

Protokoll zum Fachworkshop:

Dual-Use, Vertraulichkeit, Geheimnis. Grenzen der offenen Wissenschaft in der Sicherheitsforschung?

Veranstalter: Fachdialog Sicherheitsforschung

Datum: Freitag, 23. November 2012

Ort: Das Haus der Patriotischen Gesellschaft, Hamburg

Fragen zum Themenkomplex Dual-Use und nach möglichen Grenzen einer offenen wissenschaftlichen Kommunikation gewinnen in immer mehr Forschungsbereichen an Bedeutung. Prominentes Beispiel für solche Fragen sind die jüngsten Diskussionen um wissenschaftliche Veröffentlichungen zum H5N1-Virus. Auch im Rahmen des Forschungsprogramms für die zivile Sicherheit stellen sich solche Fragen für die Kommunikation einzelner Forschungsergebnisse. Das Forschungsprogramm selbst sieht sich immer wieder mit kritischen Fragen zur Abgrenzung von militärischer Forschung konfrontiert. Von Seiten des BMBF gibt es ein klares Bekenntnis zum zivilen, und damit: nicht-militärischen, Charakter des Programms. Aber auch klare programmatische Aussagen lassen Fragen offen. Zum einen etwa stellt sich die Frage, wo in punkto Kontrollformen Abgrenzungen von Zielen und Vorstellungen militärischer Aufklärung gezogen werden. So wurde der Sicherheitsforschung der EU mit durchaus nachvollziehbaren Argumentationen vorgeworfen, dass sie mit Projekten wie INDECT militärische Logiken, Denk- und Handlungsmodelle in die Gesellschaft hineinträgt, die geeignet sind, die demokratischen Grundlagen einer liberalen Demokratie zu gefährden. Umgekehrt stellt sich die Frage, inwiefern Ergebnisse ziviler Sicherheitsforschung auch militärisch nutzbar sind – und inwiefern dies ein Problem sein könnte. Nicht ohne Grund ist auf parlamentarischer Ebene, in den Medien sowie in den Hochschulen eine intensivierete Auseinandersetzung mit der Dual-Use-Problematik zu verzeichnen. Und Anfang November 2012 fand im Deutschen Bundestag ein öffentliches Fachgespräch zum Thema „*Umgang mit sicherheitsrelevanten Forschungsergebnissen*“ statt, in dem auch Vertreter der großen deutschen Forschungsorganisationen gehört wurden.

Was genau bedeutet der Begriff ‚Dual-Use‘? Wie ist der Begriff rechtlich, spezifisch im Außen- und Wirtschaftsrecht, gefasst, mit welchen Bestimmungen ist er dort verbunden? Wie ist Dual-Use ethisch zu bewerten? Ist jede Form der Mehrfachverwendung bedenklich oder kann diese in bestimmten Fällen auch wünschenswert sein (nachhaltige Entwicklung, Ressourceneffizienz)? Was bedeutet die Zunahme von missbräuchlichen Verwendungsmöglichkeiten von Forschungsergebnissen für die wissenschaftliche Forschungs- und Veröffentlichungspraxis? Wie viel externe Kontrolle ist für die Wissenschaft ggf. akzeptabel, welche Rolle können Mechanismen der Selbstkontrolle spielen? Diese und weitere Fragen wurden im Rahmen des Fachworkshops „*Dual-Use, Vertraulichkeit, Geheimnis. Grenzen der offenen Wissenschaft in der Sicherheitsforschung?*“ diskutiert, der am 23. November 2012 in Hamburg stattfand. Für die vom Projektteam des Fachdialog Sicherheitsforschung organisierte und konzipierte Veranstaltung konnten eine Reihe von anerkannten Expertinnen und Experten aus unterschiedlichen Forschungsbereichen, Institutionen und der behördlichen Praxis gewonnen werden. Ziel des Workshops

gefördert von



war es, zentrale Aspekte des sehr breiten Themenkomplexes aus unterschiedlicher Perspektive zu beleuchten, den Dialog über unterschiedliche Positionen, Problemlagen, über Forschungs- und Handlungsbedarf und mögliche Umgangsformen mit Problemen aufzunehmen.

Nach den einleitenden Grußworten von **Peter Zoche** (Fachdialog Sicherheitsforschung) skizzierte **Wolf Junker** (BMBF) zentrale Eckdaten des Forschungsprogramms für die zivile Sicherheit und lud die Anwesenden zur Diskussion der skizzierten Fragestellungen zur Dual-Use-Thematik ein.

Der Vortrag von **Martin Kahl** und **Oliver Meier** vom Institut für Friedensforschung und Sicherheitspolitik (IFSH) der Uni Hamburg widmete sich der Frage, welche Dual-Use-Probleme die zivile Sicherheitsforschung aufwirft und welche politischen, rechtlichen und anderen Herausforderungen sich damit ergeben. Den Ausgangspunkt bildete die Unterscheidung von zwei Dual-Use-Begriffen: (1) Gefahr des Missbrauchs legitimer Forschungsergebnisse, (2) Verwendung ziviler Forschungsergebnisse für militärische Zwecke („legale Doppelnutzung“). Die Gefahr der missbräuchlichen Verwendung habe aufgrund verschiedener Entwicklungen eine neue Qualität gewonnen. Angesichts der sich daraus ergebenden Problemlagen sei eine intensive Diskussion und die Entwicklung neuer Bewertungs- und Kontrollinstrumente erforderlich. Die von außen an das Sicherheitsforschungsprogramm herangetragenen Kritikpunkte – so ihre Analyse – fokussierten v.a. auf Dual-Use-Optionen im Sinne einer legalen Doppelnutzung von, dem Anspruch nach, dezidiert für zivile Anwendungen entwickelten Technologien. Da eine klare, prinzipielle Trennung von zivilen und militärischen Technologien immer weniger möglich sei, müssten v.a. die jeweiligen Anwendungskontexte in den Blick genommen werden. Abschließend skizzierten Meier und Kahl Handlungsbedarfe und mögliche Ansatzpunkte zum Umgang mit der Dual-Use-Problematik im Bereich der zivilen Sicherheitsforschung (s. Anhang). Die Verantwortung liege dabei nicht allein bei den Mittelempfängern sondern auch beim Geldgeber/ der Politik (Bewusstsein schaffen; Auswahl/ Förderung von Forschungsprojekten etc.). Ziel sollte es sein, alle Stakeholder in die Diskussion und Bewertung von Dual-Use-Aspekten einzubinden („technology governance“). Transparenz sollte die Regel, Geheimhaltung die Ausnahme sein.

Uwe Wiemken, Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen INT in Euskirchen, beleuchtete vor dem Hintergrund langjähriger Erfahrung mit Technikforschung auch im militärischen Bereich die Rolle der Forschung bei Dual-Use-Technologien aus historischer, ethischer und pragmatischer Perspektive. Spätestens seit den 1980er Jahren sei eine stetige Dynamisierung ziviler High-Tech-Forschung zu verzeichnen, mit der die Dual-Use-Problematik und eine Fülle von Fragen virulent geworden seien: Ist Grundlagenforschung per se unbedenklich? Ist militärischer Gebrauch von Forschungsergebnissen automatisch Missbrauch? Bereits in den 1990er Jahren wurde im Rahmen eines TAB-Projektes zum Thema präventive Rüstungskontrolle die grundlegende Ambivalenz von Technologien deutlich: Eine klare Differenzierung von Grundlagen- und Anwendungsforschung ist ebenso wenig möglich wie eine eindeutige Trennung zivil vs. militärisch. Angesichts von veränderten Kriegsbildern, neuen Konfliktformen und Bedrohungsszenarien bestehe gegenwärtig großer Diskussions- und Verständigungsbedarf, z.T. sei eine Reformulierung grundlegender Fragestellungen erforderlich. Wiemken forderte die Schaffung von Rahmenbedingungen für die Aufnahme eines gesamtgesellschaftlichen Diskurses, die Entwicklung einer „demokratischen Streitkultur“ zum Thema „Sicherheit und Verteidigung“. Neben einer Auseinandersetzung mit Optionen und Problemen, die durch technologische Dynamiken entstehen, sollten auch Auswirkungen des gesamtgesellschaftlichen Wandels in den Blick genommen werden.

GEFÖRDERT VON

Am Beispiel von Bilddaten ziviler Satelliten- und Luftbildtechnologie stellte **Stefan Voigt** vom Deutschen Zentrum für Luft- und Raumfahrt (Oberpfaffenhofen) Überlegungen zur Frage der Geheimhaltung von sensitiven Informationen an, die von immer leistungsfähigeren Erdbeobachtungstechniken in immer kürzerer Zeit verfügbar gemacht werden. Das DLR entwickelt für den zivilen Bereich der Katastrophenhilfe und für polizeiliche Aufgaben Analysemethoden und operative Unterstützungsansätze (humanitäre Hilfe, Lageerkundungen bei Katastrophen, Unterstützung des zivilen Krisenmanagements etc.). Diese stießen bisweilen auch auf militärischer Seite auf Interesse. Für Drohnentechnologien sei eine geradezu explosionsartige Ausweitung der Forschungsaktivitäten und Anwendungen zu verzeichnen. In den USA soll ein Gesetz zur Anwendung dieser Systeme im Luftraum bis 2014 entstehen, in Deutschland wird die Satellitennutzung durch das Satellitendatensicherheitsgesetz (SatDSiG) geregelt. Einen internationalen Rechtsrahmen gibt es bisher nicht. Mit Blick auf die Frage der Geheimhaltung von sensitiven Forschungsergebnissen/ Informationen plädierte Voigt für eine Differenzierung von a) öffentlicher Forschungsförderung, b) spezifischer Forschungsförderung (Auftragsforschung), c) im Wissenschaftsumfeld für operative Fragestellungen erstellten, sensitiven Informationen. In wissenschaftlichen Kontexten erstellte Forschungsergebnisse sollten prinzipiell offen verfügbar sein. In bestimmten Fällen, wie etwa dem operativen Einsatz der Fernerkundung für die Gefahrenabwehr oder auch im Kontext von NGOs, die humanitäre Hilfe leisten, könne jedoch Vertraulichkeit notwendig bzw. Geheimhaltung geboten sein (ggf. fallbezogene Prüfung und Entscheidung über Geheimschutz). Die Forschungs- und Entwicklungsdynamik im Bereich Fernerkundung sei sehr hoch, die Diskussion darüber jedoch bislang nur schwach ausgeprägt.

Die **Diskussion** zu den Beiträgen konzentrierte sich auf die drei folgenden Themen:

1) *Begrifflichkeiten: Dual-Use oder Multi-Use?*: Ist das unscharfe Konzept „Dual-Use“ überhaupt (noch) geeignet, um sehr heterogene Problembereiche und -konstellationen adäquat zu adressieren? Reichen die bislang diskutierten Differenzierungen (zivil vs. militärisch, Gebrauch vs. Missbrauch) aus? Muss man angesichts einer Vielzahl von Übergangsfeldern, Graubereichen zwischen militärischem und zivilem Bereich (Diktatorische Regime, Organisierte Kriminalität, Terrorismus etc.) u.U. eine sehr viel weiter zu fassende „Multi-Use“-Problematik in den Blick nehmen? Zur Präzisierung der Terminologie bestehe ein genereller Forschungsbedarf. Nicht zuletzt, um daraus Hinweise zur Frage des Umgangs mit Forschungsergebnissen (Transparenz vs. Geheimhaltung; Frage der Zweckbindung von verfügbaren Daten etc.), zur Entwicklung von Beurteilungskriterien, sowie zur (Weiter-)Entwicklung von Verhaltenskodizes ableiten zu können.

2) *Ansatzpunkte im Umgang mit der Dual-Use-Problematik in der zivilen Sicherheitsforschung*: Wer trägt mit Blick auf die Beurteilung von bzw. den Umgang mit der Dual-Use- oder auch Multi-Use-Problematik Verantwortung? Wie kann und soll diese Verantwortung konkret wahrgenommen werden? Projektnehmer und die Politik stünden gemeinsam in der Pflicht, Mechanismen für eine verantwortungsvolle Praxis (Forschungsförderung, -durchführung, Verwertung von Forschungsergebnissen) zu entwickeln und durchzusetzen. Missbrauchsmöglichkeiten spielen in immer mehr Forschungsbereichen eine Rolle. Um diese Problematik in den Griff zu bekommen und Missbrauch zu verhindern, sei es notwendig, alle Akteure einzubinden und bspw. im Rahmen eines gemeinsamen Forums an einen Tisch zu bekommen (Bsp. internationale Normenbildung). Erste, dringend erforderliche Schritte sollten die Schaffung bzw. Schärfung des Problembewusstseins aller Beteiligten (nicht-intendierte Effekte, strukturelle Probleme etc.) und der Eintritt in eine breite Diskussion zum Selbstverständnis der zivilen Sicherheitsforschung sein: Was heißt „zivile“ Sicherheitsforschung und wie lässt sich dieser Anspruch umsetzen? Weiterer

GEFÖRDERT VON

Handlungsbedarf wurde in der Entwicklung von Beurteilungskriterien zu Dual-Use/ Multi-Use und der (Weiter-)Entwicklung und Bekanntmachung von Verhaltenskodizes im Bereich der Forschung gesehen.

3) *Geheimhaltung(sfähigkeit) von Forschungsergebnissen*: Welche Rolle spielt die Frage der Geheimhaltung mit Blick auf die Forschungsergebnisse des zivilen Sicherheitsforschungsprogramms? Prinzipiell gilt: Die Ergebnisse aus BMBF-geförderten Projekten müssen veröffentlicht werden, sofern sie nicht Gegenstand der Geheimhaltung sind (was bislang nicht der Fall war). Im Anschluss an den Vortrag von Stefan Voigt wurde die Frage der Notwendigkeit und ggf. vertraglichen Regelung von Vertraulichkeit bzw. Geheimhaltung diskutiert: Ist die Differenzierung zwischen (offener) Forschung und (potentiell unter Geheimschutz zu stellender) operativer Anwendung sinnvoll zu treffen? Da die Frage der operativen Anwendung der (Forschungs-)Arbeit des DLR in jüngerer Zeit immer relevanter werde – so seine Antwort –, und die Unterstützungsanfragen von unterschiedlicher Seite (Katastrophenschutz, Polizei) zunehmen, arbeite man gegenwärtig gemeinsam mit dem BMI an der Erstellung eines formalen Rahmens, um klare Regelungen für die Belange des Katastrophenschutzes, für Geheimhaltungsfragen etc. zu implementieren. Angesichts eines stark wachsenden globalen Marktes für zivile, kommerzielle Geodaten gewinnen darüber hinaus auch Fragen nach Mechanismen zum Schutz geistigen Eigentums, Schutzrechten etc. zunehmend an Bedeutung.

Weitergehend wurde die Frage gestellt, ob Geheimhaltung (längerfristig) überhaupt möglich und sinnvoll sei? Muss man sich der Realität stellen, dass Wissen, Informationen sich nicht geheim halten lassen und über kurz oder lang in interessierte Hände gelangen oder öffentlich verfügbar werden? Bislang gebe es kein Bsp. dafür, dass der Ansatz „security by obscurity“ tatsächlich erfolgreich gewesen sei. Welche (alternativen) Mechanismen lassen sich entwickeln, um damit umzugehen? Wenn und weil vollständige Geheimhaltung auf Dauer nicht möglich ist, so die allgemeine Einschätzung, dienen alle Kontrollen und Regulierungsversuche primär der Abschreckung und der Verzögerung, der Verlangsamung (Verbreitung, Zugänglichkeit). Auch wenn gänzliche Geheimhaltung kaum möglich sei, könne ein solcher Zeitgewinn durchaus einen Sicherheitsgewinn bedeuten.

Holger Beutel vom Bundesamt für Wirtschaft und Ausfuhrkontrolle informierte in seinem Vortrag „*Wissenschaft und Proliferation – Die Beschränkung des Technologietransfers aus Außen- und sicherheitspolitischen Erwägungen*“ über die behördliche Kontrolle von Dual-Use-Gütern. Die gesetzlichen Rahmenbedingungen zur Kontrolle von Dual-Use-Gütern, so betonte er, gelten nicht nur für die Industrie, sondern auch für die wissenschaftliche Forschung. Gegenstand dieser Kontrollen sind alle Dual-Use-Güter, d.h. Waren, Software und Technologie, die im europäischen Rahmen in Listenform „technisch objektiv beschrieben“ sind und sowohl zivil als auch militärisch verwendet werden können. Der ursprünglich eng militärisch gefasste Dual-Use-Begriff habe sich deutlich ausgeweitet (auch Praktiken wie Folter, die Ausspähung von Oppositionellen oder Menschenrechtsverletzungen werden inzwischen darunter gefasst), daher seien Überwachungstechnologien für das BAFA ein hochaktuelles Thema. Terroristischen Gefährdungen allerdings sei durch Güterkontrolle kaum etwas entgegenzusetzen, diesen versuche man primär mit Finanzkontrollen zu begegnen („Verbot der Bereitstellung wirtschaftlicher Ressourcen“). Die Kontrollen der BAFA konzentrieren sich auf folgende Aktivitäten: a) Güterverkehr, b) elektronische Kommunikation/Bereitstellung, c) Vermittlungsgeschäfte d) technische Dienstleistungen, e) (mündliche) Wissensvermittlung, f) Bereitstellungsverbote. Ausgenommen von diesen Kontrollen ist ausschließlich der Bereich der Grundlagenforschung. Sobald wissenschaftliche Forschungsvorhaben über diesen definierten Bereich hinausgehen, müssen gesetz-

GEFÖRDERT VON

liche Bestimmungen zum Außenwirtschaftsverkehr beachtet, Genehmigungen eingeholt werden, Regelungen zu Dienstreisen und Kongressen, für Versand und Mitnahme von Produkten ins Ausland, für grenzüberschreitende elektronische Kommunikation, für Gastwissenschaftler etc. festgelegt werden – andernfalls komme es unweigerlich zu Rechtsverstößen, bei denen empfindliche Strafen drohen. Da das Bewusstsein für die Problematik in der Industrie deutlich höher ausgeprägt sei als in der wissenschaftlichen Forschung (unter jährlich 50.000 Anfragen an das BFA waren nur 40 aus dem Bereich der Wissenschaften), versuche das BAFA mit unterschiedlichen Maßnahmen zu informieren und für die Thematik zu sensibilisieren.

In der **Diskussion** wurde zum einen deutlich, dass die vorgestellten gesetzlichen Regelungen in der Wissenschaft nur sehr begrenzt bekannt sind, also erheblicher Aufklärungsbedarf besteht. Zum anderen liefen die Einschätzungen aber auch darauf hinaus, dass Regelungen zum Teil problematisch und nur schwierig umsetzbar seien¹. So sei angesichts einer zunehmenden Dynamisierung der Wissenschaft eine saubere Trennung von Grundlagenforschung und anwendungsorientierte Forschung nicht mehr möglich. Unklar sei auch, wie Wissenschaftler in Bereichen, in denen (nahezu) alle Arbeiten grundsätzlich im Bereich „Multi-Use“ angesiedelt sind (z.B. Informatik), konkret mit den genannten Regelungen umgehen sollen. De facto existierten zahlreiche Grauzonen, in denen letztlich die Verantwortung und Urteilsfähigkeit der Wissenschaftler selbst gefragt sei; Regeln könnten hier bestenfalls als Orientierung dienen. Zu beachten sei auch, dass mit der Ausweitung der Dual-Use-Problematik auf Menschenrechtsverletzungen, sich verstärkt die Frage nach Missbrauchsmöglichkeiten geistes- und sozialwissenschaftlicher Forschung (Psychologie, Kommunikationswissenschaften, Ethnologie etc.) ergebe. Thematisiert wurden darüber hinaus künftige Herausforderungen für das BAFA. Mit der immensen Dynamik in der Technologieentwicklung, die eine kontinuierliche, schnelle Anpassung von Kontrollmechanismen erfordere, könnten die Kontrollbehörden faktisch nicht Schritt halten. Vor allem die Frage nach denkbaren Missbrauchspotentialen, Aufgabe der technischen Experten der BAFA, sei nur schwer in den Griff zu bekommen.

Die genannten Probleme dürften sich in Zukunft weiter verschärfen: Werden Ausfuhrkontrollen für Güter künftig von realen Entwicklungen (zunehmende Zentralität von Wissen / Know-how etc.; "de-skilling", d.h. auch Laien können komplexe Technologien nutzen, so etwa im Bereich der synthetischen Biologie überholt? Was bedeuten die Regelungen für die gewünschte Intensivierung von internationalen Forschungs Kooperationen? Welche Projektstrukturen, Verhaltenskodizes für Forschungsprojekte werden damit u.U. notwendig? Herr Beutel betonte, dass „outreach to academia“ gegenwärtig eines der zentralen Themen im Bereich der Ausfuhrkontrolle sei, für das es jedoch keine Patentrezepte gebe. Erste Aktivitäten zielten v.a. auf eine stärkere Sensibilisierung für Problemlagen. Generell würden immer neue Themenbereiche missbrauchsrelevant und damit auch kontrollrelevant. Das Thema Know-how-Transfer (z.B. kaum kontrollierbare Verbreitung durch neue Medien) würde immer dringlicher und zugleich schwieriger. In bestimmten Bereichen werde staatliche Überwachung perspektivisch nicht mehr

¹ Dies liegt u.a. an grundsätzlich verschiedenen Perspektiven bzw. Präferenzen der Systeme (Natur-)Wissenschaft (schnelle Innovation: Behandlung einer geringen Zahl jeweils neuartiger Fälle durch fachliche Spezialisten bzw. juristische Laien; schnelle, nur in Bezug auf „Korrektheit“ kontrollierte Verbreitung von Wissen; „Multi-Use“ ist prima facie gut) und Verwaltung (standardisierte, längerlebige Verfahren; Behandlung einer großen Zahl ähnlicher Fälle durch fachliche Laien bzw. juristische Spezialisten; Kontrolle der Verbreitung von Wissen (vor allem, wenn dieses „korrekt“ ist); „Multi-Use“ ist prima facie problematisch).

greifen, zudem müsse die Forschungsfreiheit gewahrt bleiben. Künftig werde es primär darum gehen, durch Aufklärung und Überzeugung sowie und durch Abschreckung und Strafe ein gewisses compliance-Bewusstsein zu schaffen. Die Diskussion um Entwicklung und Etablierung eines code of ethics/ code of conduct für die Wissenschaft sei in Gang gesetzt, aber noch nicht umsetzungsfähig. Diskussion und Austausch zwischen Kontrollbehörden und Wissenschaft seien dringend erforderlich, fänden aber bislang weltweit nur in relativ geringem Ausmaß statt.

„Was ist gefährliches Wissen? Und wie gehen wir damit um?“ lauteten die Leitfragen des Vortrags von **Iris Hunger**, die am Robert-Koch-Institut in Berlin zu biologischen Gefahren arbeitet. Im Bereich „Biosecurity“ sei nicht Technologie oder Material sondern Wissen das entscheidende Problem. Die Bewertung der Nutzung dieses Wissens (friedliche vs. nicht-friedliche Zwecke) müsse bei der Betrachtung von Kontexten und Intentionen ansetzen. Bislang gebe es einen erregerbasierten und einen ergebnisbasierten Definitionsansatz für „besonders gefährliches Wissen“ („dual use of concern“) – beide seien insofern unbefriedigend, als sie primär auf Schadenshöhen fokussierten ohne dabei Eintrittswahrscheinlichkeiten zu berücksichtigen. Zur Definition und den Bewertungskriterien für „gefährliches Wissen“ bestehe weiterer Diskussions- und Forschungsbedarf. In noch größerem Maße gelte dies für grundlegende Fragen im Umgang mit besonders gefährlichem Wissen. Der Begriff Biosecurity bezeichne inzwischen ganz allgemein den Schutz der Bevölkerung vor der Verbreitung von Erregern (durch Terrorismus, Unfälle oder außergewöhnliche natürliche Ursachen). Die konkrete Umsetzung dieses Anspruchs sei jedoch völlig offen. Diskutiert würden v.a. Regeln für wissenschaftliches Arbeiten. Zu einigen Maßnahmen (s. Anhang) bestehe weitgehend Einigkeit, es mangle jedoch an der Umsetzung. Die Freiheit der Forschung, so Hunger, ist ein höchst schützenswertes Gut. Forschung in missbrauchsgefährdeten Bereichen sei notwendig, sollte aber rein defensiv ausgerichtet sein. Forschungsergebnisse müssten publiziert werden. Aber zugleich müssten im Bereich der hoch missbrauchsrelevanten Forschung auf unterschiedlichen Ebenen Prüfungs- und Kontrollmechanismen implementiert werden. Wissenschaftlerinnen und Wissenschaftler, unterstrich Hunger, tragen Verantwortung. Es seien aber verschiedene Maßnahmen notwendig, um sie in die Lage zu versetzen, dieser Verantwortung tatsächlich gerecht zu werden (s. Anhang).

Im Zentrum der **Diskussion** standen die folgenden Themen:

1) *Forschungsbedarf zu „gefährlichem Wissen“ (Definition, Bewertungskriterien):* Es wurde angeregt, die Forschung zur Definition von „gefährlichem Wissen“ und zu Ansatzpunkten für Regelungsmechanismen in Richtung einer stärkeren Differenzierung von verschiedenen, u.U. in unterschiedlichem Maße missbrauchsrelevanten und kontrollbedürftigen Wissensarten (z.B. Strukturwissen, Prozesswissen, Wirkungswissen) voranzutreiben. Das BAFA unterscheidet Herrn Beutel zufolge bei grenzüberschreitendem Wissenstransfer drei – unterschiedlich stark kontrollierte – Wissensarten: Entwicklung, Herstellung und Verwendung.

2) *Verantwortung der Wissenschaft: Akademische Aus- und Weiterbildung, Verhaltenskodizes etc.:* Wie kann das Bewusstsein, die Sensibilität für die Verantwortung der Wissenschaftlerinnen und Wissenschaftler gestärkt werden? Für den Bereich der akademischen Aus- und Weiterbildung wird insgesamt erheblicher Handlungsbedarf konstatiert. Auf hochschul- bzw. wissenschaftspolitischer Ebene mangle es häufig an Problembewusstsein sowie an Entschlossenheit zur Umsetzung einer angemessenen akademischen Ausbildung zu Verantwortungsbewusstsein und Selbstreflexion. Die Verantwortung liege v.a. bei den Lehrenden, die ihrerseits besser geschult werden müssten. Curricula sollten überarbeitet und vollkommen neue, konkrete Lehrkon-

zepte und Vermittlungsansätze entwickelt werden (Rollenspiele, e-learning-tools etc.); die Konzeptionierung erfordert aber Zeit und Geld.

Im Bereich der Forschung sei „awareness-raising“, die Steigerung von Aufmerksamkeit, ebenfalls von zentraler Bedeutung. Vorhandene Verhaltenskodizes seien häufig nicht (ausreichend) bekannt. Forschungsgruppenleitern komme mit Blick auf die Sensibilisierung der Mitarbeiter/ Nachwuchswissenschaftler eine zentrale Rolle zu (Verhaltenskodizes bekannt machen, Diskussionen anregen etc.). Der Vorschlag, an jedem Institut „Dual-Use-Beauftragte“ oder auch „compliance-Beauftragte“ (vgl. „Code of conduct“ der MPG) zu ernennen, wird kontrovers diskutiert. Die Durchführung regelmäßiger Schulungen, Belehrungen, mit denen alle Mitarbeiter erreicht werden, sei sinnvoll. Zugleich wird vor weiterem administrativem Ballast oder institutsinternen Ethik-Kommissionen, vor denen sich Kollegen rechtfertigen müssen, gewarnt. Angesichts einer zunehmenden Dynamisierung der Forschung sollten Diskussionen kontinuierlich geführt, vorhandene Regelungen regelmäßig überprüft und ggf. angepasst werden.

3) *Verhaltenskodizes und/oder Gesetz – Prävention und/oder Sanktionierung?* Reichen moralische Appelle, Selbstverpflichtungen, Verhaltenskodizes aus oder braucht man durchsetzbare Gesetze? Insgesamt wird für eine Kombination aus weichen und harten Regelungsmechanismen plädiert. Sanktionsdrohungen, das Setzen negativer Anreize, kodifizierte „rote Linien“ zu überschreiten, sei notwendig. Der primäre Fokus sollte indes nicht auf Sanktionierung sondern auf verfahrensgesteuerter Prävention liegen (konkrete Maßnahmen, Hilfsmittel entwickeln). Sanktionsvorschriften wirkten allenfalls indirekt präventiv, zudem sei eine Konkretisierung schwierig. Als möglicher Ansatz zur Prävention wird die Ausweitung der Selbstkontrolle durch Ethik-Kommissionen über den bisherigen Fokus auf „Forschung am Menschen“ hinaus vorgeschlagen. In den USA wurde für den Bereich „Biosecurity“ eine zentrale Kommission eingerichtet – möglicherweise könnte dies auch hier ein gangbarer Weg sein (ggf. sowohl security als auch safety-Aspekte berücksichtigen).

4) *Kontrolle vs. Forschungsfreiheit:* Inwieweit ist die Wissenschaft bereit, stärkere Verpflichtungen einzugehen? Wie viel Kontrolle ist mit der Forschungsfreiheit vereinbar? Können Regelungsansätze mit der Forschungsdynamik Schritt halten ohne sie zu sehr zu behindern? Forderungen nach intensivierter permanenter Kontrolle von außerhalb der Wissenschaft, die auch im Kontext der Anhörung im Deutschen Bundestag vorgebracht wurden, werden als problematisch bewertet. Erfahrungen im Bereich Datenschutz oder auch im Gentechnikrecht zeigten jedoch, dass Regulierungen durchaus funktionieren können, wenn Selbstverpflichtungen allein zu wenig Wirkung zeigen. Grundsätzlich verweise die Multi-Use-Problematik auf ein äußerst komplexes Themenfeld, in dem einfache Belehrungen nicht greifen, es keine einfachen Antworten geben könne. Als ein Bsp. wird der Bereich der synthetischen Biologie genannt. Zunehmend seien auch Laien in der Lage "do-it-yourself"-Biotechnologien zu nutzen. Vor diesem Hintergrund müsse man nicht allein über Bioterror sondern auch über "Bioerror" nachdenken (unbeabsichtigtes Freisetzen von Wirkstoffen, die nicht nur menschlich pathogen sind, sondern auch Umweltwirkungen hervorrufen könnten). Insgesamt habe man es mit hoch dynamischen Entwicklungen und einem sehr komplexen Diskursfeld zu tun. Angesichts dessen seien v.a. Diskussion, Aushandlung und Verständigung zwischen allen Akteuren notwendig. Die Wissenschaft selbst habe ein Interesse daran, dass die eigene Arbeit nicht missbraucht wird und das Vertrauen in die Wissenschaft erhalten bleibt. Es gelte deshalb, aktiv und glaubhaft Verantwortungsbewusstsein und verantwortungsvolles Handeln zu demonstrieren.

GEFÖRDERT VON

In der abschließenden **Podiumsdiskussion** zum Thema „*Forschungs- und Innovationsförderung: Dual-Use als Perspektive?*“ verdeutlichten die Statements der vier Diskutanden die immense Breite der Dual-Use-Thematik und möglicher Perspektiven auf die zivile Sicherheitsforschung. **Jutta Weber**, Philosophin, Medientheoretikerin und Technikforscherin an der Uni Paderborn plädierte dafür, stärker Fragen nach den soziokulturellen Auswirkungen von Sicherheitsforschung und -technologien und nach möglichen Kosten für die Demokratie in den Blick zu nehmen („Grenzen der Sicherheitsforschung“? bzw. „Grenzen von Sicherheitstechnologien in einer offenen Gesellschaft“?): Inwieweit werden militärische Logiken, strategische Konzepte, Denkmodelle über die zivile Sicherheitsforschung in den zivilen Bereich hineingetragen? Sind zivile Sicherheitsarchitekturen möglicherweise unangemessen ausgestaltet? Sind technikzentrierte Lösungen per se die besseren Lösungen zur Herstellung von Sicherheit? Eine immer umfassendere Überwachung der Bevölkerung könne zu einer Unterminierung von Grundrechten und demokratischen Prozessen in einer offenen Gesellschaft führen (Meinungsfreiheit, Versammlungsfreiheit). Mit Blick auf diese Fragen forderte Weber den Einstieg in eine qualifizierte öffentliche Debatte auf breiter demokratischer Basis. Ein möglicher Weg zur Demokratisierung von Entscheidungsprozessen seien Konsensus-Konferenzen.

Christoph Stroschein, Geschäftsführer der German European Security Association, rückte zunächst weniger die Probleme, als die Chancen von Dual-Use in den Vordergrund. Dem Statement von Weber hielt er entgegen, dass die Zivilgesellschaft durchaus vom Militär lernen könne: die zentrale Herausforderung und Chance des zivilen Sicherheitsforschungsprogramms sei es, die systemische Komplexität der Gesellschaft zu erforschen und in den Griff zu bekommen (Verwundbarkeiten, Kaskadeneffekte). Die Diskussion um Dual-Use sei vielfach schädlich und ein Zeichen von Schwäche. Das zivile Sicherheitsforschungsprogramm sollte mit Selbstbewusstsein und eigener Autorität versehen werden. Eine weitere zentrale Aufgabe sei die Erhöhung des Selbstschutzes der Industrie („Rohstoff“ geistiges Eigentum). Mit Blick auf die Zentralität von Wissen forderte Stroschein ein verstärktes Nachdenken über den Selbstschutzbedarf der Forschung und warf die Frage nach neuen „Spielregeln der Forschung(sförderung)“ auf: Forschung, die öffentlich gefördert, finanziert, auf industrielle Umsetzung abziele, und das derart generierte Know-how dienen dem Erhalt und der Mehrung des Wohlstandes und sollten eine höhere Wertschätzung genießen. Sei vor diesem Hintergrund der Wunsch nach Schutz von Forschungsergebnissen nicht durchaus legitim? Die dritte zentrale Aufgabe laute, das Thema Kommunikationsfähigkeit der Forschung voranzutreiben, um Verständnis und gesellschaftliche Akzeptanz zu verbessern. Die Weiterentwicklung des Themas zivile Sicherheit hänge entscheidend von der Entwicklung der Fähigkeit zu angemessener, proaktiver Kommunikation zum Nutzen von Sicherheitstechnologien ab.

Stephan Lingner von der Europäischen Akademie zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen plädierte dafür, das Thema Dual-Use als sozial- und kulturwissenschaftlichen Forschungsgegenstand aufzugreifen (z.B. in Projektform). Zivile Sicherheitsforschung und Dual-Use sollten auch mit Blick auf mögliche Risiken der Installation von Sicherheitstechnologien/ -vorkehrungen reflektiert werden, damit diese sich nicht mangels Akzeptanz als "Investitionsruinen" herausstellten. Meta-Perspektiven auf die gesellschaftliche Wirkung von Sicherheitstechnologien seien unverzichtbar; es gelte, verschiedene Spannungsfelder auszuloten: 1) „objektive“ (messbare) Sicherheit vs. subjektive Unsicherheit, Besorgnis, Angst; 2) Sicherheit vs. Gewissheit; 3) Sicherheit und/oder Freiheit. Die Lebensrisiken, mit denen moderne Gesellschaften sich konfrontiert sehen, hätten sich weniger quantitativ als v.a. qualitativ verändert. Auf diese qualitative Dynamik, auf das veränderte Spektrum der Risiken müsse die zivile Sicherheitsforschung reagieren. Dazu gehöre auch, nicht allein in technische Sicherheitsfor-

GEFÖRDERT VON

schung, technische Lösungen zu investieren, sondern auch in präventive Lösungen zur Herbeiführung von systemischer Stabilität (z.B. indem Fragen nach Ursachen, nach Einflussfaktoren von Kriminalität, nach Radikalisierungsprozessen etc. aufgenommen werden). „Wir brauchen nicht mehr Sicherheit“, so das Fazit, „sondern wir brauchen womöglich eine andere Sicherheit“.

Moral, so unterstrich **Regina Ammicht Quinn**, die unter anderem den Forschungsschwerpunkt Sicherheitsethik an der Universität Tübingen leitet, ist nicht gleich Ethik und warnte vor einem sehr instrumentellen Verständnis von Ethik – etwa in Sinne einer „Moral-Polizei“. In Abgrenzung davon forderte sie: 1) Eine ethisch/ rechtsphilosophisch informierte Grundlegung der gesellschaftlichen Rahmenbedingungen; 2) Die Ausgestaltung dieser Rahmenbedingungen durch gesellschaftliche Diskurse dort, wo kritische Fragen auftauchen. Die Debatte um Dual-Use sei notwendig; sie helfe dem Forschungsprogramm und schade ihm nicht. 3) Plädierte sie dafür, die im Workshop offenkundig gewordene Komplexität der Dual-Use-Thematik (legaler Gebrauch vs. Missbrauch; friedliche vs. feindselige Absichten; legitime und sinnvolle Mehrfachverwendungen) beizubehalten und um eine weitere wichtige Perspektive zu ergänzen: den Transfer ziviler Technologien, zu zivilen Zwecken in Drittstaaten mit zweifelhafter Grundrechtssituation. Möglicherweise gebe es schlicht keine rein zivile Sicherheit, könnten „kodifizierte rote Linien“ sich als kaum haltbar erweisen – dies sollte dann aber allen Beteiligten bewusst sein. Im zivilen Forschungsprogramm, so Ammicht Quinn, müssten immer Einzelfallentscheidungen getroffen werden. Als Grundlage der Bewertung/Begutachtung schlug sie einige Kriterien mittlerer Reichweite („Klugheitsregeln“) vor (s. Anhang).

Die in den Statements, wie auch im Workshop generell aufgeworfenen Fragen wurden in der abschließenden Diskussion teils kontrovers diskutiert. Auch wenn nicht alle verhandelten Aspekte unmittelbar das Sicherheitsforschungsprogramm und geförderte Projekte betreffen, herrschte Übereinstimmung, dass die Reflexion zu Dual-/Multi-Use im Programm verstärkt berücksichtigt werden sollte. Dies gelte insbesondere für den auch rechtlich definierten Problembereich von potentiell missbräuchlicher Verwendung, wofür es noch zu wenig Aufmerksamkeit gebe.

Umstritten blieb hingegen, was dies für den Bereich legaler zivil-militärischer Zusammenarbeit bedeutet: Sollen Doppelverwendungen intendiert oder problematisiert werden? Kann der Import von militärischem Wissen in die zivile Sicherheitsforschung nützlich sein? Zumindest mit Blick auf das Problem von systemischen Risiken komplexer Systeme (Verwundbarkeit Kritischer Infrastrukturen etc.) wurde davor gewarnt, vom Militär die besten Lösungen für den Umgang mit systemischer Komplexität zu erwarten. Die Übertragung militärischen Denkens und militärischer Logiken (Command-and-control; top-down-Kommunikation etc.) auf die Gesellschaft sei vielmehr hoch problematisch, da ein solches Denken die Komplexität technologischer Lösungsansätze bzw. gesellschaftlicher Problemkonstellationen vollkommen unterschätze.

Deutlich wurde in der Diskussion auch, dass sich die Bewertung solcher Dual-/Multi-Use-Probleme nicht unabhängig von übergreifenden Fragen nach dem Sicherheitsverständnis und dem Sinn und Zweck von Sicherheitsforschung beantworten lassen. Insofern führte die Diskussion zu umfassenderen Fragen und Themen: Was ist eine adäquate Beschreibung von ‚Gesellschaft‘? Welche ‚Sicherheit‘ wollen wir? Und welches sind die geeigneten Strategien, um diese herzustellen, ohne dabei die offene Gesellschaft aus dem Blick zu verlieren? Ist die Technologieausrichtung des Sicherheitsforschungsprogramms angemessen oder müsste sie ggf. um ganz andere Fragestellungen ergänzt werden? Welchen Preis – an Geld, Freiheit, Privatheit, Gerechtigkeit – sind wir für die Herstellung einer bestimmten Sicherheit bereit zu zahlen?

GEFÖRDERT VON

Grundsätzlich sollte zwischen eher kurzfristig (technische Sicherheit; Polizeipräsenz an „hot spots“) und eher langfristig orientierten Lösungsansätzen (Prävention als langfristige Investition in gesellschaftliche Sicherheit und Stabilität) unterschieden werden. Notwendig sei ein Denken in verschiedenen Zeitskalen, auf denen jeweils andere Vorgehensweisen adäquat sind. Kurzfristige Lösungen allein reichten nicht aus; diese sollten in jedem Fall mit mittel- und langfristigen, auf Nachhaltigkeit ausgerichteten, Strategien kombiniert werden. Zur Frage der Kommunikationsfähigkeit von Forschung wurde angemerkt, dass Kommunikation viel früher einsetzen und dialogisch gestaltet werden sollte (konsensfähige Lösungen durch von Beginn an integrierte Prozesse der Technologieentwicklung bzw. ggf. auch Nicht-Entwicklung bzw. modifizierte Entwicklung).

ANHANG:

Begrifflichkeiten: Dual Use, Multi Use, gefährliches Wissen

- Gebrauch vs. Missbrauch von Forschung(ergebnissen), Technologien, Wissen
- zivil vs. militärisch (legale Doppelnutzung)
 - problematisch? („Militarisierung“ der Gesellschaft, „Zivilisierung“ des Krieges)
 - sinnvoll? (Ressourceneffizienz, nachhaltige Entwicklung)
- rechtsstaatlich unbedenkliche vs. problematische zivile Nutzung (Aushöhlung demokratischer Grundrechte; Drittstaaten mit zweifelhafter Grundrechtssituation: Folter, Ausspähung von Oppositionellen, Menschenrechtsverletzungen...)
- friedliche vs. nicht-friedliche Intentionen
- offensive vs. defensive Aktivitäten
- Bezug auf Material, Technologien, Wissen/Know-how

Leitlinien und Kriterien zur Begutachtung, Beurteilung von Forschungsprojekten/ Indikatoren für Missbrauchsrisiko

- Unabhängigkeit der Begutachtung gewährleisten
- Begutachtung zu unterschiedlichen Zeitpunkten (Projektauswahl, falls notwendig ggf. projektbegleitend, Verwertung von Forschungsergebnissen) und auf unterschiedlichen Ebenen (Wissenschaft / Institutionen, Geldgeber, Zeitschriften)
- Begutungskriterien sollten konkret sein, kontinuierlich aktualisiert werden, wenn möglich international harmonisiert sein; die Kriterien sollten sich beziehen auf:
 - Art der Forschung (Grundlagenforschung vs. Entwicklung)
 - Wer forscht? (zivil/akademisch vs. militärisch)
 - Wer finanziert? (zivil vs. militärisch)
 - Wie transparent? (akademisch/offen vs. klassifiziert)
 - Wie sicher? (safety/security)
 - Wie sensibel international? (internationale Normen vs. hoher Grad der Verregelung/Normenbildung)

Klugheitsregeln/ Kriterien mittlerer Reichweite (Begutachtung)

- Das Problem, für das eine Lösung entwickelt werden soll, muss ein ziviles Problem sein
- Reflexion des Einflusses von Technologien auf die Gesellschaft
- Frage der Industriepartner: Regelungen für den Umgang mit reinen Rüstungsunternehmen, Mischkonzernen müssen gefunden werden
- Jeder Transfer einer Technologie von einem Bereich in einen anderen muss reflektiert werden: Hierzu müssten geeignete Kriterien und (Reflexions-)Instrumente entwickelt werden.

Vorschläge für verbesserte Mechanismen der wissenschaftlichen Selbstkontrolle

- (Weiter)Entwicklung und Bekanntmachung von Verhaltenskodizes;
- Strukturierte Aus- und Weiterbildung
 - in der akademischen Ausbildung (Curricula überarbeiten, Lehrkonzepte entwickeln...)
 - auf Ebene der Forschungseinrichtungen

- Dual-Use-Beauftragte, compliance-Beauftragte, Ethik-Kommissionen (mit erweitertem Auftrag über „Forschung am Menschen“ hinaus)
- Einrichtung einer zentralen (nationalen) Kommission, die die Begutachungskriterien regelmäßig überprüft und bei besonderen Problemfällen Empfehlungen aussprechen kann

Vorschläge für Regeln wissenschaftlichen Arbeitens, Umgang mit gefährlichem Wissen
("Biosecurity")

- Sensibilisierung, bewusstseinsbildende Maßnahmen, Aus-/Weiterbildung des Personals
- Kritische Prüfung/ Review von geplanten Experimenten (intern oder extern)
- Schaffung einer nationalen Beratungsinstitution
- Zertifizierung der Endnutzer von Dual-Use-Gütern
- Entwicklung von Best Practices Verbesserung/ Stärkung der gesetzlichen Bestimmungen
- Review von Publikationen, ggf. Publikationsbeschränkungen/ -verbote Internationale Harmonisierung von Kontrollmechanismen

GEFÖRDERT VON



Referenten- und Teilnehmerverzeichnis

1. Dipl.-Phys. Christian Alwardt
Institut für Friedensforschung und
Sicherheitspolitik IFSH, Uni Hamburg
2. Prof. Dr. Regina **Ammicht Quinn**
Internationales Zentrum für Ethik in den
Wissenschaften IZEW, Uni Tübingen
3. Dipl.-Psych. Harald Arnold
Abteilung Kriminologie am Max-Planck-Institut
für ausländisches und internationales
Strafrecht, Freiburg i.Br.
4. Prof. Dr. Gerhard Banse
Berliner Zentrum Technik & Kultur sowie
Institut für Technikfolgenabschätzung und
Systemanalyse am Karlsruher Institut für
Technologie KIT, Berlin / Karlsruhe
5. LRD Holger **Beutel**
Bundesamt für Wirtschaft und Ausfuhrkontrolle
BAFA, Eschborn
6. Sabine Blum M.A.
Institut für Soziologie der Albert-Ludwigs-
Universität, Freiburg i.Br.
7. Dr. Robert Gaßner
Institut für Zukunftsstudien und
Technologiebewertung IZT, Berlin
8. Dr. Iris **Hunger**
Informationsstelle des Bundes für Biologische
Sicherheit,
Robert-Koch-Institut RKI, Berlin
9. Dr. Andreas Hoffknecht
Projektträger Sicherheitsforschung, Zukunftsige
Technologien Consulting der VDI TZ GmbH,
Düsseldorf
10. Dipl. Pol. Gunnar Jeremias M.P.S.
Research Group for Biological Arms Control /
Zentrum für Naturwissenschaften und
Friedensforschung ZNF, Hamburg
11. Dr. Wolf Junker
Referat 522 Sicherheitsforschung
Bundesministerium für Bildung und Forschung
BMBF, Bonn

- | | | |
|-----|--|---|
| 12. | Dr. Martin Kahl | Institut für Friedensforschung und Sicherheitspolitik IFSH, Uni Hamburg |
| 13. | Prof. Dr. Stefan Kaufman | Institut für Soziologie der Albert-Ludwigs-Universität, Freiburg i.Br. |
| 14. | Priv.-Doz. Dr. Hans-Georg Koch | Abteilung Strafrecht am Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg i.Br. |
| 15. | Prof. Dr. Bernd Klauer | Technische Informatik an der Hochschule der Bundeswehr Hamburg sowie Fachgruppensprecher PII, Deutsche Physikalische Gesellschaft |
| 16. | Dr. Hartmut Küchle | International Center for Conversion BICC, Bonn |
| 17. | Dr. Stephan Lingner | Europäische Akademie zur Erforschung von Folgen wiss.-techn. Entwicklungen, Bad Neuenahr-Ahrweiler |
| 18. | Dr. Oliver Meier | Institut für Friedensforschung und Sicherheitspolitik IFSH, Uni Hamburg |
| 19. | Prof. Dr. Gregor Nickel | Department Mathematik, Uni Siegen |
| 20. | LKD Dr. Peter Poerting | Bundeskriminalamt BKA, Wiesbaden |
| 21. | Dr. Sabine Reiter | Referat 321 Übertragbare Krankheiten, AIDS, Seuchenhygiene - Bundesministerium für Gesundheit, Berlin |
| 22. | Dr. Arnold Sauter | Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag TAB, Berlin |
| 23. | Dr. Gabriela Schumann | Zentrale der Fraunhofer-Gesellschaft, München |
| 24. | Dipl.-Ing. Christoph Stroschein | German European Security Association GESA, Berlin |
| 25. | Dr. Joachim Vetter | Deutscher Ethikrat, Berlin |
| 26. | Dr. Stefan Voigt | Deutsches Zentrum für Luft- und Raumfahrt DLR, Wessling |
| 27. | Prof. Dr. Jutta Weber | Institut für Medienwissenschaft, Fakultät für |

GEFÖRDERT VON

Kulturwissenschaften der Uni Paderborn

28. Dr.-Ing. Karin Wey
Fachkoordination Sicherheitsforschung, VDI
Technologiezentrum GmbH, Düsseldorf
29. Prof. Dr. Uwe **Wiemken**
Fraunhofer-Institut für Naturwissenschaftlich-
Technische Trendanalysen INT, Euskirchen
30. Peter Zoche M.A.
Projektleitung Fachdialog Sicherheitsforschung,
Fraunhofer-Institut für System- und
Innovationsforschung ISI, Karlsruhe