RAT DER EUROPÄISCHEN UNION

Brüssel, den 13. Januar 2010 (14.01)
(OR. en)

5265/10

JAI 21

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	22. Dezember 2009
Empfänger:	der Generalsekretär des Rates der Europäischen Union, Herr Pierre de BOISSIEU
Betr.:	MITTEILUNG DER KOMMISSION "Eine europäische Agenda für Sicherheitsforschung und Innovation – eine erste Bilanz der Kommission über die wichtigsten Ergebnisse und Empfehlungen des ESRIF"

Die Delegationen erhalten in der Anlage das Kommissionsdokument - KOM(2009) 691 endgültig.

Anl.: KOM(2009) 691 endgültig

KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 21.12.2009
KOM(2009)691 endgültig

MITTEILUNG DER KOMMISSION

Eine europäische Agenda für Sicherheitsforschung und Innovation – eine erste Bilanz der Kommission über die wichtigsten Ergebnisse und Empfehlungen des ESRIF

EN

MITTEILUNG DER KOMMISSION

Eine europäische Agenda für Sicherheitsforschung und Innovation – eine erste Bilanz der Kommission über die wichtigsten Ergebnisse und Empfehlungen des ESRIF

1. EINLEITUNG

Eines der Hauptziele der Europäischen Union besteht darin, die europäischen Werte Gerechtigkeit, Freiheit und Sicherheit zu erhalten und weiter zu entwickeln und gleichzeitig die immer komplexer werdenden Herausforderungen im Sicherheitsbereich in Angriff zu nehmen.

Die Bekämpfung des Terrorismus und der organisierten Kriminalität, der Schutz der europäischen Außengrenzen und das zivile Krisenmanagement haben für unser tägliches Leben an Bedeutung gewonnen. Der Klimawandel könnte, wenn die richtigen Maßnahmen ausbleiben, weitreichende destabilisierende Folgen auf globaler Ebene haben. Gleichzeitig lassen sich interne und externe Sicherheit immer weniger voneinander trennen. Um diese Punkte in Angriff zu nehmen, muss moderne Technologie eingesetzt werden.

Da Sicherheitstechnologien in den modernen Gesellschaften zunehmend stärker präsent werden und zuweilen Bedenken bei den Bürgerinnen und Bürgern hervorrufen, muss unbedingt sichergestellt werden, dass Projekte im Bereich Sicherheitsforschung und –entwicklung einer ethischen Überprüfung unterzogen werden und transparent sind. Unsere Sicherheit muss auf unseren europäischen Werten aufbauen. Und umgekehrt werden Sicherheitslösungen gebraucht, um unsere gesellschaftlichen Werte zu schützen.

Ein Vorgehen gegen diese Bedenken in den kommenden Jahren setzt ein besseres Verständnis der Wechselwirkung zwischen den menschlichen und den natürlichen Faktoren voraus, die zu Sicherheitsrisiken führen können; dieses bessere Verständnis ist neben dem Einsatz moderner Technologie und innovativer Lösungen oft auch wesentlich, um wirkungsvolle Reaktionen zu konzipieren.

Die Kommission war der Auffassung, es sei unerlässlich, Vertreter der Industrie, der öffentlichen und privaten Endnutzer, von Forschungseinrichtungen und Universitäten sowie Nichtregierungsorganisationen und EU-Institutionen zusammenzubringen, um die wirksamsten Lösungen für diese Herausforderungen zu finden. 2007 schlug sie daher im Einvernehmen mit den Mitgliedstaaten vor, das „Europäische Forum für Sicherheitsforschung und Innovation“ (ESRIF)[1] einzurichten.

Das Forum erhielt den Auftrag, eine „Agenda für Sicherheitsforschung und Innovation“ für die Europäische Union zu entwickeln: einen strategischen Fahrplan für Sicherheitsforschung und Innovation, der darauf ausgerichtet ist, auf der Ebene der EU, der Mitgliedstaaten und der Regionen mehr Kohärenz und Effizienz auf diesem Gebiet zu erzielen. Sein Schwerpunkt geht über Forschung und Entwicklung hinaus und führt das „I“ für Innovation in die Europäische Agenda ein. Seine Ausrichtung auf Innovation und die Umsetzung von

[1] KOM(2007) 511 endgültig.

Sicherheitstechnologien erwies sich im aktuellen Zusammenhang der weltweiten ökologischen und wirtschaftlichen Herausforderungen sogar als noch wichtiger.

Am 23. November 2009 verabschiedete das ESRIF seine wichtigsten Ergebnisse und Empfehlungen (nähere Informationen über das ESRIF und seine Konzepte sind in der Zusammenfassung des ESRIF-Abschlussberichts im Anhang enthalten).

Diese Mitteilung enthält die **erste Stellungnahme der Kommission zu den wichtigsten Ergebnissen und Empfehlungen des ESRIF**.

2. DIE GESELLSCHAFTLICHE DIMENSION DER SICHERHEIT

Das ESRIF gründete sein Konzept der Sicherheitsforschung zurecht auf der Auffassung, dass Sicherheit zuallererst ein menschliches und gesellschaftliches Phänomen ist. Menschen sind nicht nur Ziele und Opfer von Angriffen und Bedrohungen der Sicherheit, sondern auch Retter, Entscheidungsträger und diejenigen, die auf Sicherheitsbedrohungen reagieren.

Um diesen Herausforderungen zu begegnen, müssen alle Sicherheitslösungen auf den europäischen Werten Freiheit und Gerechtigkeit und den grundlegenden ethischen Prinzipien und rechtlichen Anforderungen beruhen, die bei allen sicherheitsrelevanten FuE- und Innovationstätigkeiten berücksichtigt werden. Dies bedeutet:

a) Stärkung der rechtlichen und ethischen Dimension

Es kann keine Sicherheitsmaßnahmen geben ohne Wahrung der Rechte und Freiheiten des Einzelnen, insbesondere des Schutzes der Privatsphäre der Bürgerinnen und Bürger. Sicherheitsmaßnahmen müssen legitim und verhältnismäßig sein, um von der Gesellschaft akzeptiert zu werden, und sie müssen stets nach den Regeln der Rechtsstaatlichkeit angewandt werden. Grundlegende ethische Prinzipien und Datenschutzanforderungen an Sicherheitsmaßnahmen müssen die Basis für die Entwicklung und Durchführung von Sicherheitsprogrammen bilden. Das ESRIF verlangt, dass Anforderungen im Zusammenhang mit dem Schutz der Privatsphäre neben den Anforderungen für die Verbesserung der Sicherheit stehen sollten, und zwar vom frühesten Stadium der Erwägung neuer Sicherheitslösungen an. Es bezeichnet dies als eingebauten oder konzeptionsintegrierten Datenschutz („Privacy by design“).

Ein solches Konzept, das von der Kommission begrüßt wird, wird weitreichende Folgen für den gesamten Forschungs- und Innovationszyklus haben.

b) Stärkung der gesellschaftlichen Dimension

Einer weiteren gesellschaftlichen Dimension muss vom Standpunkt der Technologieeffizienz aus Rechnung getragen werden. Keine Sicherheitstechnologie kann ohne die aktive Beteiligung (und Akzeptanz) der breiten Öffentlichkeit langfristig eine wirkliche Sicherheitslösung sein. In der Tat argumentiert das ESRIF, dass ein gesellschaftliches Sicherheitskonzept eine Vision der Sicherheit beinhaltet, die sich nicht auf Prävention und Schutz egal zu welchen Kosten konzentriert, sondern sich vielmehr in der Fähigkeit unserer Gesellschaften ausdrückt, Risiken – und manchmal auch Verlusten – gegenüberzutreten und damit fertig zu werden. Eine solche „gesellschaftliche Widerstandsfähigkeit“ hängt ebenso stark vom freien Willen der informierten Bürgerinnen und Bürger ab wie von der Qualität der

technischen Systeme und den Möglichkeiten der Unternehmen und Verwaltungen zur Gewährleistung der Funktionsfähigkeit.

Um Widerstandsfähigkeit zu erzielen, sind spezifische, an die breite Öffentlichkeit gerichtete Programme erforderlich, um für Bedrohungen zu sensibilisieren, das Verständnis der Prozesse zu verbessern, die eingeführt wurden, um Herausforderungen zu begegnen und um die Akzeptanz von Sicherheitslösungen zu diskutieren. Spezifische Maßnahmen unter Einbeziehung der Medien haben Priorität. In Übereinstimmung mit dem ESRIF-Bericht sind weitere Forschungsmaßnahmen zu den Beziehungen zwischen neuen Technologien und Bürger- und Menschenrechten erforderlich.

3. VERBESSERUNG DER WETTBEWERBSFÄHIGKEIT DER EUROPÄISCHEN SICHERHEITSINDUSTRIE

Die EU-Sicherheitsindustrie mit einem geschätzten Marktwert (2008) von 26 bis 36 Milliarden Euro[2] wächst schnell und verfügt über hochqualifizierte Arbeitskräfte sowie einen hohen Anteil an Forschung und Entwicklung. Das ESRIF empfiehlt eine „starke und unabhängige technologische und wissenschaftliche Grundlage für die EU zu schaffen, um die Interessen ihrer Bürgerinnen und Bürger zu wahren und sicherzustellen, dass ihre Industrie in der Lage ist, wettbewerbsfähige Produkte und Dienstleistungen bereitzustellen“. Es empfiehlt, dass die EU die führende Position auf dem Sicherheitsmarkt anstreben sollte und unterstützt die Idee einer Leitmarktinitiative im Sicherheitssektor.

Dies setzt allerdings voraus, dass wir heute in eine ehrgeizige Industriepolitik für den Sicherheitssektor investieren müssen, damit wir morgen Innovation und Wachstum ernten können.

a) Die Marktzersplitterung überwinden

Die Sicherheitsindustrie in Europa muss wettbewerbsfähiger und effizienter werden. Bisher litt die Branche unter der Zersplitterung der Märkte, die dazu führte, dass diese eine nationale oder gar regionale Ausrichtung hatten. Ihre geringe Größe führte zu Ineffizienz und einer geringen Kostenwirksamkeit sowohl für die Industrie als auch für die Endnutzer. Dies stellt eine große Hürde auf dem Weg zu Interoperabilität und Integration von Sicherheitslösungen auf nationaler und europäischer Ebene dar. Die Schaffung europaweiter Märkte als Lösung dieses Problems wird zu einer Verbesserung der Wettbewerbsfähigkeit und Attraktivität der Industrie auf globaler Ebene und zu einer größeren Effizienz der öffentlichen Ausgaben führen.

(i) Zertifizierung, Validierung und Normung

Ausgehend von den Anforderungen der Endnutzer und den Forschungsergebnissen müssen neue Technologien und Lösungen nicht nur validiert werden; sie sollten auch zertifiziert und gegebenenfalls genormt werden, um zu einer wirkungsvollen

[2] Die Sicherheitsindustrie umfasst die traditionelle Sicherheitsindustrie (basierend auf der Bereitstellung allgemeiner Sicherheitsanwendungen, z. B physische Zugangskontrollen), die sicherheitsorientierte Rüstungsindustrie (basierend auf der Nutzung von Rüstungstechnologien in Sicherheitsanwendungen oder durch den Erwerb und die Umformung ziviler Technologien zu Sicherheitsanwendungen) sowie Neuzugänge, d. h. hauptsächlich Unternehmen, die ihre vorhandenen (zivilen) Technologien auf Sicherheitsanwendungen ausdehnen, wie beispielsweise IT-Unternehmen.

Reaktion auf Sicherheitsrisiken beitragen zu können. FuE-Aktivitäten sollten mit einer klaren Validierungs- und Beschaffungsstrategie verknüpft werden, die den einschlägigen politischen Fragen sowie den wirtschaftlichen Interessen Rechnung trägt. Dies sollte die Herausbildung eines europäischen Sicherheitsmarktes und eine bessere Zusammenarbeit zwischen Interessenträgern im Sicherheitsbereich auf nationaler und europäischer Ebene fördern. Das ESRIF empfiehlt, dass die Kommission die Anwendbarkeit und Effizienz eines „europäischen Sicherheitskennzeichens" bewerten sollte.

CEN und ETSI[3] haben mit der Normungsarbeit im Sicherheitsbereich begonnen. CEN konzentriert sich zunächst auf eine Reihe von Fragen, für die es Normungsaufträge erhalten hat (insbesondere zur Sicherheit der Lieferkette, zum Schutz kritischer Infrastrukturen und zur sicheren Gestaltung von Produkten als Schutz gegen Kriminalität). Normen können ein wirksames Mittel zum Transfer von Forschungsergebnissen auf innovative Produkte sein, und deshalb wird erwartet, dass die Arbeiten im Zuge des 7. Rahmenprogramms zu weiterer Normungstätigkeit führen werden. Diese Arbeiten müssen beschleunigt werden.

In der Zwischenzeit prüft die Kommission Wege zur Erprobung der Ergebnisse relevanter Forschungsmaßnahmen, um zukünftige Zertifizierungsmechanismen zu entwickeln. Mit solchen Mechanismen sollte das Ziel verfolgt werden, die Übereinstimmung von Sicherheitsprodukten und -verfahren mit den einschlägigen Normen zu zertifizieren.

(ii) Regulierungsrahmen

Das ESRIF hat darauf hingewiesen, dass angesichts der Zersplitterung des Sicherheitsmarktes, die oft auf abweichende nationale Rechtsvorschriften zurückzuführen ist, ein harmonisierter Regulierungsrahmen in bestimmten Bereichen in Kombination mit einer frühzeitigen Koordinierung ratsam wäre. Die Kommission hält dies für einen ersten Schritt; eine umfassende Analyse des bestehenden Regulierungsrahmen ist erforderlich.

(iii) Interoperabilität

Die gemeinsame Nutzung von Anlagen und Informationen stärkt unsere Möglichkeiten zur Bewältigung komplexer grenzüberschreitender Sicherheitsprobleme. Der Austausch von Informationen zwischen nationalen Behörden und anderen europäischen Akteuren ist wesentlich für die Bekämpfung von grenzüberschreitender Kriminalität. Jedoch wird heute dieser Informationsaustausch durch die mangelnde technische und organisatorische Interoperabilität behindert. Es besteht daher ein dringender Bedarf an der Entwicklung von Normen im Bereich der Interoperabilität.

b) Stärkung der industriellen Basis

Die Europäische Union benötigt eine starke industrielle und technologische Basis, um den Bürgern innerhalb und außerhalb der EU moderne Sicherheitslösungen zu bieten. Die

[3] http://www.cen.eu/CENORM/sectors/sectors/security+and+defence/security/index.asp
http://www.etsi.org/WebSite/Technologies/Security.aspx

folgenden Themen müssen in Angriff genommen werden, um die industrielle und technologische Basis des europäischen Sicherheitssektors zu stärken.

(i) Kartierung der industriellen Basis des Sicherheitssektors

Um ein genaues Bild der technologischen und industriellen Basis des europäischen Sicherheitssektors (ESTIB) zu erhalten, müssen diese Kompetenzen unbedingt kartiert werden. Eine solche Kartierung wird die Feststellung der Stärken und Schwächen der ESTIB und die Ermittlung angemessener Maßnahmen im Hinblick auf die Stärkung der ESTIB ermöglichen. Dabei sollte den KMU besondere Aufmerksamkeit geschenkt werden. „Kritische Sektoren des verarbeitenden Gewerbes" (beispielsweise elektrische Ausrüstungen usw.) – die im verarbeitenden Gewerbe eine ähnliche Rolle spielen wie die kritischen Infrastrukturen im Infrastrukturbereich – sollten ebenfalls besonders berücksichtigt werden.

(ii) Innovationspolitik

Der Schwerpunkt der Innovationspolitik liegt auf der Umwandlung von Wissen in neue Produkte und Methoden und gleichzeitig in wirtschaftliche Werte und kommerziellen Erfolg[4]. Dies gilt besonders für sicherheitsbezogene FuE. Die Kommission wird daher untersuchen, inwieweit die innovativsten Sicherheitssektoren in die Leitmarktinitiative eingebracht werden sollten.

Darüber hinaus ist die vorkommerzielle Auftragsvergabe ein nützliches Hilfsmittel, um die Beschaffung innovativer Produkte und Technologien[5] zu fördern. Die Kommission wird weiter untersuchen, wie die vorkommerzielle Auftragsvergabe im Sicherheitsbereich vorangetrieben werden kann. In Bezug auf das öffentliche Auftragswesen fällt die Beschaffung sowohl von Verteidigungsgütern als auch von sicherheitsempfindlichen Gütern in den Anwendungsbereich der Richtlinie 2009/81/EG[6]. Die Kommission wird Vorschläge für die Gewährleistung einer transparenten und harmonisierten Anwendung dieser Richtlinie auf dem Gebiet der Sicherheit vorlegen.

(iii) Konzeptionsintegrierte Sicherheit („Security by design")

Das ESRIF empfiehlt „die Förderung eines Konzepts der konzeptionsintegrierten Sicherheit (*„Security by design"*) für alle neu entwickelten komplexen Systeme oder Produkte, wobei sicherzustellen ist, dass die Sicherheit schon bei der Konzeption berücksichtigt wird, so wie dies bereits beim Konzept der Auslegungssicherheit (*„Safety by design"*) geschieht".

Die Kommission begrüßt diese Empfehlung und wird prüfen, mit welchen Mitteln sichergestellt werden kann, dass bei Forschungsmaßnahmen mit potenziellen Sicherheitsauswirkungen diese gegebenenfalls immer vom frühestmöglichen Zeitpunkt an berücksichtigt werden.

(iv) Synergien zwischen zivilen und militärischen Technologien

---

4 KOM(2005) 488 endgültig.
5 KOM(2007) 799 endgültig.
6 ABl. L 216 vom 20.8.2009.

Die sich entwickelnde Beziehung zwischen den militärischen Technologien einerseits und den Sicherheitstechnologien andererseits ist besonders im FuE-Bereich zu bemerken, wo Technologien potenzielle Entwicklungen in beiden Bereichen aufweisen.

Komplementarität und Zusammenarbeit müssen in bestimmten Bereichen, wo Technologien sowohl zivil als auch militärisch angewandt werden können, beispielsweise im Bereich der Grenzkontrollen und der Sicherheit im Internet, verstärkt werden. Auf der Grundlage eines bei der Tagung des Europäischen Rates im Dezember 2008 erfolgten Aufrufs zur weiteren Stärkung der Synergien zwischen Aktivitäten, die im Rahmen des FuE-Programms durchgeführt werden, und dem Rüstungsbereich muss eine enge Zusammenarbeit mit der Europäischen Verteidigungsagentur (EDA) sichergestellt werden.

4. IN DIE ZUKUNFT INVESTIEREN

Das ESRIF hat in seiner Europäischen Agenda für Sicherheitsforschung und Innovation (ESRIA) einen Fahrplan für die sicherheitsbezogene FuE für die nächsten 15 Jahre vorgelegt, der auch systemische Anforderungen enthält. Es ist zu unterscheiden zwischen FuE-Maßnahmen und Maßnahmen, die sicherstellen sollen, dass technologische Fortschritte, die durch FuE erzielt werden, zum tatsächlichen Einsatz dieser neuen Technologie führen.

a) Sicherheitsaufgaben und –prioritäten im FuE-Bereich

Im Hinblick auf FuE hat das ESRIF darauf hingewiesen, dass die wichtigsten, in RP 7 genannten Forschungsmaßnahmen zur Unterstützung der Sicherheitsaufgaben auch in naher Zukunft gültig bleiben. Längerfristig müssen sie neu geprüft und möglicherweise verstärkt und erweitert werden.

Das ESRIF wies darauf hin, dass es nicht möglich ist, Risiken für die Sicherheit Europas genau vorherzusagen, egal, ob es sich um vom Menschen verursachte oder um natürliche Gefahren handelt. Die FuE im Sicherheitsbereich muss sich daher auf die Stärkung der europäischen Widerstandsfähigkeit gegenüber Risiken und der Fähigkeit, mit Krisen umzugehen, konzentrieren. Dazu gehört auch die Verbesserung der Kohärenz und der Robustheit gesellschaftlicher Systeme und ihrer Schnittstellen mit Technologien. In diesem Zusammenhang empfahl das ESRIF, die Forschung über den Schutz kritischer Infrastrukturen zu verstärken und zu erweitern, beispielsweise im Hinblick auf Forschungsarbeiten im Zusammenhang mit der Energieversorgungssicherheit und der Sicherheit der Verkehrsnetze[7].

(i) Weiterentwicklung der Prioritäten

Die Europäische Agenda für Sicherheitsforschung und Innovation (ESRIA) deckt das vollständige Spektrum der FuE-Unterstützung für aktuelle Sicherheitsaufgaben ab. Es ist in fünf Gruppen unterteilt (siehe Zusammenfassung des ESRIF-Berichts im Anhang).

Die Kommission nimmt zur Kenntnis, dass das ESRIF in der gesamten ESRIA die Notwendigkeit eines integrativen Konzepts betont, egal ob es sich auf Explosiv- oder

[7] Siehe Richtlinie 2008/114/EG des Rates.

CBRN-Stoffe, kritische Infrastrukturen oder Krisenmanagement bezieht: die ESRIA legt den Schwerpunkt auf das Ganze, nicht auf die Teile, und weist auf die Bedeutung von Netzwerken, Referenzzentren, Interoperabilität und Systemen von Systemen hin. So empfiehlt das ESRIF beispielsweise, Vorkehrungen dafür zu treffen, „den vorhersehbaren Bedarf an europaweiten netzwerkgestützten Fähigkeiten und komplexen Systemen decken zu können, der im Bereich von Frühwarnsystemen für und der Reaktionsbereitschaft auf durch den Menschen hervorgerufene oder natürliche Vorfälle entstehen wird."

Es spricht sich für Innovation aus und unterstützt ein „ganzheitliches Konzept" des Grenzschutzes, wie es von der EU und ihren Mitgliedstaaten in der Tat bereits im vierstufigen Schengen-Modell der Zugangskontrolle[8] entwickelt wurde, das den Kern der integrierten Grenzkontrolle bildet. Das ESRIF weist auf die Bedeutung der Interoperabilität hin und vertritt die Auffassung, dass die „Forschung die Aspekte der technischen Interoperabilität zwischen errichteten Systemen sowie die Interoperabilität auf organisatorischer Ebene abdecken und dabei die kulturellen Unterschiede berücksichtigen muss, die beim Überschreiten von Grenzen zum Tragen kommen. Die Interoperabilität kann auch durch harmonisierte oder gemeinsame operationelle Verfahren für Entwicklung, Beschaffung und Ausbildung verbessert werden."

Das ESRIF ist der Ansicht, dass Informations- und Kommunikationstechnologien „von wesentlicher Bedeutung für die europäische Sicherheit sind, denn sie sind selbst kritische Infrastrukturen und schaffen darüber hinaus die Voraussetzungen für andere Dienstleistungen und Sektoren", insbesondere bezogen auf den Forschungsbedarf zur Erhöhung der systemischen Widerstandsfähigkeit. Das ESRIF befürwortet die Erforschung rechtlicher Rahmenbedingungen zur Unterstützung von Forensik und Beweismittelsicherung im IKT-Bereich.

Das ESRIF hat die Rolle des Weltraums als „wesentlich für bestimmte sicherheitsbezogene Technologiebereiche" bezeichnet und auf die Bedeutung von GMES und Galileo bei der Bereitstellung „einer breiten Palette von Mehrwertdiensten zur Unterstützung der Sicherheit" hingewiesen, unter Bezugnahme auf das Erfordernis, weltraumgestützte Systeme zu schützen.

Die Kommission begrüßt dieses umfassende Konzept der Sicherheitsforschung und Innovation.

(ii) Künftige Aufgaben

Einige der Sicherheitsaufgaben, die vom ESRIF hinsichtlich der dafür erforderlichen Fähigkeiten und der damit zusammenhängenden Forschungsbemühungen analysiert wurden, werden derzeit eingehend geprüft. Dies trifft unter anderem auf die Grenzüberwachung und –kontrolle, den Schutz kritischer Infrastrukturen, z. B. IKT, die CBRN-Schutz-Politik, Maßnahmen zur Verbesserung der Sicherheit von Sprengstoffen und Zündmitteln oder die Überprüfung von Waren und Passagieren

[8] Dabei handelt es sich um die folgenden vier Stufen: Maßnahmen in Drittstaaten, Zusammenarbeit mit den Nachbarländern, Grenzkontrollen sowie Überwachungsmaßnahmen im Raum der Freizügigkeit einschließlich Zurückweisung.

zu. Eine weitere Präzisierung dieser Sicherheitsbereiche wird in dem künftigen Aktionsplan von Stockholm (Stockholm Action Plan) vorgenommen werden

Bedrohungen der IKT-Sicherheit finden sich in unterschiedlichen Politikbereichen und Lösungen sind dementsprechend im Kontext der Informationssystemarchitektur der künftigen EU-Strategie der inneren Sicherheit zu finden.

Das ESRIF stellte fest, dass sein Auftrag manche Forschungsthemen, die in den nächsten Jahren mit Sicherheit an Bedeutung gewinnen werden, nicht umfasste. Dies betrifft vor allem einige Aufgaben der äußeren Sicherheit. Das ESRIF empfahl, „der äußeren Dimension der Sicherheit hohe Priorität einzuräumen", in Anbetracht der Tatsache, dass „Forschungs- und Innovationsprogramme die Maßnahmen zum Zwecke der Friedenserhaltung, das Management humanitärer Aktionen und von Krisensituationen einschließlich gemeinsamer Maßnahmen mit anderen Regionen und internationalen Organisationen, insbesondere im Hinblick auf die Entwicklung globaler Normen" unterstützen sollten.

Die Kommission ist der Ansicht, dass es sich hierbei zwar in der Tat um Bereiche handelt, die sich weiterentwickeln, es aber dennoch angebracht ist, Überlegungen zur Erweiterung der Sicherheitsforschungs- und –entwicklungsprogramme auf Bereiche wie Katastrophenschutz, Konfliktprävention und die Stabilisierung nach Krisen auszudehnen.

– Katastrophenschutz: Der Katastrophenschutz und damit die Sicherheitsforschung zur Unterstützung von Katastrophenschutzmaßnahmen gewinnen tendenziell an Bedeutung, nicht zuletzt in Anbetracht des Klimawandels; dies wurde in einem Papier des Hohen Vertreters und der Europäischen Kommission an den Europäischen Rat dargelegt, in dem der Klimawandel als „Bedrohungsmultiplikator"[9] bezeichnet wird. Das Papier fordert die Verbesserung der EU-Forschungskapazitäten im Hinblick auf die Verknüpfung von Sicherheit und Klimawandel. Überdies betonte die Kommission in ihrer Mitteilung „Stärkung der Katastrophenabwehrkapazitäten der Europäischen Union" die Notwendigkeit, die Verhütung von Katastrophen, die Folgenbegrenzung, die europäischen Katastrophenschutzkapazitäten und die wertvolle Unterstützung, die die Forschung leisten kann, zu verbessern.

– Konfliktprävention und Stabilisierung nach Krisen: Die Gemeinschaft hat über das Instrument für Stabilität[10] bereits operationelle Mittel bereitgestellt. Das Instrument für Stabilität soll wesentliche Voraussetzungen für die richtige Umsetzung der Entwicklungspolitik der Gemeinschaft bei oder kurz vor Ausbruch von Krisen schaffen oder wiederherstellen und dabei helfen, Kapazitäten zum Vorgehen gegen spezifische globale oder regionenübergreifende Gefahren aufzubauen und den Aufbau von Kapazitäten für die Bewältigung von Situationen vor und nach Krisen gewährleisten. Auf Gemeinschaftsebene fehlen jedoch die Forschungsmittel zur Finanzierung dieser Maßnahmen.

b) Über Forschung und Entwicklung hinaus

---

9 Siehe 7249/08 vom 3.3.2008 sowie die Mitteilung der Kommission „Stärkung der Katastrophenabwehrkapazitäten der Europäischen Union", KOM(2008) 130 endgültig.

10 Verordnung (EG) Nr. 1717/2006, ABl. L 327 vom 24.11.2006, S. 1.

(i) Einbeziehung der Endnutzer

Das ESRIF riet zur „engen europaweiten Zusammenarbeit zwischen Interessenträgern der Angebots-, Nachfrage- und Endnutzerseite über die Planung, Durchführung und Überprüfung der Sicherheitsforschungspolitik hinaus“, stellte jedoch auch fest, dass die Regierungen und Endnutzer eine „organisatorische Umstrukturierung zur Gestaltung und Reaktion auf die Innovation im Sicherheitsbereich“ vornehmen müssen.

Die Kommission teilt die Auffassung, dass häufig der Bedarf besteht, dass die – öffentlichen wie privaten – Endnutzer weitere Anstrengungen unternehmen müssen, um ihre Wissensgrundlage über Sicherheitstechnologie und ihre Fähigkeiten zur prospektiven Analyse zu stärken, damit sie die Gelegenheit nutzen und sicherstellen können, dass zukünftige Lösungen auf ihren tatsächlichen Bedarf zugeschnitten werden, beispielsweise durch Demonstrationsmodelle.

(ii) Zukünftige Programme zur Verbreitung innovativer Lösungen

Die Kommission hat bereits darauf hingewiesen, dass es sinnvoll wäre, in die operationellen Aspekte der Sicherheit zu investieren, insbesondere in einer Reihe von Bereichen, in denen nationale und internationale Behörden technologische Lösungen anwenden[11]. Das ESRIF ist der Auffassung, dass der Erfolg auf dem globalen Markt stark von den EU-Vergabevorschriften abhängt und empfiehlt, die vorkommerzielle Auftragsvergabe für innovative Lösungen in großem Umfang zu nutzen.

Das ESRIF unterstützt die Entwicklung eines Modells auf der Grundlage eines strategischen und koordinierten Konzepts der transeuropäischen Koordination. Es nennt die transeuropäischen Netze als Beispiel, die als Vorbild für die EU-weite systemische Integration im Sicherheitsbereich erwogen werden sollten. Wie im Falle der TEN würden Mittel zur Aufstockung nationaler Finanzmittel bereitgestellt werden, um die Kritischen Europäischen Infrastrukturen abzusichern. In Anbetracht der Tatsache, dass die für Forschung und technologische Entwicklung zur Verfügung stehenden Mittel ausgeschöpft werden müssen, um den Erwartungen der Nutzer voll zu entsprechen, stellte das ESRIF fest, dass ein solcher Prozess durch die Einrichtung eines Fonds für innere Sicherheit unterstützt werden kann.

(iii) Aus- und Fortbildung

Das ESRIF weist darauf hin, dass es wichtig ist, die forschungsbezogene Aus- und Fortbildung zu verknüpfen und ist der Auffassung, dass alle Interessenträger dafür zuständig sind. Sicherheitsbeauftragte, politische Entscheidungsträger, Vollzugsbehörden, Zivilgesellschaft, Industrie, Forschungseinrichtungen, Hochschulen und Medien. Es sprach sich für neue, an die breite Öffentlichkeit gerichtete Sensibilisierungsprogramme aus, um das Bewusstsein für Gefahren, Risiken und Schwachstellen zu schärfen und ihr Verständnis der politischen Maßnahmen und der technologischen Lösungen zu verbessern, die für die Sicherheit erforderlich sind.

[11] KOM(2008) 68 endgültig, KOM(2008) 130 endgültig, KOM(2009) 262 endgültig.

5. UMSETZUNG DER EUROPÄISCHEN AGENDA FÜR SICHERHEITSFORSCHUNG UND INNOVATION (ESRIA)

Die Empfehlungen des ESRIF im Hinblick auf die Governance betreffen die ständige Aktualisierung der ESRIA und die engere Einbeziehung aller Interessenträger. Das ESRIF empfiehlt, dass *ein transparenter, alle Interessenträger einbeziehender Mechanismus geschaffen werden sollte, um die ESRIA ausgewogen und rigoros umzusetzen.*

Da Sicherheitsforschung benutzerorientiert und fähigkeitsgesteuert ist stellt das ESRIF fest, dass ein Bedarf an angemessenen Schnittstellen und Austauschmechanismen zwischen der Endnutzergemeinschaft und der Forschung und Industrie besteht.

6. FAZIT

Dies ist eine erste Reaktion der Kommission auf den ESRIF-Abschlussbericht. Die Kommission misst den Ergebnissen der Arbeit des ESRIF große Bedeutung bei und begrüßt ihre strategische Ausrichtung. Sie nimmt die darin enthaltenen Empfehlungen zur Kenntnis und hebt folgende Punkte hervor, die die nächste Kommission gegebenenfalls noch eingehender analysieren könnte:

- die Rolle der Agentur der Europäischen Union für Grundrechte[12][13] in Bezug auf die Forschung hinsichtlich des Verhältnisses von einerseits Sicherheit und andererseits Privatsphäre und Datenschutz;

- die Notwendigkeit einer verstärkten „ethischen Überprüfung“ von Projekten, die unter den Themenbereich „Sicherheit“ des 7. RP fallen, und einer möglichst weiten Verbreitung der Ergebnisse laufender F&E-Projekte im Bereich der Sicherheit

- die gesellschaftliche Dimension als automatisch zu erwartende Folge für alle ihre Ausschreibungen im Themenbereich „Sicherheit“ des 7. RP;

- die mögliche Aufnahme der innovativsten Sicherheitsbereiche in die Leitmarktinitiative;

- Möglichkeiten der Beschleunigung der vorkommerziellen Auftragsvergabe im Sicherheitsbereich;

- Möglichkeiten für eine Beschleunigung der Zertifizierung, Validierung und gegebenenfalls der Normung im Sicherheitsbereich, insbesondere im Hinblick auf die Anwendbarkeit und Effizienz eines „Europäischen Sicherheitskennzeichens“;

- Ausloten der geeignetsten Reaktionsmöglichkeiten auf vorhersehbare neue Sicherheitsaufgaben und Prioritäten, entweder innerhalb des laufenden 7. RP oder als Vorbereitung des künftigen Rahmenprogramms;

- auf der Ebene der EU und der Mitgliedstaaten: bessere Verknüpfung der europäischen Sicherheitsforschung und –entwicklung mit jenen Sicherheitsaspekten, die die operative Seite stärker berücksichtigen;

---

12 Beschluss des Rates Nr. 2008/203/EG, ABl. L 63 vom 7.3.2008.

13 Verordnung (EG) Nr. 168/2007 des Rates, ABl. L 53 vom 22.2.2007.

- Einrichtung einer ständigen Arbeitsstruktur zur Umsetzung der ESRIF-Empfehlungen;

- Möglichkeit der Einrichtung eines Forums zur Stärkung der Wettbewerbsfähigkeit der Sicherheitsindustrie im Bereich von Forschung und Entwicklung, beispielsweise einer Hochrangigen Gruppe bestehend aus Vertretern von Interessengruppen des öffentlichen und privaten Sektors sowie der Zivilgesellschaft.

Annex: Executive Summary of the ESRIF Final Report

Europe stands on the threshold of a new global approach to security – and of ways to use scientific research and innovation to reinforce and implement that new thinking

The security of Europe and its citizens is linked to internal and external events and threats, as well as to the increasing convergence of civil and defence capabilities. Above all, it derives from societal imperatives that demand a balancing of the state's policy and technological exigencies with privacy rights, European cultural values and the tenets of democracy.

ESRIF, the European Security Research and Innovation Forum, has spent the past two years analyzing the medium and long-term challenges that Europe faces. These range from natural disasters to organised crime to man-made incidents, whether small-scale in impact or those with potential "mass disruption" effects.

Assisted by more than 600 experts, ESRIF and its 64 members from 31 countries have examined the full range of such threats and tied them to the EU's central civil security missions and to the capabilities required to carry them out.

This collective effort has resulted in a set of key messages that encompass the logic and necessity of future European security and its related research. These messages point to the essence, as ESRIF sees it, of what security research and innovation should flow from – and what it should deliver to society.

Security research should be grounded in an industrial policy that frames a systematic approach to capability development which, in turn, promotes interoperability among the 27 EU nations and establishes common standards. Ultimately this effort must increase societal security in a globalised world, while fostering trust between European citizens, governments and national and European institutions. These and other ideas are among ESRIF's main recommendations included in this executive summary.

To reach an interoperable, trust-embedded and resilient society, however, Europe needs an R&D roadmap, and a mechanism should be set up to implement it in a balanced and rigorous manner. ESRIF thus proposes its European Security Research and Innovation Agenda – "ESRIA" which should go a long way toward achieving that goal.

A research and innovation agenda cannot be created and implemented in a vacuum.

The framework is defined by principles given in the **Key Messages**:

Societal Security

Human beings are at the core of security processes.

Societal Resilience

Certain risks cannot be catered for, nor avoided. Societies must prepare to face shocks and must have the ability to recover.

Trust

Assuring security implies nurturing trust among people, institutions and technologies.

Awareness raising through education and training

Security is a common responsibility of all stakeholders, the citizen is at the fore front.

Innovation

Europe can only rely on its own scientific, technological and industrial competences.

Industrial policy

A competitive European security industry is a prerequisite for future security. The EU must address the fragmentation of its security markets.

Interoperability

A seamless approach to security is essential for Europe; Interoperability is essential to allow security forces to work together.

A systematic approach to capability development

The increasing complexity of security, demands increasing sophistication of our Response.

Security by design

Security features must become integral part of any given system: Europe's society needs a systemic approach to security.

ESRIF has defined a **European Security Research and Innovation Agenda** (ESRIA) that identifies and roadmaps key capabilities and research needs in line with the main work results.

The ESRIA has been organized into **five content clusters** and differentiates research topics according to short-, medium- or long-term needs:

The first cluster centres on the classic event cycle of prevention, protection, preparing, responding and recovering. It focuses on the securing of people, civil preparedness and crisis management.

The second cluster deals with the countering of different means of attack, as a way of dealing with specific, known and projected future risks. It examines ways to detect and identify conventional as well as non-conventional attacks, unintended impacts of other actions, and naturally occurring incidents, to mitigate their effects, and it analyzes potential dangers inherent to coming technologies.

The third cluster aims at securing critical assets, such as energy, transport and other crucial infrastructures. It examines security economics and outlines the necessity to analyze and cope with limited access to critical natural resources as well as securing the existence of key manufacturing capabilities and capacities in Europe.

The fourth cluster is about securing identity, access and movement of people and goods. It mainly centres on border security and secure identity management.

Lastly, the fifth cluster lists additional enabling capabilities of special interest, due to cross-cutting characteristics or prior political strategic decisions. The crucial role of Information and Communication Technologies (ICT) is examined, as are security implications of European space programmes.

ESRIF strongly recommends that the EU and its Member States launch new measures to enhance the security of its citizens. These should also aim to create amenable conditions for European excellence in research and innovation, and thus advance Europe's security. The below sets out policy and operational recommendations for achieving stronger security research and innovation results:

COMMON EUROPEAN CAPABILITIES

The EU must draw on its collective strengths and knowledge by developing common capability via enhanced transnational co-operation.

1. This calls for *close consultation across Europe* among supply, demand and end-user stakeholders across the planning, execution and review cycles of security research policy. The demand side in particular – governments and end-users – needs organisational re-alignment to both shape and respond to security innovation.

2. *Resources and incentives* are essential to developing common capability. ESRIF recommends, notably with a view to the implementation of ESRIA, that the EU maintains the current rate of growth of its security research programmes – with the aim of reaching an annual budget of one billion euros as proposed in 2004 by the Group of Personalities. National programmes should reflect this degree of ambition. Regarding the necessary research and industrial synergies, technical compatibility and interoperability of new security solutions, a significant effort is required to ensure the coherence of national and EU efforts through enhanced coordination.

3. Research programmes should be complemented by additional implementation programmes. Success on the global market strongly depends on EU market procurement references. Pre-commercial procurement of innovative solutions should be exploited as a mechanism to bring research results closer to the market.

NEW POLICY INITIATIVES

The above should be supported by stronger articulation of demand, and delivery of the most appropriate solutions by the supply side.

4. New initiatives and programmes should include:

   – creation of knowledge centres such as CBRN expert groups to guide research

– preparations to meet foreseeable needs for pan-European network-enabled capabilities and complex systems in early warning and response readiness that deal with natural and man made incidents

– expanded critical infrastructure protection programmes

– evaluating the applicability and efficacy of the numerous initiatives available to the EU and its Members States such as: a Lead Market initiative, Trans European Networks for Security, the creation of an Internal Security Fund or a "European Security Label".

– the early engagement of all stakeholders and transparency of the regulatory environment, including standards to stimulate private sector investments in security research. If upcoming regulations are understood early on, a return on security investments can be foreseen and investments can thus be expected to take place.

INTEGRATED APPROACH TO SECURITY

Effective civil security must embrace interoperability, standardisation, certification, validation, communication with the public, education & training, exchange of best practices, consultations on privacy issues and other factors that cut across public and private spheres and provide synergies between civil security and defence research fields.

5. A *holistic approach* must include:

– efforts to ensure that the social, cultural, legal and political aspects of security research and development are taken into account. Research programmes should reflect relevant ESRIF key messages, and thus promote overall "societal coherence".

– the promotion of a *security by design* approach in any newly developed complex system or product, ensuring that security is addressed at the point of conception, as it has been the case for *safety by design*.

– programmes to raise societal awareness of security threats, risks and vulnerabilities – and the security and safety impact of emerging critical technologies.

THE GLOBAL DIMENSION

The EU's civil security is a collective responsibility touching government, societal organisations, industry and individual citizens. It cannot stand in isolation from the world.

6. The globally inter-related nature of security calls for:

– a strong and independent technological and scientific base for the EU to safeguard the interests of its citizens and ensure that its industry is able to provide products and services in a competitive manner.

– giving high priority to security's external dimension and closer home affairs/defence consultation. Research and innovation programmes should support peacekeeping, humanitarian and crisis management tasks, including joint initiatives with other regions and international organisations, notably as regard the development of global standards.

SECURITY RESEARCH: THE FUTURE

The proposed European Security Research and Innovation Agenda – ESRIA – should be seen as a living document.

7. For *ESRIA to evolve* with Europe's internal and external threat environments:

– A transparent mechanism involving all stakeholders should be set up to implement ESRIA in a balanced and rigorous manner.

– ESRIA should be revisited and evaluated on a regular basis with special attention to evaluating any measures flowing from ESRIF key messages.