EUROPÄISCHE KOMMISSION

Brüssel, den 26.7.2012
COM(2012) 417 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT UND DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS

Eine Industriepolitik für die Sicherheitsbranche

Maßnahmenkatalog für eine innovative und wettbewerbsfähige Sicherheitsbranche

{SWD(2012) 233 final}

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT UND DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS

Eine Industriepolitik für die Sicherheitsbranche

Maßnahmenkatalog für eine innovative und wettbewerbsfähige Sicherheitsbranche

1. EINLEITUNG

Für Sicherheit zu sorgen, ist eine der wichtigsten Aufgaben jeder Gesellschaft. Jeder Politikbereich enthält eine wichtige Sicherheitskomponente. Jede stabile Gesellschaft ist auf ein sicheres und geschütztes Umfeld angewiesen. Eine wettbewerbsfähige, in der EU ansässige Sicherheitsindustrie, die optimierte Sicherheitslösungen anbietet, kann einen wesentlichen Beitrag zur Widerstandskraft der europäischen Gesellschaft leisten.

Die Sicherheitsindustrie ist eine Branche mit erheblichem Wachstums- und Beschäftigungspotenzial. In den vergangenen zehn Jahren hat sich das Volumen des Sicherheitsweltmarkts von rund 10 Mrd. EUR auf etwa 100 Mrd. EUR 2011 nahezu verzehnfacht. Zahlreiche Studien zeigen, dass die Wachstumsrate des Sicherheitsmarkts sowohl in der EU als auch weltweit über dem durchschnittlichen BIP-Wachstum liegen wird.[1]

Die Kommission hat dieses enorme Wachstumspotenzial aufgegriffen, indem sie die Sicherheitsindustrie zu einem Kernelement der Leitinitiative „*Eine integrierte Industriepolitik für das Zeitalter der Globalisierung - Vorrang für Wettbewerbsfähigkeit und Nachhaltigkeit*“ der Strategie „Europa 2020“[2] gemacht hat.

Dieser Maßnahmenkatalog ist die erste Stufe ebendieser Initiative. Sein übergeordnetes Ziel besteht darin, das Wachstum der EU-Sicherheitsindustrie zu steigern und die Beschäftigung in dieser Branche zu erhöhen.

Da die Unternehmen der EU (in der Sicherheitsbranche) auf einem hohen technischen Entwicklungsstand sind, können sie sich nach wie vor in den meisten Branchensegmenten neben den Weltmarktführern behaupten. Allerdings weisen jüngste Trends und Marktprognosen darauf hin, dass die Anteile europäischer Unternehmen auf dem Weltmarkt in den kommenden Jahren konstant schrumpfen werden. In Wirtschaftsprognosen und unabhängigen Studien wird vorhergesagt, dass der derzeitige Marktanteil der EU-Unternehmen im Sicherheitsgewerbe von rund 25 % des Weltmarktes im Jahr 2010 bis 2020 um etwa ein Fünftel auf 20 % einbrechen könnte, wenn nichts unternommen wird, um die Wettbewerbsfähigkeit der EU-Sicherheitsindustrie zu stärken.

Die Marktführer sind US-Firmen, weil sie technisch führend sind und zusätzlich von einem einheitlichen rechtlichen Umfeld und einem stabilen Inlandsmarkt profitieren. Damit verfügen sie nicht nur über eine komfortable Ausgangsbasis, sondern auch über eine US-Marke mit

---

[1] Sämtliches Zahlenmaterial und alle Studien, die in diesem Maßnahmenkatalog genannt werden, werden in der begleitenden Arbeitsunterlage der Kommissionsdienststellen im Detail aufgeführt.

[2] KOM(2010) 614 endg.

hohem Wiedererkennungswert, was sich im internationalen Wettbewerb als äußerst wertvoller Vorteil gegenüber den EU-Unternehmen erwiesen hat.

Dass eine vergleichbare „EU-Marke“ nicht existiert, ist besonders bedenklich, wenn man sich vor Augen führt, dass die wichtigsten Märkte für Sicherheitstechnik künftig nicht in Europa, sondern in den aufstrebenden Volkswirtschaften Asiens, Südamerikas und des Nahen und Mittleren Ostens liegen werden.

Asien schließt außerdem technologisch immer schneller zu den EU-Unternehmen auf. Geht ihr technologischer Vorsprung einmal verloren, wird der Wettbewerb für die EU-Unternehmen besonders schwierig, weil sie auch durch die in der EU höheren Produktionskosten häufig benachteiligt sind.

Vorrangiges Ziel der Kommission ist es daher, einen besser funktionierenden europäischen Binnenmarkt für Sicherheitstechnologien aufzubauen. Die Schaffung positiver Bedingungen auf dem Binnenmarkt, eine Verbesserung des Wettbewerbs und die Senkung der Produktionskosten durch die Nutzung von Skaleneffekten sind weitere Grundvoraussetzungen dafür, die Position der EU-Sicherheitsindustrie in jenen Schwellenländern zu stärken, in denen die Zukunft der Sicherheitsbranche liegt. Besonderes Augenmerk sollte dabei der Unterstützung der KMU gelten, die sich um Zugang zu Auslandsmärkten in Drittländern bemühen.

Im Europäischen Forum für Sicherheitsforschung und Innovation (ESRIF) sowie in der darauf aufbauenden Mitteilung der Kommission[3] wurden bereits eine ganze Reihe dieser Fragen aufgegriffen. Für die IKT-Branche stellt die Erhöhung der Sicherheit ein unverzichtbares Element der Geräte und Produkte dar, die von den IKT-Firmen angeboten werden, und ist entscheidend für die künftige Wettbewerbsfähigkeit. Dies wird auch Gegenstand der Europäischen Strategie für Internetsicherheit sein, die gerade ausgearbeitet wird. Bislang gab es jedoch keinen EU-weit einheitlichen Ansatz, um die EU-Sicherheitsindustrie wettbewerbsfähiger und innovativer zu machen.

Wie aktuelle Studien und das Meinungsbild der Interessenträger[4] zeigen, sind dem internationalen Wettbewerbsdruck nicht so sehr die Dienstleistungen ausgesetzt, sondern vielmehr die Herstellung der Produkte und Technologien, weil der Löwenanteil der potenziellen Ausfuhren in der Sicherheitsindustrie auf sie entfällt. Deshalb erstreckt sich dieser Maßnahmenkatalog nicht auf Sicherheitsdienstleistungen an sich (z. B. vor Ort eingesetztes Sicherheitspersonal), sondern nur auf jene Leistungen, die im Zusammenhang mit Aufbau und Wartung von Sicherheitsgeräten erbracht werden.

Die Kommission wird mit allen verfügbaren Mitteln einen echten Binnenmarkt für Sicherheitstechnik schaffen und so der EU-Sicherheitsindustrie zu einer starken Binnenbasis verhelfen, von der ausgehend sie neue Anteile auf den sich entwickelnden Märkten gewinnen kann.

Die Kommission wird sicherstellen, dass alle zur Entwicklung des Binnenmarktes für Sicherheitstechnik ergriffenen Initiativen mit der EU-Grundrechtecharta im Einklang stehen und insbesondere das Grundrecht auf Schutz der Privatsphäre und Schutz der personenbezogenen Daten achten.

---

[3] KOM(2009) 691 endg.

[4] Siehe Arbeitsunterlage der Kommissionsdienststellen.

2. DIE EU-SICHERHEITSINDUSTRIE UND IHR MARKT

Schätzungen zufolge weist die Sicherheitsindustrie weltweit ein Marktvolumen von etwa 100 Mrd. EUR auf (im Jahr 2011) und bietet Arbeitsplätze für rund 2 Mio. Menschen. In der EU liegt der Sicherheitsmarkt bei einem Volumen in der Größenordnung von 26 Mrd. EUR bis 36,5 Mrd. EUR und bei einem Beschäftigungsstand von 180 000 Mitarbeiten (im Jahr 2011).

Bislang gibt es jedoch noch keine klare Definition der Sicherheitsindustrie und die methodische Erfassung dieses Wirtschaftszweigs in einer Systematik scheitert aus mehreren Gründen:

- Die Sicherheitsindustrie selbst wird von den wichtigsten statistischen Systematiken (NACE, Prodcom usw.) nicht erfasst.

- Die Herstellung von sicherheitsbezogenen Produkten verbirgt sich in zahlreichen Positionen. In den Statistiken über diese Positionen wird nicht zwischen sicherheitsbezogenen und nicht sicherheitsbezogenen Tätigkeiten unterschieden.

- Auf Seiten der Industrie selbst gibt es keine Quelle für europaweite statistische Daten.

- Von der Angebotsseite betrachtet, sind die Abnehmer von Sicherheitsanlagen und -systemen häufig nicht bereit, Angaben zu ihren Sicherheitsausgaben zu machen.

Um diesem Mangel an Daten über die Sicherheitsindustrie und ihren Markt abzuhelfen, wird die Kommission eine empirische Grundlage entwickeln, von der ausgehend verlässlichere Zahlen über die Sicherheitsmärkte gewonnen werden können. Für dieses Vorhaben bedarf es der Zusammenarbeit mit den wichtigsten Branchenverbänden.

Immerhin lässt sich die EU-Sicherheitsindustrie grob in folgende Branchen unterteilen[5]:

- Luftsicherheit,

- Sicherheit des Seeverkehrs,

- Grenzschutz,

- Schutz kritischer Infrastrukturen,

- Informationsgewinnung zur Terrorismusbekämpfung (einschließlich Cybersicherheit und Kommunikation),

- Krisenbewältigung/Katastrophenschutz

- physische Sicherheit durch Schutz und

- Schutzkleidung.

[5] Diese Auflistung ist nicht vollständig. Einen ausführlicheren Überblick über die Einzelbranchen und die von ihnen repräsentierten Technologien enthält die Arbeitsunterlage der Kommissionsdienststellen.

Der Sicherheitsmarkt wird von drei Merkmalen gekennzeichnet:

(1) **Es handelt sich um einen stark zersplitterten Markt, der durch nationale oder sogar regionale Grenzen unterteilt ist.** Gerade in der Sicherheitspolitik, einem der sensibelsten Politikbereiche, sind die Mitgliedstaaten am wenigsten bereit dazu, ihre nationalen Souveränitätsrechte abzutreten.

(2) **Es handelt sich um einen institutionellen Markt.** Der Sicherheitsmarkt ist zu großen Teilen noch immer ein institutioneller Markt, d. h. die Käufer sind Behörden. Selbst dort, wo der Markt inzwischen kommerziell geprägt ist, sind die Sicherheitsanforderungen noch immer von gesetzlichen Vorgaben bestimmt.

(3) **Es handelt sich um einen Markt mit starker gesellschaftlicher Dimension.** Sicherheit ist nicht nur eines der menschlichen Grundbedürfnisse, sondern auch ein äußerst sensibler Bereich. Sicherheitsmaßnahmen und -technologien können Folgen für die Grundrechte haben und schüren häufig die Angst vor einer möglichen Beschneidung der Privatsphäre.

3. DIE HAUPTPROBLEME FÜR DIE EU-SICHERHEITSINDUSTRIE

Durch diese drei Merkmale des Sicherheitsmarkts sind auch die folgenden drei Hauptprobleme der EU-Sicherheitsindustrie bedingt:

(1) Die Zersplitterung des EU-Sicherheitsmarkts

Das größte aller Probleme ist die starke Zersplitterung des EU-Sicherheitsmarktes (d. h. das Fehlen einheitlicher Zertifizierungsverfahren und Normen). Durch unterschiedliche Ansätze bildeten sich in der Tat wenigstens 27 verschiedene Sicherheitsmärkte heraus, die ihrerseits jeweils in eine Unzahl von Sicherheitsbranchen zerfallen.

Dieser Umstand bringt nicht nur eine eher ungewöhnliche Situation in Bezug auf den Binnenmarkt mit sich, sondern auch negative Auswirkungen sowohl auf die Angebotsseite (Industrie) als auch auf die Nachfrageseite (öffentliche und private Käufer von Sicherheitstechnologien). Dies führt zu hohen Schranken für den Markteintritt und erschwert echte Skaleneffekte außerordentlich bzw. verhindert sie ganz und gar. Darüber hinaus geht damit ein fehlender Wettbewerb unter den Anbietern und ein suboptimaler Einsatz der öffentlichen Mittel einher.

(2) Die Kluft zwischen Forschung und Markt

Wenn FuE an neuen Technologien betrieben wird, kann die EU-basierte Sicherheitsindustrie oft nur sehr schwer vorhersagen, ob sich das Ergebnis am Ende vermarkten lassen wird, oder auch nur einigermaßen absehen, ob es überhaupt einen Markt dafür geben wird. Dieses Problem ist zwar weit verbreitet und tritt auch in vielen anderen Industriebranchen auf, in der Sicherheitsindustrie ist es aber besonders ausgeprägt, weil sie hauptsächlich auf einem institutionellen Markt agieren muss.

Dies hat einige negative Konsequenzen: So werden potenziell aussichtsreiche FuE-Ansätze nicht weiterverfolgt, was wiederum bedeutet, dass manche Technologien, die einen Sicherheitsgewinn für die Bürger darstellen könnten, gar nicht für die Nachfrageseite verfügbar sind.

(3) Die gesellschaftliche Dimension der Sicherheitstechnologien

Die Akzeptanz neuer Produkte und Technologien durch die Gesellschaft ist ein generelles Problem für alle Industriebranchen. Es gibt jedoch eine Reihe von Besonderheiten, die Sicherheitstechnologien von anderen Bereichen unterscheiden. Sicherheitstechnologien betreffen mittelbar oder unmittelbar die Grundrechte wie das Recht auf Achtung des Privat- und Familienlebens, auf den Schutz personenbezogener Daten, auf Privatsphäre oder Menschenwürde.

Die Problematik der gesellschaftlichen Akzeptanz der Sicherheitstechnologien hat eine Reihe negativer Konsequenzen zur Folge. Für die Industrie bringt sie das Risiko mit sich, in Technologien zu investieren, die dann aber nicht von der Öffentlichkeit akzeptiert werden, so dass die Investition verloren ist. Für die Abnehmer bedeutet es, dass sie stattdessen ein weniger umstrittenes Erzeugnis erwerben müssen, das jedoch den Sicherheitsanforderungen nicht voll und ganz gerecht wird.

4. LÖSUNGSANSÄTZE

Die Kommission hat eine Reihe von zentralen politischen Maßnahmen ermittelt, durch die die Wettbewerbsfähigkeit der EU-Sicherheitsindustrie gestärkt, ihr Wachstum stimuliert und die Schaffung von Arbeitsplätzen ausgebaut werden können, und die Folgendes umfassen:

- **Überwindung der Marktzersplitterung**, durch Schaffung von EU-weiten/internationalen Normen, Vereinheitlichung der Zertifizierungs-/Konformitätsbewertungsverfahren für Sicherheitstechnologien in der EU und eine bessere Nutzung der Synergien zwischen den Sicherheits- und den Verteidigungstechnologien;

- **Schließen der Lücke zwischen Forschung und Markt**, durch Anpassung der Finanzierungsprogramme und verbesserte Nutzung der Rechte des geistigen Eigentums sowie umfassenden Einsatz der vorkommerziellen Auftragsvergabe bei der Sicherheitsforschung im Rahmen von „Horizont 2020“[6];

- **bessere Einbeziehung der gesellschaftlichen Dimension** durch gründliche Bewertung der sozialen Folgen, einschließlich der Auswirkungen auf die Grundrechte, und durch Schaffung von Mechanismen zur Prüfung der gesellschaftlichen Auswirkungen während der FuE-Phase.

4.1. Überwindung der Marktzersplitterung

4.1.1. Normung

Normen spielen eine wichtige Rolle bei der Defragmentierung der Märkte und unterstützen die Industrie bei der Erzielung von Skaleneffekten. Normen sind zudem von höchster Bedeutung für die Abnehmer, weil sie vor allem die Interoperabilität der Technologien sicherstellen, die u. a. von Ersthelfern und Strafverfolgungsbehörden eingesetzt werden. Darüber hinaus tragen die Normen wesentlich dazu bei, dass die Sicherheitsdienste in einheitlicher Qualität erbracht werden. Für die internationale Wettbewerbsfähigkeit der EU-

[6] KOM(2011) 809 endg.

Sicherheitsindustrie kommt es ganz entscheidend darauf an, EU-weite Normen zu erarbeiten und diese weltweit zu fördern.

Leider gibt es derzeit nur wenige EU-Normen im Sicherheitsbereich. Das Entstehen eines echten Sicherheitsbinnenmarktes wird durch unterschiedliche nationale Normen stark behindert, die damit die Wettbewerbsfähigkeit der EU-Industrie schwächen. Diese nationalen Unterschiede abzubauen, ist eine Grundvoraussetzung dafür, dass die EU bei der Ausarbeitung globaler Normen maßgeblich mitwirken kann.

Die Kommission kündigte in ihrer Mitteilung über eine strategische Vision der europäischen Normung[7] an, dass die Normungsarbeiten im Sicherheitsbereich beschleunigt werden müssten. Daher beauftragte die Kommission 2011 die Europäischen Normungsorganisationen, einen detaillierten Überblick über die bestehenden internationalen, europäischen und nationalen Normen im Sicherheitsbereich zu erarbeiten und Normungslücken aufzulisten. Die größten Lücken wurden in folgenden Bereichen festgestellt:

– Chemische, biologische, radiologische und nukleare Bedrohungen sowie Sprengstoffe – Mindeststandards für die Detektion sowie die Probenahme, auch im Bereich der Luftverkehrssicherheit;

– Grenzsicherung – gemeinsame Normen für technische Aspekte und Interoperabilität bei automatischen Grenzkontrollsystemen sowie Normen für biometrische Identifikatoren und

– Krisenmanagement/Zivilschutz – Normen für Interoperabilität in der Kommunikation sowie Interoperabilität von Befehl und Überwachung, einschließlich der organisatorischen Interoperabilität, sowie Massenbenachrichtigung der Bevölkerung.

Maßnahme 1: Ausgehend von diesen ersten Prioritäten wird die Kommission die Europäischen Normungsorganisationen ersuchen, konkrete und präzise Normungsfahrpläne auszuarbeiten. Bei diesen Normungsfahrplänen sollte das Hauptaugenmerk auf der nächsten Generation von Instrumenten und Technologien liegen. Voraussetzung dafür ist die Einbeziehung der Endnutzer und der Sicherheitsindustrie sowie eine kohärente Politik.

Durchführungszeitraum: ab Mitte 2012

4.1.2. Zertifizierungs-/Konformitätsbewertungsverfahren

Es gibt heute keine EU-weit geltenden Zertifizierungssysteme für Sicherheitstechnologien. Die nationalen Systeme weichen stark voneinander ab und sind somit einer der Hauptgründe für die Zersplitterung des Marktes. Die Kommission hat die Bereiche ermittelt[8], in denen es in einer ersten Phase am sinnvollsten wäre, ein EU-weit geltendes Zertifizierungssystem einzurichten, und zwar zunächst bei:

– Durchleuchtungsgeräten auf Flughäfen (Detektoren) und

[7] KOM(2011) 311 endg.

[8] Genauere Informationen über die Grundüberlegung und die Kriterien, nach denen die Zielbereiche ausgewählt wurden, sind der Arbeitsunterlage der Kommissionsdienststellen zu entnehmen.

– Alarmanlagen[9].

Für die Durchleuchtungsgeräte auf Flughäfen gibt es eine ganze Reihe von EU-Rechtsvorschriften, in denen die Leistungsanforderungen für solche Geräte festgelegt sind.[10] Allerdings enthalten diese Vorschriften keine Bestimmungen über den vorgeschriebenen Konformitätsbewertungsmechanismus, so dass die Zertifizierung von Durchleuchtungsgeräten aus einem Mitgliedstaat durch die gegenseitige Anerkennung auch in allen anderen Mitgliedstaaten akzeptiert würde. Dass auf EU-Ebene harmonisierte Normen und eine rechtlich vorgeschriebene Konformitätsbewertung für Durchleuchtungsgeräte auf Flughäfen fehlen, führt auch zur Zersplitterung des Binnenmarktes.

Für Alarmanlagen bestehen zwar bereits europäische Leistungsnormen. Zudem gibt es den Zertifizierungsmechanismus „CertAlarm“, der von der Industrie betrieben wird. Dieses System krankt allerdings daran, dass es privatrechtlich verwaltet wird und die Behörden der Mitgliedstaaten nicht verpflichtet sind, die im Rahmen dieses Systems ausgestellten Zertifikate anzuerkennen.

Würden Produkte künftig anhand eines EU-weiten Zertifizierungssystems zertifiziert, könnten sie ein „EU-Zeichen“ tragen, das der CE-Kennzeichnung für die Produktsicherheit ähneln könnte. Wie vom ESRIF vorgeschlagen, könnte ein solches Zeichen als Qualitätssiegel für (in der EU hergestellte und validierte) Sicherheitsprodukte dienen.

Zurückhaltenden Schätzungen zufolge könnten die Hersteller allein bei diesen beiden Produktklassen Prüf- und Zertifizierungskosten von bis zu 29 Mio. EUR im Jahr einsparen.

Eine Vereinheitlichung der Zertifizierungssysteme für Durchleuchtungsgeräte auf Flughäfen und Alarmanlagen sollte sich zudem positiv auf die Entstehung einer klaren europäischen Identität (einer möglichen „EU-Marke“) bei diesen Technologien auswirken. Diese „Marke“ sollte zur Stärkung der weltweiten Wettbewerbsfähigkeit der EU-Unternehmen gegenüber ihren Konkurrenten in den USA und China beitragen.

---

[9] Es ist darauf hinzuweisen, dass die Alarmanlagen mit einem Volumen von 4,5 Mrd. EUR oder einem Anteil von 50 % des Marktes für Objektschutz ein extrem wichtiges Segment darstellen.

[10] Siehe Verordnung (EG) Nr. 300/2008, Verordnung (EG) Nr. 272/2009 und Verordnung (EU) Nr. 185/2010.

Maßnahme 2: Vorbehaltlich einer gründlichen Folgenabschätzungsanalyse und einer Konsultation der Interessenträger würde die Kommission zwei Gesetzesinitiativen vorschlagen: einen Rechtsakt zur Festlegung eines EU-weit einheitlichen Zertifizierungssystems für Durchleuchtungsgeräte auf Flughäfen (Detektoren) und einen weiteren Rechtsakt zur Festlegung eines EU-weit einheitlichen Zertifizierungssystems für Alarmanlagen. Bezweckt wird damit die gegenseitige Anerkennung der Zertifizierungssysteme.

Durchführungszeitraum: Mitte 2012 bis Ende 2014

4.1.3. Nutzung der Synergien zwischen Sicherheits- und Verteidigungstechnologien

Man kann klar zwischen einem (zivilen) Sicherheits- und einem (militärischen) Verteidigungsmarkt unterscheiden. Doch könnte man bereits die Existenz dieser beiden getrennten Märkte an sich als Zersplitterung betrachten. Eine Zersplitterung ist bis zu einem gewissen Grad normal, da die Industriebasis, die diese beiden Märkte beliefert, nicht voll und ganz deckungsgleich ist und sich auch die Endnutzer, die Anwendungsbereiche und die Anforderungen unterscheiden. Diese Zersplitterung setzt sich allerdings sowohl nach oben bis zur Ebene der FuE und der Fähigkeitenentwicklung als auch nach unten bis zur Ebene der Normung fort. Dies führt hin und wieder dazu, dass sich FuE-Aktivitäten überschneiden und Skaleneffekte nicht genutzt werden können, weil auf beiden Märkten unterschiedliche Standards herrschen.

In der FuE werden von der Europäischen Verteidigungsagentur (EDA) derzeit durch die *Europäische Rahmenvereinbarung für eine Zusammenarbeit* Synergien zwischen zivilem und militärischem Bereich angestrebt. Im Rahmen dieser Zusammenarbeit wird eine laufende Koordinierung zwischen dem Themenbereich „Sicherheit“ des 7. Forschungsrahmenprogramms (RP7) und der Verteidigungsforschung der EDA gewährleistet. Auf diesem Weg soll diese Forschung synchronisiert werden, damit Überschneidungen vermieden werden und mögliche Synergien zum Tragen kommen können. Die Kommission will diese Kooperation im Rahmen von „Horizont 2020“ fortsetzen.

Obwohl eine noch weiter vorgelagerte Kooperation im Hinblick auf eine bessere Synchronisierung der Fähigkeitenplanung nützlich wäre, ist die Kommission der Ansicht, dass im zivilen Bereich der Sicherheit derart viele Behörden beteiligt sind, dass es heute nicht möglich ist, mit dem Verteidigungsbereich, wo es pro Mitgliedstaat mit dem jeweiligen Verteidigungsministerium in der Regel nur einen Akteur gibt, eine gemeinsame Fähigkeitenplanung zu erstellen.

Im Zusammenhang mit der nachgelagerten Kooperation sollte nach dem Dafürhalten der Kommission die Entwicklung von „Hybridnormen“, also Normen, die sowohl auf die zivilen Sicherheits- als auch auf die Verteidigungstechnologien anwendbar sind, aktiv vorangetrieben werden, sofern die Technologien gleich und die Anwendungsbereiche sehr ähnlich sind. Die Kommission prüft einige vielversprechende Bereiche für solche „Hybridnormen“, darunter auch software-definierte Funktechnik und bestimmte technische Anforderungen an unbemannte Luftfahrzeugsysteme (z. B. Erkennungs- und Ausweichtechnik, Lufttüchtigkeitsanforderungen). Allein bei der software-definierten Funktechnik wird

geschätzt, dass Hybridnormen alles in allem zu einer Umsatzsteigerung von insgesamt 1 Mrd. EUR führen könnten.

Maßnahme 3: Die Kommission will in enger Zusammenarbeit mit der Europäischen Verteidigungsagentur Normungsaufträge für Hybridnormen an die Europäischen Normungsorganisationen richten. Der erste davon wird in Kürze für software-definierte Funktechnik erteilt werden.

Durchführungszeitraum: ab Mitte 2012

4.2. Schließen der Lücke zwischen Forschung und Markt

4.2.1. Anpassung von Förderprogrammen, Nutzung der Rechte des geistigen Eigentums

In ihrem Vorschlag zur Strategie „Horizont 2020" stellt die Kommission eine enge Verbindung zu einigen Politikfeldern, insbesondere dem Bereich Inneres, her. Aus diesem Grund sind in „Horizont 2020" besondere Vorschriften für den Schutz der Rechte des geistigen Eigentums in der Sicherheitsforschung vorgesehen, die der Kommission und den Mitgliedstaaten nicht nur Zugang zu den bei Projekten der Sicherheitsforschung gewonnenen neuen Erkenntnissen gewähren, sondern ihnen auch deren Nutzung zu fairen und angemessenen Bedingungen bei der öffentlichen Auftragsvergabe gestatten.[11]

Dies soll zu einer unmittelbareren und rascheren Verwertung der Ergebnisse der EU-Sicherheitsforschung durch die nationalen Behörden und zu einer engeren Zusammenarbeit mit den überwiegend öffentlichen Endnutzern führen, was wiederum die Bemühungen um den Lückenschluss zwischen Forschung und Markt im Sicherheitsbereich enorm unterstützt.

Zudem ist in den beiden Komponenten des für den nächsten Finanzplanungszeitraum vorgeschlagenen Fonds für die innere Sicherheit, die auf Außengrenzen und Visa, polizeiliche Zusammenarbeit, Kriminalprävention und Kriminalitätsbekämpfung sowie Grenzmanagement abgestellt sind, die Möglichkeit vorgesehen, mit Unionsmaßnahmen die Ergebnisse von EU-Projekten aus der Sicherheitsforschung zu erproben und zu validieren.[12]

Die Sondervorschriften über Rechte des geistigen Eigentums in der Sicherheitsforschung, die der Kommission die Nutzung dieser Rechte zu fairen und angemessenen Bedingungen erlauben, sind eine Voraussetzung dafür, dass diese Möglichkeit wirksam genutzt wird, damit die Ergebnisse der Sicherheitsforschung durch eine anschließende Erprobung und Validierung verwertet werden können.

Sollten EU-Kapazitäten benötigt werden, wird die Kommission erwägen, diese Erprobungs- und Validierungsmaßnahmen gegebenenfalls sogar durch den Ankauf von Prototypen für die EU zu verstärken.

Maßnahme 4: Die Kommission wird die neuen Vorschriften von „Horizont 2020"[13] über die Rechte des geistigen Eigentums in der Sicherheitsforschung umfassend nutzen, insbesondere im Rahmen der Möglichkeiten, die die beiden spezifischen Programme des Fonds für innere

[11] KOM(2011) 810 endg.

[12] KOM(2011) 750 und 753 endg.

[13] Zur Verabschiedung dieser Vorschriften bedarf es jedoch noch der Annahme durch den Europäischen Rat und das Europäische Parlament.

Sicherheit zur Erprobung und Validierung der Ergebnisse von EU-Projekten der Sicherheitsforschung bieten.

Durchführungszeitraum: ab Beginn 2014

4.2.2. Vorkommerzielle Auftragsvergabe

Die vorkommerzielle Auftragsvergabe[14] ist sehr nützlich für den Lückenschluss zwischen Forschung und Markt. Die Kommission hat bereits in ihrer Mitteilung über die Innovationsunion[15] deren Bedeutung insbesondere in den Bereichen mit einem institutionellen Markt oder einem hauptsächlich gesetzlich gesteuerten Markt betont, da öffentliche Aufträge für innovative Produkte und Dienstleistungen unerlässlich für die Verbesserung der Qualität und Effizienz öffentlicher Dienstleistungen in einer Zeit schwieriger Haushaltslagen sind. Die vorkommerzielle Auftragsvergabe sollte es den öffentlichen Nutzern letztlich erlauben, durch den Ankauf neuartiger Technologien eine wichtigere Rolle im Innovationszyklus zu spielen. Auftraggeber sollten als „Entwicklungsmotoren" fungieren.

Trotzdem haben sich bislang nur wenige Mitgliedstaaten die Programme für vorkommerzielle Auftragsvergabe im Sicherheitsbereich zunutze gemacht. Auf EU-Ebene wurde im Themenbereich Sicherheit des RP7 ein präoperatives Validierungsprogramm in die Aufforderung zur Einreichung von Vorschlägen für 2011 aufgenommen, was als Vorläufer für ein etwaiges künftiges Programm für vorkommerzielle Auftragsvergabe gelten kann.

„Horizont 2020" enthält ein besonderes einschlägiges Instrument, das wesentlich dazu beitragen dürfte, die praktischen Hindernisse bei der Einführung der vorkommerziellen Auftragsvergabe zu überwinden.

Aufbauend auf den Erfahrungen, die die USA mit SBIR[16] gemacht haben, kann man davon ausgehen, dass ein Anstieg der jährlichen Wachstumsrate um 1 % der auf die FuE-Förderung durch ein Programm für vorkommerzielle Auftragsvergabe zurückzuführen ist, in der Sicherheitsindustrie bis 2020 mit einer Umsatzsteigerung um 2 Mrd. EUR zu Buche schlagen dürfte.[17]

Maßnahme 5: Die Kommission will das in „Horizont 2020" dargelegte Instrument für vorkommerzielle Auftragsvergabe umfassend nutzen und einen beträchtlichen Teil ihrer Mittel für die Sicherheitsforschung für dieses Instrument veranschlagen. Dieses neuartige Finanzierungskonzept soll die Forschung und den Markt einander annähern, indem Industrie, öffentliche Hand und Endnutzer bereits ab Beginn eines Forschungsprojekts an einem Strang ziehen. Die Kommission verspricht sich am meisten von der vorkommerziellen Auftragsvergabe in den Bereichen Grenzsicherheit und Luftfahrtsicherheit.

Sie will außerdem die Mitgliedstaaten dazu auffordern, ähnliche Initiativen auf nationaler Ebene im Einklang mit dem maßgeblichen EU-Vergaberecht ins Leben zu rufen.

---

14 Die vorkommerzielle Auftragsvergabe ist hier als Ansatz für den Einkauf von FuE-Diensten zu verstehen, bei dem die Rechte des geistigen Eigentums nicht (ausschließlich) bei der Vergabebehörde liegen. Siehe KOM(2007) 799 endg.

15 KOM(2010) 546 endg.

16 SBIR – „Small Business Innovation and Research": ein Programm in den USA zur Förderung der Innovation in KMU mit Hilfe eines Projekts der vorkommerziellen Auftragsvergabe.

17 Siehe Arbeitsunterlage der Kommissionsdienststellen.

Durchführungszeitraum: ab Beginn 2014

4.2.3. Zugang zu internationalen Beschaffungsmärkten

Der öffentliche Beschaffungsmarkt der EU weist traditionell ein hohes Maß an Offenheit auf, was jedoch auf den Märkten unserer Handelspartner nicht immer in ähnlichem Umfang der Fall ist. Weltweit ist insgesamt nur ein Viertel der Beschaffungsmärkte für den internationalen Wettbewerb geöffnet.

Die Kommission hat einen Vorschlag für eine Verordnung[18] vorgelegt, die vor allem die Öffnung der öffentlichen Beschaffungsmärkte weltweit fördern und einen fairen Zugang europäischer Unternehmen zu diesen Märkten gewährleisten soll. Diese Verordnung dürfte eine Reihe von Instrumenten bieten, mit denen sich die Erreichung dieser Ziele gewährleisten lässt.

Maßnahme 6: Die Kommission wird die ihr zur Verfügung stehenden Instrumente umfassend nutzen, um der EU-Sicherheitsindustrie einen gleichberechtigten Zugang zu den internationalen Beschaffungsmärkten zu sichern. In Anbetracht der Sensibilität der Sicherheitstechnik wird auf die einschlägigen Ausfuhrregelungen ganz besonders geachtet werden.

Durchführungszeitraum: ab Ende 2013

4.2.4. Haftungsbegrenzung

Um den Lückenschluss zwischen Forschung und Markt zu erreichen und insbesondere sicherzustellen, dass das Haftungsrisiko die Sicherheitsindustrie nicht von der Entwicklung, dem Einsatz und der gewerblichen Verwertung von potenziell lebensrettenden Technologien und Dienstleistungen abhält, haben die Vereinigten Staaten nach den Anschlägen vom 11. September den US Safety Act eingeführt. Dieses Gesetz enthält eine Beschränkung der gesetzlichen Haftung für die Anbieter von Technologien und Dienstleistungen der Terrorismusbekämpfung. Die Marktführer unter den US-Unternehmen könnten durch dieses Gesetz einen Vorteil gegenüber ihren EU-Wettbewerbern auf Drittlandsmärkten erhalten.

Natürlich ist der US Safety Act im besonderen rechtlichen Umfeld der USA entstanden, wo Sammelklagen recht häufig vorkommen. Zwar soll der US Safety Act nicht in Europa kopiert werden, aber wir müssen genauer verstehen und untersuchen, wie stark Haftungsprobleme die Industrie davon abhalten, vielversprechende Technologien und Dienstleistungen zu vermarkten.

In dieser Frage gibt es keinen breiten Konsens unter den Interessenträgern der Branche, weshalb die Vereinbarkeit mit nationalen oder EU-Vorschriften erst noch eingehend juristisch analysiert werden muss.

Maßnahme 7: Die Kommission hat eine maßgebliche Studie zur Analyse der rechtlichen und wirtschaftlichen Folgen einer Beschränkung der Haftung gegenüber Dritten ausgeschrieben. Darin wird auch untersucht, welche Alternativen es zu einer Haftungsbeschränkung gibt, wie sie durch den US Safety Act eingeführt wurde, beispielsweise einen freiwilligen Fonds der

[18] COM(2012) 124 final.

Industrie oder eine Empfehlung der Kommission usw. In dieser Studie werden auch die Folgen für die Wahrung der Grundrechte gebührend berücksichtigt.

Durchführungszeitraum: 2012 bis Mitte 2013

4.3. Bessere Einbeziehung der gesellschaftlichen Dimension

4.3.1. „Prüfung" der gesellschaftlichen Tragweite in der FuE-Phase

Durch eine bessere Einbeziehung der gesellschaftlichen Dimension in die Tätigkeiten der Sicherheitsindustrie ließe sich die Unsicherheit der gesellschaftlichen Akzeptanz verringern. Dies soll nicht nur einen effizienten Einsatz der FuE-Investitionen ermöglichen, sondern den Abnehmern den Kauf von Produkten erlauben, die einerseits deren Sicherheitserfordernisse voll und ganz erfüllen und andererseits von der Gesellschaft auch akzeptiert werden.

Daher sollten die Auswirkungen auf die gesellschaftlichen Rechte und die Grundrechte nach Auffassung der Kommission bereits vor und während der FuE-Phase durch Einbeziehung der Gesellschaft berücksichtigt werden. Damit könnten gesellschaftliche Probleme in einem frühen Stadium thematisiert werden.

Die Kommission hat bereits mehrere Maßnahmen eingeleitet, mit denen sie die gesellschaftliche Dimension im Themenbereich Sicherheit des RP7 als Querschnittsthema verankern will. Im Hinblick auf „Horizont 2020" ist es nun aber an der Zeit, diese Bemühungen um Einbeziehung der Gesellschaft in Forschung und Entwicklung auf festere Grundlagen zu stellen und eine systematischere Prüfung der gesellschaftlichen Folgen einzuführen.

Die Kommission wird die Gesellschaft einbeziehen und eine Gesellschaftsfolgenabschätzung für alle ihre künftigen Forschungsprojekte im Sicherheitsbereich vorschreiben.[19] Die Kommission wird die gesellschaftlichen Folgen neuer Technologien in allen ihren bereits erörterten Programmen für die vorkommerzielle Auftragsvergabe im Sicherheitsbereich gesondert „prüfen".

4.3.2. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen in der Entwurfsphase

Einerseits ist es äußerst schwierig, gesellschaftliche Erwägungen in technologische Anforderungen umzusetzen; dies wird dadurch zusätzlich erschwert, dass es eine große Vielfalt von Sicherheitsprodukten auf dem Markt gibt. Andererseits unterscheidet sich die gesellschaftlichen Problematik im Zusammenhang mit der Sicherheit enorm von Mitgliedstaat zu Mitgliedstaat.

Aus diesem Grund ist die Kommission der Auffassung, dass sich am ehesten Fortschritte erzielen lassen, indem man in der Entwurfsphase die Konzepte Datenschutz durch Technik (*privacy by design)* und datenschutzfreundliche Voreinstellungen (*privacy by default*)[20] einführt. Der Wirtschaftsteilnehmer, der seinen Produktionsprozess als mit dem Datenschutz

---

[19] Davon ausgenommen bleiben „ungeeignete" Bereiche wie technologische Grundlagenforschung und Projekte zu weit in die Zukunft reichenden Themen und Szenarios.

[20] Ausführlichere Informationen zum Datenschutz durch Technik sind der Arbeitsunterlage der Kommissionsdienststellen zu entnehmen.

durch Technik vereinbar auditieren lassen will, müsste ein Paket von Anforderungen erfüllen, die in einer entsprechenden EU-Norm festgelegt wären. Die Einhaltung dieser Norm ist freiwillig. Die Kommission ist allerdings überzeugt, dass die Unternehmen unter einem starken Druck durch ihre Wettbewerber stehen würden, diese Norm ebenfalls einzuhalten, so dass sie einen ähnlichen Wiedererkennungswert entwickeln würde wie die ISO 9000 Normenreihe über das Qualitätsmanagement.[21]

Maßnahme 8: Die Kommission wird einen Normungsauftrag an die Europäischen Normungsorganisationen richten, die eine Norm entwickeln sollen, die sich an bestehenden Qualitätsmanagementsystemen orientiert, aber die Behandlung der Datenschutzproblematik in der Entwurfsphase zum Gegenstand hat.

Durchführungszeitraum: Mitte 2012 bis Mitte 2015

5. ÜBERWACHUNG

Die Überwachung der angekündigten politischen Maßnahmen wird durch eine von der Kommission einzurichtende gesonderte Sachverständigengruppe verfolgt. In dieser Gruppe werden alle maßgeblichen Akteure des Sicherheitsbereichs vertreten sein.

Sie wird wenigstens einmal im Jahr zur Überwachung des Fortschritts zusammentreten.

6. SCHLUSSFOLGERUNG

Dieser erste Maßnahmenkatalog der Kommission ist speziell auf die Sicherheitsindustrie ausgerichtet. Daher sind nicht nur die angekündigten Maßnahmen, sondern auch die umfassende Herangehensweise, die von der FuE-Phase bis zur Normung und Zertifizierung reicht, völlig neuartig. Von den künftigen Bewertungen wird abhängen, welche Bereiche für eine Harmonisierung vorgesehen werden könnten; in Frage kämen Bereiche wie der Land- und Seeverkehr oder auch die Haftungsbeschränkung.

Dabei ist stets zu bedenken, dass alle in diesem Dokument aufgeführten Maßnahmen stark von der Bereitschaft der Mitgliedstaaten abhängen, mit den EU-Organen, den Normungsorganisationen sowie den öffentlichen und privaten Interessenträgern zusammenzuarbeiten, um die Zersplitterung der Märkte der EU-Sicherheitsbranche zu überwinden. Die Kommission fordert daher die Mitgliedstaaten auf, ihre Initiative zur Stärkung der Wettbewerbsfähigkeit der Unternehmen der EU-Sicherheitsbranche und zum Abbau der bestehenden Hindernisse für den Markteintritt mitzutragen.

Die Kommission ist fest davon überzeugt, dass die Maßnahmen dieses Katalogs enorm dazu beitragen können, die Wettbewerbsfähigkeit der europäischen Sicherheitsindustrie zu stärken. Ziel der Kommission ist es, der EU-Sicherheitsindustrie zu einer starken Binnenbasis zu verhelfen, von der ausgehend sie auf den neuen und sich entwickelnden Märkten expandieren kann, auf denen auch künftig mit einem Wachstum des Sicherheitsmarktes zu rechnen ist.

Dieses Wachstum innerhalb und außerhalb der EU muss mit einer Verstärkung jener Maßnahmen einhergehen, mit denen die gesellschaftliche Dimension besser in die Aktivitäten

[21] COM(2012) 11.

der Sicherheitsindustrie einbezogen werden soll. Der Datenschutz durch Technik (*privacy by design*) und die Achtung der Grundrechte müssen zu Schlüsselelementen aller EU-Sicherheitstechnologien werden.