch in der Entwicklungsphase stehen und die zu technischen Hilfsmitteln führen werden, mit denen Staaten, Strafverfolger und Experten diese Aufgaben wahrnehmen können. Zu den erörterten Themen gehören Siliziumdrähte zum Aufspüren von Bomben, Mustererkennungssoftware und Biosensor-Chips, die vorhandene biologische und chemische Kampfstoffe erkennen.

Die Bedrohung durch biologische und chemische Waffen stellt die Vorbeugung mit physischen oder technischen Mitteln vor große Schwierigkeiten. Für chemische und biologische Stoffe gibt es zahlreiche unbedenkliche Anwendungen in der Industrie, der wissenschaftlichen Forschung und der medizinischen Therapie. Krankheitserreger und Toxine lassen sich aus natürlichen Quellen wie Tieren oder dem Boden gewinnen. Ein physischer Schutz vor extrem tödlichen Stoffen ließe sich in

Laboratorien oder Militäreinrichtungen verwirklichen, wo ihr Vorhandensein und ihre Verwendung bekannt und gesetzlich erlaubt sind. Technologien ähnlich denen, die für den Umgang mit Kernwaffen und Nuklearmaterial vorgeschlagen werden, könnten von Nutzen sein. Damit wäre aber nicht das Problem gelöst, wie sich verhindern lässt, dass chemische und insbesondere biologische Waffen in die Hände von Terroristen gelangen.

Die Entschlüsselung des menschlichen Genoms und die Offenlegung der Genome zahlreicher Krankheitserreger, das schnell wachsende Wissen über die molekularen Mechanismen der Pathogenese und der Immunantwort sowie neue Arzneimittel und Impfstoffe bieten noch nie da gewesene Chancen, mit Hilfe der Wissenschaft Bedrohungen durch Bioterroristen vorzubeugen und sie abzuwenden. Die gleichen Entwicklungen könnten jedoch auch einen Missbrauch der Wissenschaft zur Schaffung neuer Massenvernichtungswaffen erlauben. Wenn Terroristen der Zugang zu gefährlichen Erregern verwehrt werden soll, müssen zur Erhöhung der biologischen Sicherheit internationale Standards und Bestimmungen ausgearbeitet werden. Ihr Berichterstatter wird in Kapitel IV auf diese Frage eingehen.

Das Sandia-Laboratorium in den USA hat den effektivsten im Handel erhältlichen Chemikalien-detektor entwickelt. Er weist die gängigsten Nervengase und Hautkampfstoffe nach und kann auch zur Erkennung anderer Stoffe, wie z.B. erstickender Gase oder gasförmiger Hautkampfstoffe umprogrammiert werden. Die gegenwärtigen Biowaffendetektoren sind weit weniger effektiv als Chemiewaffendetektoren und können niemanden warnen, bevor die betreffende Person eine tödliche Dosis eines biologischen Kampfstoffs erhalten hat.

50. In der Erkenntnis, dass es bei einem Bioterroranschlag vor allem auf Schnelligkeit ankommt, wird zur Zeit an der Entwicklung eines „Labors auf einem Chip“ gearbeitet, das auch kleine Mengen einer biologischen oder chemischen Substanz in der Luft schnell zu identifizieren vermag. Das *Tissue Based Biosensors Program* der *Defense Advanced Research Project Agency* (DARPA) erwartet innerhalb von 18 Monaten einen Prototyp. Mit diesem Chip wird sich die Reaktionszeit auf die eingesetzten Stoffe verkürzen, sodass die Behörden Informationen und Therapiehinweise weiterleiten und möglicherweise auch die Angreifer ermitteln können. Nach den Milzbrandanschlägen erkannten die Verantwortlichen im Gesundheitswesen, dass die Testanordnung, mit der sie Krankheiten erkennen können, sie zu einem Kompromiss zwischen Genauigkeit und Schnelligkeit zwingt. Die Genauigkeit kam bisweilen zu kurz, als zum Beispiel einige Gebäude, die sich später als sicher erwiesen, milzbrandpositiv getestet wurden und umgekehrt.

51. Milzbrandbakterien stehen wegen der Anschläge in den Vereinigten Staaten ganz oben auf der Liste der biologischen Kampfstoffe, die bei weiteren Bioterrorangriffen eingesetzt werden könnten. Die Öffentlichkeit interessiert sich wieder mehr dafür, wie die Krankheit sich auswirkt. Jüngste Forschungsarbeiten, die von einem der führenden Milzbrandexperten im *Scientific American* vorgelegt wurden, weisen auf einige neue Erkenntnisse hin. Milzbrand wird gegenwärtig mit einem Antibiotikum behandelt – dem mittlerweile allseits bekannten „Cipro“ –, das eine Vermehrung der Bakterien verhindert. Dieses Antibiotikum lässt das Milzbrandtoxin jedoch intakt, das aus drei gefährlichen Proteinen besteht, die sich nach dem Eindringen in eine Zelle ausbreiten. Im letzten Sommer wurde die entscheidende Liste der Rezeptorproteine der Toxine entdeckt, womit weitere Forschungen über eine eventuelle Hemmung ihrer Aktivität möglich geworden sind. Gegenwärtig wird ein diese Toxine neutralisierendes Präparat an Ratten getestet. Ebenso wird zurzeit aus einem mittels rekombinanter DNA-Technologie entwickelten Antigen eine neue, schnellere Vakzine entwickelt. An weiteren technologischen Fortschritten wird gearbeitet, um verschiedene biologische und chemische Bedrohungen bekämpfen zu können, so z.B. Pocken, Lungenpest, tödliche Gase und sogar das Ebola- und das Marburg-Virus.

52. Auch neue Software kann bei dem Behandlungsprozess helfen. Die Symptome bestimmter Krankheiten können an banale Erkrankungen erinnern. Während der Milzbrandpanik in den USA

forderte der damalige Bürgermeister von New York, Rudolph Giuliani, die Bürger seiner Stadt auf, sich gegen Grippe impfen zu lassen, damit sie bei ihrer Wintergrippe nicht gleich an Milzbrand dächten. Die für Krankenhäuser in Entwicklung befindliche Software erkennt Symptomschemata und einen Ausbruch frühzeitig. Ein US-Unternehmen lizenziert Softwaretechnologie, die Infektionskrankheiten auch anhand extrem kleiner Proben erkennen kann.

Eine weitere Verteidigungslinie gegen den Bioterrorismus wäre Mike Powers vom CBACI zufolge eine Verbesserung des inländischen Bereitschaftsgrades durch Schulung des Notfallpersonals, Ausbau des öffentlichen Gesundheitswesens, Einlagerung medizinischer Versorgungsgüter und Verbesserung der Impfstoffe.

53. Im öffentlichen Gesundheitswesen haben die Ärzte sich Gedanken über bisher unvorstellbare Szenarien machen müssen. Die Milzbrandfälle beschworen das Gespenst einer umfassenden Krise der Gesundheitsversorgung herauf, bei der nicht speziell geschulte Ärzte eine Flut von Patienten behandeln müssen, die einem bioterroristischen Anschlag zum Opfer gefallen sind. Zurzeit wird neue, internetgestützte Software entwickelt, die Ärzten in der Notaufnahme Zugang zu einem Online-Kurs über Bioterrorismus im Operationssaal gibt. Der Kurs wird aus drei Teilen bestehen – Milzbrand und Bakterien, Chemiewaffen und Viren sowie Mustererkennung – und mit dem US Center for Disease Control and Prevention abgestimmt werden.

54. Auch die Mikrotechnologie könnte im Kampf gegen den Bioterrorismus eine potenzielle Hilfe darstellen. Der kleinste Roboter der Welt wird zurzeit in den Sandia National Laboratories in den USA entwickelt. Mit diesem Gerät von der Größe einer Küchenschabe werden biologische und chemische Kampfstoffe und sogar Bomben oder Minen erkannt werden können. An dem jeweiligen Standort könnten einige dieser Mikroroboter eingesetzt werden, um die Art der vorliegenden Bedrohung zu ermitteln.

C. TECHNOLOGIEN GEGEN DEN CYBERTERRORISMUS

55. Der Einsicht in die grundlegende Verwundbarkeit unserer von der Informationstechnik abhängigen entscheidenden Infrastruktureinrichtungen für drohende Cyberangriffe kommt große Bedeutung zu. Dennoch könnten mit Hilfe einer Reihe von Technologien höhere Barrieren errichtet und dem öffentlichen Sektor wie der Privatwirtschaft Hilfsmittel zur Erkennung, zur Abwehr und für die Überwindung solcher Attacken zur Verfügung gestellt werden. In den Vereinigten Staaten hat vor kurzem die DARPA im Rahmen ihrer Informationssicherungs- und Überlebensfähigkeitsprogramme verschiedene Technologien entwickelt, die zum Schutz der Netzwerke des Verteidigungsministeriums beitragen. Einige dieser Programme können zum Beispiel 1. die Auswirkungen von Cyberattacken auf bestimmte Informationssysteme bewerten, 2. korrumpierte oder bösartig geschädigte Netzwerkbereiche isolieren, 3. Denial-of-Service-Angriffe und andere Attacken vereiteln und 4. groß angelegte Analysen vornehmen, mit deren Hilfe sich das Ausmaß, die Virulenz und die Ausbreitungsgeschwindigkeit umfassender Attacken ermitteln lassen.

56. Viele verbündete Regierungen überwachen den elektronischen Kommunikationsverkehr. In den Vereinigten Staaten hat das FBI zwei wichtige Internet-Überwachungssysteme entwickelt: Carnivore und Magic Lantern. Das erste ist ein Gerät, das auf gerichtliche Anordnung bei Internet-Anbietern (ISPs) zum Durchsuchen des E-Mail-Verkehrs installiert werden kann. Carnivore sucht nur nach ganz bestimmten Empfängern von Schlüsselwörtern in von Verdächtigen abgesandten E-Mails, sodass die Sicherheitskräfte Zeit sparen und sich auf die aussagekräftigsten Mitteilungen konzentrieren können. Magic Lantern und andere „Key-Logging"-Programme erlauben Bediensteten, die über einen Durchsuchungsbefehl verfügen, jeden Tastaturanschlag auf einem bestimmten Computer zu erfassen. Dadurch können Passwörter offenbart werden, denen entscheidende

Bedeutung zukommt, wenn Kriminelle oder Terroristen leistungsfähige Verschlüsselungssoftware verwenden.

57. In den Vereinigten Staaten erzwingen Innovationen im Softwarebereich eine erneute Partnerschaft zwischen dem amerikanischen Militär und den Laboratorien und Softwareentwicklungsfirmen im Silicon Valley. Viele Programmierer und Wissenschaftler, die im Zuge der jüngsten Rezession ihren Arbeitsplatz verloren, sind nun bereit, dem „Waffenappell" der US-Regierung Folge zu leisten. Keine Technologie scheint ausgeklammert zu werden, und es wird allgemein anerkannt, dass ein Informationsaustausch – ob nun zwischen dem Staat und der Wirtschaft oder zwischen verschiedenen Staaten – einen entscheidenden Bestandteil der Terrorismusbekämpfung bildet.

58. Angemessene Finanzmittel für Forschungsarbeiten zur Cybersicherheit sind ebenfalls eine Grundvoraussetzung, um der sich abzeichnenden cyberterroristischen Bedrohung begegnen zu können. Ein entsprechendes Gesetz wurde im Februar 2002 im US-Repräsentantenhaus angenommen. Nach diesem Cyber Security Act, das von dem Vorsitzenden des Wissenschaftsausschusses (und ehemaligen Vorsitzenden Ihres Ausschusses) Sherwood Boehlert eingebracht wurde, wird die National Science Foundation neue Forschungszentren für Sicherheit in der Informationstechnik errichten und eine Reihe von Studienbeihilfen ausloben. Aufgrund des Gesetzes werden für diese neuen Programme 880 Millionen US-Dollar bereitgestellt.

Im Dezember 2001 forderte der Europäische Rat eine „umfassende Sicherheitsstrategie für elektronische Netzwerke einschließlich praktischer Umsetzungsmaßnahmen", und der eEurope-Aktionsplan 2005 umreißt eine Reihe von Strategien zur Förderung praktischer Sicherheitsmaßnahmen, einer Sicherheitskultur und vertrauenswürdiger Netzwerke. Die von Rand Europe koordinierte Dependability Development Policy Initiative (DDSI), die von Juni 2001 bis Oktober 2002 durchgeführt wurde, ist ein Projekt zur Unterstützung der Ausarbeitung von Maßnahmen zur Informationssicherheitspolitik. An der Initiative, die Leitlinien für europäische FuE-Programme und politische Schritte auf dem Gebiet der Informationssicherung und -sicherheit anbietet, waren der öffentliche Sektor wie auch die Privatwirtschaft beteiligt.

D. SONSTIGE TECHNOLOGIEN

59. Verschiedene Technologien, die nicht unbedingt mit den in diesem Bericht betrachteten Bedrohungen zusammenhängen, könnten sich in dem weltweiten Kampf gegen den Terrorismus als nützlich erweisen. Wissenschaftler unterziehen das gesamte technische Grundgefüge unserer Gesellschaften (Gebäude, Straßen, Eisenbahnnetze, Wasserversorgung, Elektrizitätsnetze usw.) einer Überprüfung und fragen sich, wie es besser gegenüber der zerstörerischen Gewalt des Terrorismus abgesichert werden kann. Ingenieure, Sicherheitsberater und Stellen für Terrorismusbekämpfung entwickeln zurzeit Technologien, mit denen Teile der Infrastruktur zu einem sichereren, „seiner selbst bewussten" System verbunden werden sollen. Der Grundgedanke, der von Forschern des Massachusetts Institute of Technology (MIT) ausgearbeitet wurde, besteht dabei darin, „die einzelnen „Fäden" dieser technologischen Struktur miteinander zu verweben und überall Geräte einzubauen, die im Krisenfall schädliche Chemikalien in einem Trinkwasserreservoir erkennen, Rettungskräften Daten über die Statik eines beschädigten Gebäudes übermitteln, zur Angabe möglicher Fluchtwege beitragen oder die Stromversorgung optimieren können." In Verbindung mit Simulationswerkzeugen, verbesserten Kommunikationswegen und sichereren Gebäudekonstruktionen könnten solche High-Tech-Netzwerke letztlich eine Art „intelligente Stadt" entstehen lassen, in der Gefahren lokalisiert und Notfallmaßnahmen zielgenau gesteuert werden können.

60. Andere Technologien werden in der Praxis gezielt eingesetzt, um Terroristen aufzuspüren, noch bevor sie zuschlagen können. Biometrische Verfahren versprechen den Einsatz von Personenerkennungssystemen, die hierbei hilfreich sein könnten. Die Biometrie nutzt persönliche Merkmale zur sofortigen Identifizierung: Fingerabdrücke, Irismuster, Voiceprints (Sprachmuster) und Unterschriften können im Vergleich mit Gegenstücken in einer Datenbank verifiziert werden. Dass zwei Menschen die gleiche Iris besitzen, ist extrem unwahrscheinlich ($1:10^{78}$). In letzter Zeit wurde die Iriserkennungsmethode nach Zufallsverfahren in Saudi-Arabien während der alljährlichen Pilgerfahrt nach Mekka eingesetzt. Von zufällig ausgewählten Gläubigen wurde mit Hilfe der Iriserkennungstechnik eine Datei erstellt, die später zur Identifizierung genutzt werden konnte. Auf einigen Flughäfen in den Vereinigten Staaten wird mit dieser Methode der Zugang zu Sicherheitsbereichen überwacht.

61. Mit Hilfe dieser Verfahren könnte auch die Ausstellung amtlicher Dokumente, z.B. von Pässen, Zugangsgenehmigungen, Führerscheinen oder Sozialversicherungskarten, überwacht werden. In viele dieser Dokumente sind schon heute winzige, Daten enthaltende Computerchips eingelassen. Darüber hinaus könnten diese Chips auch eine verschlüsselte Version eines einzigartigen biometrischen Erkennungsmerkmals enthalten, z.B. einen digital gescannten Fingerabdruck oder ein Irismuster, sodass es so gut wie unmöglich wäre, ein falsches Dokument zu erstellen oder die Identität einer anderen Person anzunehmen. Die gleiche Technik könnte auch für die Ausstellung von Visa an ausländische Besucher verwendet werden, was die Vereinigten Staaten und Kanada bereits vereinbart haben.

62. Auch die Grenzkontrollen könnten durch neue Technologien verbessert werden. Nicht eigens ausgewiesene Übergänge könnten mit Webcams (Internetkameras) überwacht werden, die Bewegungen oder Wärme erkennen. Andere Kameras können Menschenmengen optisch abtasten, um Gesichter zu erfassen und mit Computer-Datenbanken abzugleichen, in denen die Gesichtsgeometrie bekannter oder mutmaßlicher Terroristen gespeichert ist. Ein besserer Zugriff auf Datenbanken könnte auch bei der Grenzüberwachung sehr nützlich sein. Außerdem könnten solche Technologien zur großräumigen Überwachung sensibler Infrastruktureinrichtungen wie Kernkraftwerke, biochemische Forschungsanlagen oder Trinkwasserspeicher Verwendung finden.

IV. NICHTVERBREITUNGSREGELUNGEN UND ANDERE MULTILATERALE ANSTRENGUNGEN

63. Nach Ansicht Ihres Berichterstatters gehört zu jeder weltweiten Strategie der Terrorismusprävention, -abwehr und -bekämpfung – insbesondere in Bezug auf den CBRN-Terrorismus – ein kohärenter Rahmen multilateraler Nichtverbreitungsinitiativen unter Einschluss der bestehenden Verträge und anderer Kooperationsstrategien. Auch wenn wir in Nichtverbreitungsmaßnahmen kein Allheilmittel sehen sollten, können sie doch Terroristen Möglichkeiten nehmen, CBRN-Waffen zu beschaffen oder zu entwickeln. Die gegenwärtigen Nichtverbreitungsregelungen sollen gewöhnlich Staaten vom Erwerb von Massenvernichtungswaffen (MVW) abhalten und zielen nicht auf nichtstaatliche Gruppierungen oder Einzelpersonen ab. Wie jedoch Amy Sands, der Stellvertretende Direktor des CNS, diesem Unterausschuss im letzten Sommer in Monterey mitteilte, gilt hierfür, dass „je mehr Staaten zur Verbreitung von MVW beitragen und entsprechende Programme betreiben, desto größer … auch die Möglichkeit (ist), dass Akteure unterhalb der staatlichen Ebene solche Waffen erwerben, ob nun über direkte Unterstützung oder auf verdecktem Wege einschließlich Diebstahl“. Wenn nichts geschieht, um internationale (bilaterale und multilaterale) Nichtverbreitungsregelungen und Exportkontrollmaßnahmen zu stärken, erhalten nichtstaatliche Akteure und Terroristengruppen viel leichter Zugang zu dem für die Herstellung und den Einsatz von CBRN-Waffen benötigten Wissen. Darüber hinaus bilden diese Verträge und Übereinkommen einen völkerrechtlichen Rahmen, der die allgemeine Überzeugung stützt, dass Massenvernichtungswaffen für die Kriegführung letztlich nicht akzeptabel sind. Ebenso können sie

unter Wissenschaftlern und in anderen Kreisen die humanitäre Grundüberlegung verbreiten, dass diese Waffen verabscheuenswürdig und gesetzwidrig sind.

64. Wir wollen in diesem Kapitel versuchen, einen Überblick über die bestehenden Nichtverbreitungsverträge, -programme und -initiativen zu geben, die für die in diesem Bericht analysierten Bedrohungen unmittelbar relevant sind und zu ihrer Bewältigung beitragen können. Außerdem folgen einige Anregungen zu denkbaren Möglichkeiten, diese Regelungen auszubauen sowie zu auf das neue Sicherheitsumfeld zugeschnittenen neuen Strategien und Initiativen.

A. KERNWAFFEN

65. In dem Generalbericht des Ausschusses aus dem Jahre 2001 wurden detailliert die Initiativen analysiert, die Russland und andere aus der Sowjetunion hervorgegangene unabhängige Staaten (NIS) in Zusammenarbeit mit den Vereinigten Staaten und anderen Mitgliedern der internationalen Gemeinschaft ergriffen haben, um die Sicherheit ihrer Kernmaterialien zu verbessern und die Grenzüberwachung effizienter zu gestalten. Die US-Programme zur Unterstützung Russlands bei der Bewältigung seines riesigen nuklearen Komplexes gerieten 2002 in einige Schwierigkeiten. Im April teilte die US-Administration mit, sie könne Russlands Engagement bei der Einhaltung einer Reihe entscheidender Standards, wie z.B. der Befolgung „aller einschlägigen Rüstungskontrollvereinbarungen“, nicht bestätigen. Infolge der Weigerung der Administration, die Einhaltung durch Russland zu bescheinigen, wurden die Planungen für weitere Programme und die Finanzierung erst einmal eingestellt. Die Administration ersuchte jedoch den Kongress, von der Forderung nach einer Bestätigung („Zertifizierung“) absehen zu dürfen, sodass Finanzmittel für die Nichtverbreitung auch ohne Verweis auf die Einhaltung der Bestimmungen durch Russland bereitgestellt werden konnten. Diese von dem Kongress im August 2002 erteilte Ausnahmegenehmigung ist am 1. Oktober 2002 ausgelaufen, womit die Fortsetzung der Nichtverbreitungsunterstützung in Russland durch die USA einmal mehr gefährdet ist. Für die Vorlage im Senat wurde ein einschneidender Gesetzentwurf erwartet, der eine dauerhafte Ausnahmegenehmigung im Hinblick auf Einschränkungen der Nichtverbreitungsunterstützung fordert. Der Entwurf findet bei der Administration vollen Rückhalt: Außenminister Colin Powell rief den Kongress auf, „uns möglichst bald eine dauerhafte Ausnahmegenehmigung zuzubilligen“. Bei einer Begegnung im Juli dieses Jahres in der Bundeshauptstadt Washington schlug das führende republikanische Mitglied des Außenpolitischen Ausschusses, Senator Richard Lugar, gegenüber diesem Unterausschuss vor, die Finanzierung von US-Programmen zur Vernichtung oder Sicherung von MVW in den Staaten der ehemaligen Sowjetunion – zu deren Einführung er (zusammen mit dem ehemaligen Senator Sam Nunn) Anfang der 1990er Jahre beigetragen hatte – deutlich aufzustocken.

Das MPC&A-Programm des US-Verteidigungsministeriums zur Sicherung, Überwachung und Bilanzierung von Kernmaterialien und andere Programme des US-Energieministeriums haben bereits bei rund 40% der nuklearen Materialien in den NIS Maßnahmen zur Erhöhung der Sicherheit durchgeführt. Nach dem 11. September unterzog die Bush-Administration diese Programme einer umfassenden Überprüfung, was in erster Linie zu einer beträchtliche Haushaltsaufstockung und einer Beschleunigung der Sicherheitsarbeiten in Russland und anderswo führte. Das Gesamtbudget für „*Defense Nuclear Nonproliferation*“ im Haushaltsjahr 2002 beträgt über 1 Milliarde Dollar (36% mehr als im Haushaltsjahr 2001), und für das Haushaltsjahr 2003 hat der Kongress Mittel in Höhe von $ 1,1 Mrd. angefordert. Zu dem Programm gehören eine Reihe von Aktivitäten zur Sicherung von Kernmaterialien in militärischen und zivilen Einrichtungen, zur Unterstützung ehemaliger sowjetischer Wissenschaftler und zum Ausbau der Grenzüberwachung in Russland.

66. Für eine sachgerechte Auseinandersetzung mit der Bedrohung durch Nuklearschmuggel in den NIS ist eindeutig weiterhin eine verstärkte bilaterale (Vereinigte Staaten-Russland) und

internationale Zusammenarbeit erforderlich. Die US-Administration hat ihre Verbündeten zu größeren Beiträgen zu Bedrohungsverminderungsprogrammen aufgefordert. Im Juni 2002 verkündeten die G-7-Staaten das „10 Plus 10 Over 19"-Programm, bei dem der Beitrag der USA von $10 Mrd. zu Bedrohungsverminderungsprogrammen während der nächsten 10 Jahre von den übrigen G-7-Staaten zusammengenommen durch Leistungen in gleicher Höhe ergänzt werden wird. Während bei einem solchen Betrag der derzeitige Stand der Finanzierung von Bedrohungsverminderungsprogrammen durch die USA beibehalten würde, käme es zu einem deutlichen Anstieg der Beiträge anderer G-7-Staaten, und zur Erfüllung dieser neuen Verpflichtung werden geänderte Finanzierungspläne erforderlich sein.

Im Juni 2002 beschlossen die G-8-Staaten (einschließlich Russlands) in Kanada sechs Grundsätze, um Terroristen den Zugang zu Massenvernichtungswaffen zu verwehren. Zu diesen Grundsätzen gehörten Verpflichtungen, effektive Grenz- und Exportkontrollen einzurichten und aufrechtzuerhalten und den Staaten bei der Sicherung des Transports und der Lagerung von MVW und ähnlicher Materialien zu helfen.

Darüber hinaus planen die Vereinigten Staaten und ihre Verbündeten zusammen mit den NIS im Rahmen der Terrorismusbekämpfung einen regelmäßigen Austausch von Aufklärungsdaten zum Nuklearschmuggel. Innerhalb der NATO wird zurzeit an einer Verbesserung des internationalen Austauschs von Aufklärungserkenntnissen über alle Aspekte des potenziellen Schmuggels und der illegalen Weitergabe von Massenvernichtungswaffen oder Vorläufermaterialien gearbeitet. Auch internationale Organisationen wie die IAEA und Interpol sind an diesen Anstrengungen beteiligt.

67. Die NATO spielt über ihr Zentrum für Massenvernichtungswaffen eine führende Rolle bei der Erfassung von Informationen über Hilfsprogramme für Russland. Im Jahre 2001 stellte sie ihre *Matrix of Bilateral WMD Destruction and Management Assistance Programmes* vor, eine Datenbank aller derartigen Programme in allen Staaten und bei allen internationalen Organisationen, mit der Doppelarbeit vermieden und die Koordinierung erleichtert werden kann.

68. Auch viele andere Staaten könnten beim physischen Schutz von Kernenergieanlagen und Nuklearmaterialien noch Verbesserungen vornehmen. Mit dem Nichtverbreitungsvertrag (NVV) wurde ein internationales System nuklearer Safeguards aufgebaut, das von der IAEA verwaltet wird und verhindern soll, „dass Kernenergie von der friedlichen Nutzung abgezweigt und für Kernwaffen oder sonstige Nuklearsprengkörper verwendet wird" (Art. III NVV). Mit Hilfe der IAEA-Safeguards würde letztlich das Fehlen von Material in Kernenergieanlagen festgestellt werden, doch vermögen sie einen wirksamen physischen Schutz nicht zu ersetzen. Die meisten Staaten nehmen eine physische Sicherung ihrer Nuklearanlagen vor: Mauern, Zäune, Wachpersonal, Sensoren und Alarmanlagen. Im März 2002 kündigte die IAEA in der Erkenntnis, dass „die nationalen Maßnahmen zum Schutz von Nuklearmaterialien und entsprechender Einrichtungen … von ihrer Substanz und ihrem Inhalt her ungleichwertig (sind)", einen Aktionsplan zur Erweiterung des weltweiten Schutzes an, das so genannte PANT-Programm (*Protection Against Nuclear Terrorism*). Zu dem Plan gehören Verbesserungen des physischen Schutzes, die Aufdeckung böswilliger Aktivitäten in Verbindung mit Nuklearmaterialien und der Ausbau der nationalen Bilanzierungs- und Kontrollsysteme für Nuklearmaterialien. Aus den Reihen der gegenwärtigen NATO-Mitglieder haben die Niederlande, das Vereinigte Königreich und die USA finanzielle Unterstützung für den Aktionsplan versprochen, und Frankreich, Deutschland und die Türkei haben eine Unterstützung durch Sachleistungen zugesagt. Die IAEA wird weitere Mittelzusagen benötigen, um ihren veranschlagten jährlichen Finanzierungsbedarf von $ 12 Mio. für Programme und von $ 20 Mio. für dringende Sicherheitsverbesserungen decken zu können.

69. Gegenwärtig wird in keinem multilateralen Übereinkommen ein Schutz von Kernmaterial und Nuklearanlagen vor solchen Bedrohungen verlangt. Ein Vertrag, das Übereinkommen über den physischen Schutz von Kernmaterial aus dem Jahre 1980, bezieht sich ausschließlich auf ziviles

Nuklearmaterial während seiner grenzüberschreitenden Beförderung. Zurzeit werden Vorschläge erörtert, um dieses Übereinkommen zu ändern und sein Anwendungsgebiet auf ziviles Nuklearmaterial, Lagerung und Beförderung sowie Nuklearanlagen im Inland auszuweiten.

B. BIOWAFFEN

70. Das Übereinkommen von 1972 über biologische Waffen und Toxine (BWÜ), das die Entwicklung, Herstellung und Lagerung biologischer Waffen verbietet, ist der umfassendste internationale Vertrag, der sich mit Biowaffen beschäftigt. Allerdings weist das BWÜ keine Zwangsmaßnahmen auf, um die Umsetzung des Übereinkommens zu verbessern. Auf der Fünften BWÜ-Überprüfungskonferenz wurde im November 2001 ein Vorschlag eines rechtlich bindenden Textes (das Ergebnis sechsjähriger Bemühungen einer Ad-hoc-Gruppe von Vertragsstaaten) von den Vereinigten Staaten abgelehnt, weil er für die Verhütung der Verbreitung von Biowaffen unzulänglich sei. Viele Vertragsstaaten wandten ein, das vorgeschlagene Protokoll hätte zwar nicht das Gesamtproblem biologischer Waffen (und insbesondere das des Bioterrorismus) gelöst, aber zumindest rechtlich bindende Verfahren eingeführt, um gegen der Entwicklung solcher Waffen verdächtigte Staaten vorgehen zu können.

71. Der Schritt der USA bedeutet eine ernste Gefahr für die Zukunft des BWÜ. Wie die Treffen und Informationssitzungen dieses Ausschusses im Juli dieses Jahres in den Vereinigten Staaten deutlich gemacht haben, steht die Bush-Administration, obwohl sie über die Bedrohung durch biologische Waffen und den Bioterrorismus sehr besorgt ist, multilateralen Nichtverbreitungsabkommen im Allgemeinen ablehnend gegenüber und wendet sich auch gegen Verifikationsmaßnahmen, die nach ihren Befürchtungen ihre geheimen Bioabwehr- und Aufklärungsaktivitäten an den Tag bringen könnten. Diese Haltung wurde im September bestätigt, als die US-Administration ihren Verbündeten mitteilte, sie wünsche eine Verschiebung weiterer Gespräche über das BWÜ bis 2006. Die BWÜ-Überprüfungskonferenz soll im November 2002 wieder zusammentreten.

Auf der Suche nach Alternativansätzen zur Stärkung des BWÜ veröffentlichte die britische Regierung im April ein Grünbuch, in dem sie mehrere neue Ideen vorschlug. Der wichtigste dieser Gedanken beruht auf Artikel VI des Übereinkommens, der Vertragsstaaten bei Verdacht auf Nichteinhaltung eine Beschwerde beim VN-Sicherheitsrat erlaubt. Da dieser Mechanismus noch nie angewandt worden ist, schlägt das Vereinigte Königreich vor, dem VN-Generalsekretär zusätzlich die Befugnis zu erteilen, bei einem verdächtigen Ausbruch von Krankheiten und Verdacht auf einen Missbrauch von Einrichtungen Ermittlungen anzustellen.

72. Zusammen mit ihrer Ablehnung des vorgeschlagenen BWÜ-Protokolls regten die Vereinigten Staaten eine Reihe freiwilliger Maßnahmen einzelner Staaten ohne bindende vertragliche Verpflichtung an. Insbesondere fordert die Bush-Administration 1. die Vertragsstaaten auf, illegale Biowaffenaktivitäten in ihrer einzelstaatlichen Gesetzgebung strafrechtlich zu untersagen, 2. Mechanismen zur Untersuchung verdächtiger Krankheitsausbrüche oder eines behaupteten Einsatzes von Biowaffen einzuführen und 3. die Vertragsstaaten zu verstärkter technischer und wissenschaftlicher Zusammenarbeit beim Ausbruch schwerer Erkrankungen anzuhalten. Die meisten dieser nicht völlig neuen Vorschläge werden von der Mehrzahl der übrigen Vertragsstaaten und zahlreichen Experten – auch aus den USA – als zwar interessant, aber unzureichend betrachtet. In der Tat werden darin keine nachdrücklichen internationalen Maßnahmen vorgesehen, wie zum Beispiel ein gesetzlich zwingend vorgeschriebener Informationsaustausch, Inspektionen vor Ort und Sanktionen bei Verstößen.

Um diese Vorgehensweise zu stärken und einen Flickenteppich einzelstaatlicher Gesetze zu vermeiden, regten CNS-Experten in Monterey an, die Vereinigten Staaten und ihre Verbündeten

sollten sich für ein internationales Biosicherheitsübereinkommen einsetzen, um den unbefugten Zugang zu Krankheitserregern zu verhindern und den Handel mit Bakterienkulturen zu regulieren. Das Übereinkommen soll eine Reihe grundlegender Verpflichtungen und Leitlinien festlegen, die von jedem Mitgliedstaat in seiner eigenen Gesetzgebung im Einzelnen umgesetzt werden würden. Die Schaffung einheitlicher Biosicherheitsstandards würde nicht nur strengere internationale Bestimmungen über den Zugang zu gefährlichen Erregern einführen, sondern auch die Forschungszusammenarbeit zwischen den Verbündeten bei der Entwicklung neuer Impfstoffe und Präparate zu Verteidigungszwecken erleichtern.

Zur Umgehung der Schwierigkeiten des Biowaffenübereinkommens sind auch in anderen Foren Initiativen ergriffen worden. Auf ihrer Sitzung im Juni beschlossen die 34 Mitglieder der Australia Group, von der die Exportkontrollaktivitäten bei chemischen und biologischen Dual-Use-Substanzen und -Technologien koordiniert werden, mehrere neue Maßnahmen zu einer deutlichen Ausweitung der Exportkontrollen. Die Gruppe bemüht sich außerdem, durch die Überwachung von Informationen, die zur Herstellung von Bio- und Chemiewaffen dienen könnten, verstärkt Terroristen ins Visier zu nehmen. Die Ausfuhr wichtiger DNA-Bestandteile unterliegt bereits Einschränkungen, und diese Maßnahme könnte auch auf genetische Informationen über gefährliche Krankheitserreger ausgedehnt werden.

Auch die NATO überprüft zurzeit ihre Strategie gegen chemische und biologische Angriffe. Das MVW-Zentrum hat neue Programme über Verbreitungsfragen und terroristische Bedrohungen ausgearbeitet und fördert darüber hinaus Workshops, Seminare und Schulungen zur Erhöhung des Bereitschaftsgrades der einzelstaatlichen Stellen im Hinblick auf Angriffe mit Bio- und Chemiewaffen. So beschäftigte sich ein Workshop im März 2002 mit der Erarbeitung wirksamer logistischer, operativer und medizinischer Mechanismen für den Umgang mit einem Angriff mit Bio- oder Chemiewaffen. Aus den Arbeiten des Prager Gipfels (21./22. November 2002) dürften sich neue Initiativen zur Abwehr von MVW ergeben. Dazu werden wahrscheinlich ein mobiles ABC-Analysenlabor, ein ABC-Reaktionsteam, ein virtuelles „*Centre of Excellence*“ für ABC-Waffen-Abwehr, ein NATO-Lager für die B- und C-Waffenabwehr und ein Krankheitsüberwachungssystem gehören.

C. CHEMIEWAFFEN

73. Das Chemiewaffenübereinkommen (CWÜ) von 1993, das die Entwicklung, die Herstellung, den Erwerb, die Lagerung, das Zurückbehalten oder die Weitergabe chemischer Waffen untersagt (und darüber hinaus deren Vernichtung verlangt), ist wohl das komplexeste und am weitesten gehende Nichtverbreitungsübereinkommen aller Zeiten. Seine strengen Verifikationsbestimmungen werden von der Organisation für das Verbot chemischer Waffen (OPCW) gehandhabt, die (nach dem Stand vom April 2002) recht erfolgreich die Vernichtung von 6 700 Tonnen Chemiewaffen, zwei Millionen Stück Munition und Behälter und 27 Chemiewaffen-Produktionsanlagen überwacht und 1 169 Inspektionen durchgeführt hat, um die Einhaltung der Bestimmungen durch die Staaten zu verifizieren. Die Vernichtung der gewaltigen deklarierten Chemiewaffenbestände Russlands hat jedoch noch nicht begonnen.

In diesem Jahr ging die Organisation durch Turbulenzen, die ein Schlaglicht auf einige ihrer Finanz- und Managementprobleme warfen. Auf einer CWÜ-Sonderkonferenz im April wurde der brasilianische OPCW-Generaldirektor José Mauricio Bustani von CWÜ-Vertragsstaaten (mit 48 Neinstimmen bei 7 Jastimmen und 43 Enthaltungen) abgewählt, womit eine von den Vereinigten Staaten angeführte dreimonatige diplomatische Kampagne zu Ende ging. Washington warf Bustani Mismanagement im Personal- und Finanzbereich der OPCW sowie „schlecht durchdachte Initiativen“ vor, die die Organisation von ihrer Hauptaufgabe der Verifikation abgebracht hätten. Obwohl viele Staaten einige der Bedenken der USA teilten und zu Bustanis Fähigkeiten kein Ver-

trauen mehr hatten, betrachten viele die Problembehandlung durch die Bush-Administration zugleich als unnötig plump und zerstörerisch.

Die Finanzprobleme der OPCW liegen dabei teils an verspäteter Entrichtung von Mitgliedsbeiträgen, teils am so genannten „Besitzerprinzip", wonach die Staaten der Organisation die Kosten erstatten müssen, die dieser durch die Überwachung der Vernichtung ihrer Chemiewaffenbestände entstehen. Haushaltsansätze werden nach von den Besitzerstaaten vorgelegten Plänen erstellt, die bisweilen ungenau oder zu ehrgeizig sind. 2001 gingen bei der OPCW fast die gesamten veranschlagten Beiträge der Mitgliedstaaten, jedoch nur 1% der Inspektionserstattungen ein. Daraus ergab sich ein Haushaltsdefizit von rund € 4,3 Mio. bei einem genehmigten Haushalt von € 60,2 Mio. Dementsprechend wurden 2001 nur 68% der geplanten Verifikationsaktivitäten durchgeführt – zumeist Pflichtaufgaben im Gegensatz zu Ermessensaufgaben, wie z.B. Industrieinspektionen. Obwohl das Übereinkommen unangemeldete Inspektionen zulässt, wurden sie noch nie von OPCW-Mitgliedern verlangt.

Im Juli wurde der argentinische Diplomat Rogelio Pfirter für vier Jahre zum neuen Generaldirektor der OPCW ernannt. Neben der Lösung von Management- und Haushaltsproblemen wird sich Herr Pfirter im Hinblick auf die erste CWÜ-Überprüfungskonferenz im April 2003 einer Reihe von Herausforderungen gegenübersehen, darunter dem zu findenden Gleichgewicht zwischen Verifikation der Bestandsvernichtung und Verifikation von Verstößen, dem Verhältnis zwischen dem CWÜ und dem BWÜ und den Auswirkungen des wissenschaftlich-technischen Fortschritts.

74. In Verbindung mit ihren Studien zur Umsetzung des CWÜ und des BWÜ führt die Science and Technology Policy Research Unit (SPRU) an der University of Sussex Forschungsarbeiten zur Frage der Dual-Use-Technologien im Rahmen der wehrtechnischen und der zivilen Forschung und Entwicklung (FuE) durch. Ihre Experten erläuterten dem Unterausschuss, dass FuE-Ergebnisse oft für militärische wie für zivile Zwecke genutzt werden können. Die Arbeiten der SPRU konzentrieren sich auf die Untersuchung von Dual-Use-Technologien speziell in der chemischen und biotechnologischen Industrie/Forschung und auf die Entwicklung von Kontrollstrategien. Das geht auf die Erkenntnis zurück, dass der internationale Waffenhandel nicht mehr nur die Lieferung von Waffen, sondern auch die Weitergabe kommerzieller Technologien umfasst. In baldiger Zukunft werden neue Kontrollregelungen nötig werden, um diese Handelsströme zu steuern. Die Forscher der SPRU beschäftigen sich vor allem mit der Frage, wie die entsprechenden Industriezweige und die FuE auf dem Gebiet der zivilen Biotechnologie in internationale Kontrollregelungen einbezogen werden sollen.

D. CYBERTERRORISMUS

75. Im Anschluss an Forderungen aller Verbündeten nach einer effektiveren internationalen Zusammenarbeit für den Fall grenzüberschreitender Cyberattacken könnte demnächst ein vom Europarat ausgearbeitetes internationales Übereinkommen zur Bekämpfung des Cyberterrorismus zustande kommen. Im November 2001 unterzeichneten gut 30 Staaten, darunter alle EU-Mitglieder, Kanada, Japan, Südafrika und die Vereinigten Staaten ein vom Europarat entworfenes internationales Übereinkommen zur Computerkriminalität. Dieses weit gespannte Übereinkommen beschäftigt sich mit der internationalen Zusammenarbeit bei den meisten Aspekten der Computerkriminalität – einschließlich des Betruges, der Veruntreuung sowie Leib und Leben bedrohender Verbrechen –, und seine Unterzeichner werden rund um die Uhr besetzte nationale Zentren errichten müssen, um einander im Notfall zu helfen. Das Übereinkommen setzt sich außerdem für die Stärkung der einzelstaatlichen Umsetzungsverfahren und die Entwicklung von Mechanismen für die internationale gesetzliche Zusammenarbeit bei Ermittlungen und der Strafverfolgung ein. Der Europarat arbeitet zurzeit an der Fertigstellung eines Zweiten Protokolls zum Übereinkommen über Computerkriminalität, das auch terroristische Aktivitäten abdecken soll. Vom Europarat nicht

offiziell bestätigten Medienberichten zufolge könnte das Protokoll die Grenzen bei der Verschlüsselungstechnologie weiter hinausschieben, die Code-Breaking-Bemühungen der Mitgliedstaaten koordinieren und die elektronische Überwachung von dem Terrorismus nahe stehenden Personen ausweiten.

76. Anstrengungen zur Förderung der internationalen Zusammenarbeit bei Cyberattacken und zur genaueren Untersuchung derartiger Vorgänge können zu einem weiter reichenden Konsens über das wahre Ausmaß der Bedrohung beitragen. Im gegenwärtigen Stadium sehen viele Staaten die Ausarbeitung eines Vertrages zur Lenkung der staatlichen Bemühungen zur Bekämpfung der Computerkriminalität nicht als sonderlich zweckmäßig an, da dies einen Eingriff in Bereiche des Völkerrechts bedeuten könnte, die unmittelbar mit ihren eigenen Aktivitäten zur Informationsbeschaffung zusammenhängen. Vor allem die Vereinigten Staaten scheinen sehr skeptisch zu sein: In einem Dokument des US-Verteidigungsministeriums hieß es: „Gegenwärtig scheint kaum geklärt zu sein, wie ein solches Übereinkommen funktionieren soll und wie es einen sinnvollen Beitrag zur Informationssicherung und zum Schutz entscheidender Infrastruktureinrichtungen leisten könnte."

Die NATO hat darauf hingewiesen, dass der Prager Gipfel auch zu einer spezifischen Initiative in Bezug auf die Cyberverteidigung führen könnte. Dazu sollen Maßnahmen für einen besseren Schutz vor einer möglichen Ausschaltung lebenswichtiger Infrastruktureinrichtungen sowie von Informations- und Kommunikationssystemen der Allianz und der einzelnen Staaten gehören.

V. SCHLUSSFOLGERUNG

Die Anschläge vom 11. September ließen weltweit die feste Entschlossenheit entstehen, gegen den Terrorismus vorzugehen: Über 150 Staaten sind jetzt an den Bemühungen beteiligt, dem Terrorismus die Stirn zu bieten und mehr als 200 Nachrichten- und Sicherheitsdienste koordinieren gegenwärtig Maßnahmen zur Terrorismusbekämpfung. Auch wenn die Quelle der anschließenden Milzbrandanschläge in den Vereinigten Staaten noch nicht ermittelt werden konnte, haben diese doch plastisch die – materiellen wie psychischen – Verheerungen deutlich gemacht, die ein derartiger Anschlag zu verursachen vermag. Zweifellos sind Terrororganisationen wie Al-Qaida aktiv bemüht, biologische, chemische und radiologische Waffen für Terroranschläge zu erwerben. Anders gesagt: Es wird mittlerweile allgemein anerkannt, dass eine psychische Schwelle überschritten worden ist und die Staaten sich einer sehr realen Bedrohung durch einen denkbaren terroristischen Einsatz von Massenvernichtungswaffen gegenübersehen.

Im Hinblick auf generelle Antworten auf terroristische Bedrohungen durch Massenvernichtungswaffen oder ABC-Waffen sowie Strahlenwaffen (CBRN) weisen Experten ständig darauf hin, dass dieses Problem nicht mit einem einzelnen politischen Handlungsinstrument – einer einzigen „Wunderlösung" – bewältigt werden kann und dass es einer umfassenden, integrierten Politik bedarf. Michael Moodie, der Präsident des CBACI, erklärte dieses Jahr in einem Beitrag auf einem Rose-Roth-Seminar in Bratislava, die Frage der Abwehr des CBRN-Terrorismus lasse sich bewältigen, aber nicht in vollem Umfang einer Lösung zuführen. Zur Maximierung der Effektivität bei der Verringerung der Dimension dieses Problems setzt eine internationale Reaktion zuerst einmal ein integriertes transatlantisches Vorgehen voraus. Zu den Kooperationsfeldern zwischen den Vereinigten Staaten und Europa sollten gehören: die Strafverfolgung, der Austausch von Aufklärungsdaten, die Erarbeitung von Normen, vorbeugende Maßnahmen (durch Exportkontrollen und die Einschränkung des Zugangs zu gefährlichen Materialien), die nötige Abwehr mit einem entsprechenden Bereitschaftsgrad, eine Analyse der gewonnenen Erkenntnisse sowie Forschung und Entwicklung.

Auf dem Rose-Roth-Seminar in Bratislava regte Paul Schulte, der Direktor für Verbreitungs- und Rüstungskontrollfragen im britischen Verteidigungsministerium, eine Reihe ineinander greifender Maßnahmen an, die die NATO-Verbündeten als Antwort auf die Bedrohung durch den Bioterrorismus ergreifen könnten (wobei die meisten dieser Maßnahmen auch gegen andere MVW wirksam sein könnten). Er sprach von den sieben D's (im Englischen): Abbringen (*dissuasion*), Abrüstung (*disarmament*), Verwehren (*denial*), Zerschlagung (*disruption*), Abschreckung (*deterrence*), Erkennung (*detection*) und Verteidigung (*defence*). Die internationalen Akteure könnten bei der Nutzung der verschiedenen Maßnahmen unterschiedliche Wege gehen, doch müssten diese Reaktionen, wie Schulte betonte, mit großem Nachdruck betrieben werden. Ihr Berichterstatter möchte sich an den von Schulte vorgegebenen Rahmen anlehnen und zusammenfassend die verschiedenen Strategien darstellen, die erforderlich sein werden, um den in diesem Bericht analysierten Bedrohungen zu begegnen.

- **Abbringen**: Dazu gehören im Wesentlichen nichtmilitärische Versuche, Konflikte zu lösen, abzumildern oder ihnen „die Spitze zu nehmen", um so die Gefahr zu verringern, dass irgendjemand Biowaffen einsetzen will. Auch wenn ein solches Vorgehen langsam und schwierig wäre und Fanatiker nicht von ihrem Vorhaben abzubringen vermöchte, werden sich Maßnahmen wie Wirtschaftshilfe, Unterstützung und konstruktive Diplomatie als vernünftige und sogar moralisch notwendige Schritte erweisen, um die eigentlichen Ursachen des Terrorismus anzugehen.
- **Abrüstung**: Der Besitz oder die Anwendung von MVW muss weltweit zunehmend mit einem dauerhaften rechtlichen und moralischen Tabu belegt werden. Das mag sich nicht direkt auf den Terrorismus auswirken, doch je weniger MVW die Staaten besitzen, desto geringer ist die Gefahr, dass diese durch Diebstahl, Verlust oder bewusste Überlassung in die Hände von Terroristen geraten.

  Das mit dem NVV geschaffene System nuklearer Safeguards sollte ausgebaut werden. Russland und die Vereinigten Staaten sollten eine förmliche Vereinbarung über die Reduzierung taktischer Kernwaffen aushandeln.

  Die Zahl der Mitgliedstaaten des BWÜ sollte erhöht und die entsprechenden Verpflichtungen sollten verstärkt werden, auch wenn der nötige Konsens eine Einigung erschwert. Die gegenwärtige Lähmung beim BWÜ könnte durch andere Initiativen kompensiert werden, wie z.B. ein internationales Biosicherheitsübereinkommen zur Verhinderung des unbefugten Zugangs zu Krankheitserregern und zur Regelung des Handels mit Bakterienkulturen.

  Die OPCW sollte auf dem Wege über ein solideres Management, eine flexiblere Haushaltspraxis und größeren Nachdruck auf die Verifikation bei Verstößen (unter Einschluss unangemeldeter Inspektionen) gestärkt werden.

  Wir sollten nicht vergessen, dass im Irak die Glaubwürdigkeit des gesamten Abrüstungs-/Nichtverbreitungssystems auf dem Spiel steht. Die internationale Gemeinschaft sollte alle denkbaren Anstrengungen zugunsten des neuen Inspektionsregimes unternehmen, dass unter einem VN-Mandat beginnen soll.
- **Verwehren**: Der beste Weg, um Terroristen und ihren staatlichen Unterstützern die Materialien zu verweigern, verläuft über Exportkontrollregelungen wie die Australia Group. In dem Maße, wie die technologische Entwicklung weitergeht, müssen die bestehenden Kontrollen verstärkt werden. Der Transfer von für Chemie- und Biowaffen nutzbaren Informationen muss kontrolliert werden. So sollte insbesondere der Zugang zu genetischen Informationen über gefährliche Erreger beschränkt werden. Die Gebiete der chemischen und biotechnologischen Industrie/Forschung sollten in internationale Kontrollregime einbezogen werden.

  Zusätzlich zu den internationalen Exportkontrollen sollten konzertierte nationale Maßnahmen ergriffen werden, um die Bestimmungen über Biosicherheit (Personenschutz – *biosafety* – wie Schutz von Bevölkerung und Umwelt – *biosecurity*) zu verschärfen und die Effektivität der einzelstaatlichen Regelungen beständig zu steigern. Der physische Schutz vor extrem tödlichen Substanzen in Laboratorien oder Militäreinrichtungen, wo ihr Vorhandensein und ihre Verwendung bekannt und gesetzlich erlaubt sind, sollte verstärkt werden.

Alle internationalen (multilateralen und bilateralen) Initiativen zur Zerstörung, Zerlegung und Sicherung von Kernwaffen und Kernmaterial sollten, gerade auch in den Ländern der ehemaligen Sowjetunion, gestärkt werden. Anhaltende, intensivierte internationale polizeiliche Zusammenarbeit ist erforderlich, um der Bedrohung durch den Schmuggel von Kernmaterialien zu begegnen. Innovative Technologien könnten dazu beitragen, den Schutz, die Kontrolle und die Bilanzierung von Kernwaffen und Nuklearmaterialien an der jeweiligen Quelle zu verbessern. Das Übereinkommen über den physischen Schutz von Kernmaterialien sollte so geändert und erweitert werden, dass zivile Nuklearmaterialien während der Lagerung und Beförderung und in Kernenergieanlagen im Inland erfasst werden.

- **Zerschlagung**: Wir sollten bereit sein, energisch gegen Vorbereitungen für die verschiedensten terroristischen Akte mit massenhafter Todesfolge vorzugehen. Außerdem kann es bisweilen erforderlich sein, eine vorbeugend eingreifende starke internationale Polizeistreitmacht vorzuhalten und – in wenigen Fällen – militärisch einzugreifen. Wir sollten jedoch nicht vergessen, dass ein zu energisches Vorgehen der „*dissuasion*“ schaden könnte. Eine enge internationale Zusammenarbeit wäre für die Durchführung solcher Militäraktionen erforderlich.
  Wir müssen außerdem den unerlaubten Material- und Geldzufluss zugunsten von Terroristengruppen unterbrechen. Die Technik könnte bei diesen Maßnahmen mit Nachweisgeräten und Angriffswerkzeugen einige Hilfe leisten – insbesondere auf dem Gebiet der Informationstechnologie. Um einer Nutzung des Internets durch Terroristen entgegenzuwirken, sollten die Nachrichtendienste regelmäßig das Web im Auge behalten und Informationen austauschen. Wenn notwendig, sollten aktive Schritte, wie z.B. Gegenangriffe zur Ausschaltung oder Zerstörung von Ausrüstungen und Software, ergriffen werden.
- **Abschreckung**: Eine Abschreckung von Selbstmordattentätern könnte nur schwer durchzusetzen sein, was jedoch nicht für ihre Führungskader oder die politischen Führer von Unterstützerstaaten gelten würde. Eine Betonung der mit Sicherheit zu erwartenden negativen Folgen für diese auf allen Ebenen in den Terrorismus mit Massenvernichtungswaffen verwickelten Personen könnte die Abschreckung verbessern. So sollten Personen, die auf irgendeiner Ebene für Biowaffen verantwortlich sind, von allen Staaten als Kriegsverbrecher verfolgt werden. Das könnte entweder über ein internationales Übereinkommen oder eine Entscheidung des VN-Sicherheitsrats zur Kriminalisierung des Besitzes und Einsatzes von MVW erreicht werden.
- **Erkennung**: Auffinden und Ergreifung von Personen und Durchdringung von Terrornetzwerken, bevor diese zuschlagen und, wenn dies nicht ausreicht, Ermittlung und Nachverfolgung der Herkunft von Materialien oder der Bewegungen Beteiligter. Ein internationaler Informationsaustausch und verbesserte Datenauswertung sollten zur frühzeitigen weltweiten Erkennung von Bewegungsmustern, Verbindungen und Verhaltensweisen beitragen.
  In allen diesen Bereichen können innovative Technologien wirklich weiterhelfen, auch wenn die Rolle der Technik bei der Aufklärungsarbeit nicht überbewertet werden sollte. Um den Nachrichtendiensten und den Strafverfolgern zu helfen, sollte der Aufbau einer laufend aktualisierten Datenbank über Terrorgruppen und terroristische Anschläge (insbesondere mit MVW) und die Erweiterung der Fähigkeiten der Weltgesundheitsorganisation (WHO) zur Überwachung weltweiter Entwicklungstendenzen bei Infektionskrankheiten und ungewöhnlichen Krankheitsausbrüchen berücksichtigt werden.
- **Verteidigung**: Die Abwehr von CBRN-Anschlägen hat sich seit dem 11. September verbessert, erfordert jedoch ein breiteres Tätigkeitsspektrum, darunter z.B. mehr Studien, mehr Schutzausrüstungen, die Entwicklung und Beschaffung mobiler Luftsensoren (die stationiert werden, wo die Bedrohung den Aufklärungsdaten zufolge am größten ist), um frühzeitig vor einem Angriff zu warnen.
  Die möglichst schnelle Erkennung bestimmter Kampfstofftypen ist für eine erfolgreiche medizinische Behandlung von entscheidender Bedeutung. Ebenso sind die Schulung, die Notfallplanung und die Einweisung einer ausreichenden Zahl von Rettungskräften und Medizinern in die Erkennung ungewöhnlicher Substanzen und neuartiger Krankheitsbilder entscheidende Voraussetzungen.

Ansteckende Krankheitserreger erfordern eine flexible, landesweit einheitliche Reaktion und z.B. auch die Anwendung öffentlicher Informationsstrategien, die überzeugend vor eigenmächtiger Flucht bei einem Anschlag warnen und über die Art des Anschlags informieren, Hinweise zu einer möglichst geringen Gefährdung geben sowie Behandlungs- und Beratungsstellen nennen.

Außerdem könnten Vorkehrungen für eine schnelle und wirksame internationale Hilfe getroffen werden, um zu verhindern, dass die einzelstaatlichen Abwehr- und Behandlungskapazitäten überfordert werden. Dabei sollten Regelungen innerhalb des Bündnisses den Vorrang haben.

Es sollten politische Schritte zum Schutz der nationalen Infrastruktur unternommen werden. Die Strategie der USA ist ein gutes Beispiel, doch sind noch Verbesserungen möglich, insbesondere durch verstärkte Verwendung leistungsfähiger Verschlüsselungs- und elektronischer Tarnmethoden. Passive Abwehrverfahren sollten mit aktiven Vorgehensweisen kombiniert werden, so z.B. bei Techniken zum Aufspüren und Zurückschlagen von Angreifern oder zur Ausschaltung ihrer Ausrüstungen.

77. Letztlich können wirksame Maßnahmen gegen Terroristen, die chemische oder biologische Waffen, „schmutzige“ Bomben oder Nuklearwaffen einsetzen sowie gegen Cyberattacken unmöglich ganz allein von einem einzelnen Staat durchgeführt werden. Wie Jayantha Dhanapala, der VN-Untergeneralsekretär für Abrüstungsfragen, vor kurzem hervorhob, „(kann) kein einzelnes Land ... alle weltweiten Exporte kontrollieren, den gesamten Technologietransfer überwachen oder die Einhaltung aller gesetzlichen Verpflichtungen durchsetzen.“ Materialien wie Plutonium, hoch angereichertes Uran und viele Stämme tödlicher Bakterien sowie Toxine sind „von Hause aus gefährlich“. Ihre Herstellung, ihre Lagerung und ihr Transport sind gefährlich, und das gilt sogar für ihre Verwendung für offensichtlich friedliche Zwecke. Darüber hinaus entstehen, wie der vorliegende Bericht zu verdeutlichen versucht, durch die schnellen Fortschritte in Wissenschaft und Technik – gerade auch in der Biotechnologie und der Informationstechnik – sowie deren schnelle Verbreitung in einer global vernetzten Welt neue Gefährdungspotenziale. Auch der mächtigste Staat kann nicht darauf hoffen, mit diesen Bedrohungen im Alleingang fertig zu werden. Darum erscheint ein nachdrückliches multilaterales Vorgehen als einziger sinnvoller Weg, Ihr Berichterstatter ist überzeugt, dass eine Organisation wie die Parlamentarische Versammlung der NATO sich bei ihrer Arbeit mit Abgeordneten von beiden Seiten des Atlantiks weiterhin für ein solches Vorgehen einsetzen sollte.

_____