Internationale Zusammenarbeit zur Bekämpfung von Gefahren für die Wirtschaft

Die Bedrohung durch den internationalen Terrorismus ist die größte Herausforderung für alle Sicherheitsbehörden weltweit. Die Nationalstaaten werden mit völlig neuartigen Bedrohungen konfrontiert, die ihre Handlungsfähigkeit zunehmend auf den Prüfstand stellen: Immer mehr wirken sich globale Entwicklungen auf lokaler Ebene aus und umgekehrt. Krisen, deren Auswirkungen wir spüren, können ihre Ursachen weitab von Deutschland haben – irgendwo in der Welt. Auch die neuen Verwundbarkeiten moderner Industriegesellschaften haben die Sicherheitsumgebung maßgeblich verändert.



PROF. DR. JÜRGEN STOCK
Vizepräsident beim
Bundeskriminalamt

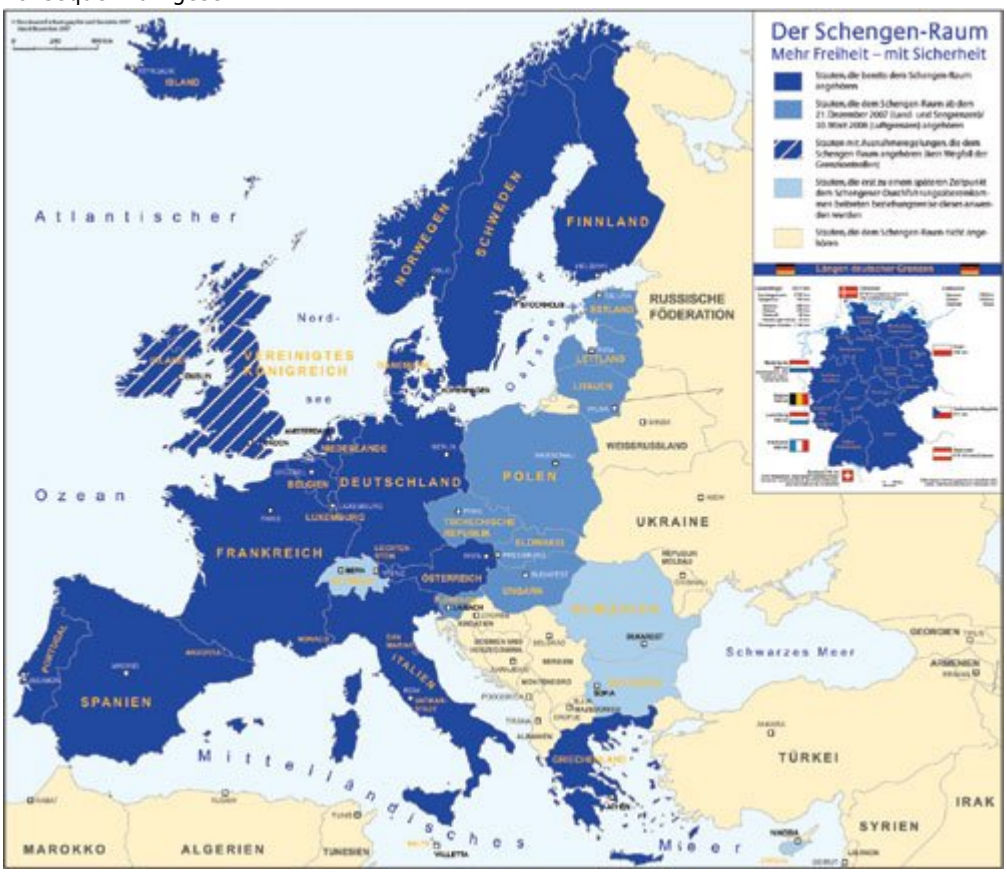
Bedrohungen für die Wirtschaft

Durch die rasante Verbreitung der Informations- und Kommunikationstechnologien im Zuge der Globalisierung hat sich Kriminalität verändert. Zwar sind die Unternehmen heute nach wie vor durch klassische Kriminalitätsfelder der Wirtschaftskriminalität, durch Eigentumsdelikte, Geldwäsche, Korruption, Produkt- und Markenpiraterie sowie Wirtschafts- und Industriespionage gefährdet. Hinzugekommen sind jedoch insbesondere neue Bedrohungen durch Kriminalitätsformen, die unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen werden - kurz bezeichnet als IuK-Kriminalität. Im Jahr 2007 sind die Fallzahlen der IuK-Kriminalität im engeren Sinne mit rund 34.000 Fällen um rund 17 Prozent gegenüber dem Vorjahr (29.155) gestiegen.
Bei Straftaten mit dem Merkmal „Tatmittel Internet„ registrierte die Polizei 2007 mit rund 180.000 Fällen eine Steigerung von acht Prozent gegenüber 2006 (165.720).
Der Anteil der Wirtschaftskriminalität daran lag bei ca. 10.000 Fällen, also rund fünf Prozent.
Die Zahlen verdeutlichen es: Wir verzeichnen einen deutlichen Trend hin zur Nutzung des Internets bei der Begehung von Wirtschaftsstraftaten. Diese Entwicklung hat sich in den letzen Jahren kontinuierlich fortgesetzt.
Gerade die Entwicklungen der Informationstechnik haben zu neuen Tatbegehungsweisen mit enormem Schadens-potenzial geführt. Gelangte z. B. Schadsoftware noch vor wenigen Jahren lediglich durch den Austausch infizierter Datenträger in Umlauf, wird sie heute mit vielfacher Geschwindigkeit über das Internet verbreitet. Durch die Vernetzung von IT-Systemen kommt es in kürzester Zeit zu globalen Epidemien mit erheblichen – nicht nur finanziellen – Auswirkungen.
Diese Gefahren werden u. a. potenziert durch die kriminelle Nutzung von über das Internet verbundenen, fernsteuerbaren Netzwerken von Computern, so genannten Bot-Netzen. So können beispielsweise durch DDoS-Angriffe (Distributed Denial of Service) mittels unzähliger unsinniger Anfragen ganze Internetportale lahmgelegt werden. Bot-Netze bilden die Infrastruktur für „moderne Straftaten„; angedrohte DDoS-Attacken bilden z. B. die Basis zukünftiger Erpressungsszenarien. Die Ausbreitung von Bot-Netzen steigt stetig an. Der IT-Sicherheit kommt damit eine herausragende Bedeutung zu. Das entsprechende Bewusstsein ist noch nicht überall verbreitet. Die Möglichkeiten, die das Internet für Kriminelle bietet, bringen Gefahren mit sich - für jeden Einzelnen, aber auch für die Gesellschaft insgesamt.
Weite Teile unseres Gemeinwesens sind nur noch dann arbeitsfähig, wenn die dahinter stehende Informations- und Kommunikationstechnik zuverlässig und sicher funktioniert. Der Schutz so genannter Kritischer Infrastrukturen, die sich zu ca. 80 % in privatwirtschaftlicher Hand befinden, gewinnt vor diesem Hintergrund, aber auch angesichts der Bedrohung durch den internationalen Terrorismus, zunehmend an Bedeutung.
Informationsangriffe mit erpresserischer Absicht auf Versorgungseinrichtungen, auf Verkehrsleitzentralen und auch auf Sicherheitsbehörden sind vorstellbar.
Deutsche Unternehmen sehen sich zudem, auch durch ihr verstärktes Auslandsengagement, vermehrt Risiken ausgesetzt – die Palette reicht von Entführungen bis hin zu terroristischen Anschlägen. Aktuelles Beispiel: Die Entführung eines Mitarbeiters einer deutschen Baufirma Anfang März 2008 in Nigeria, der glücklicherweise nach kurzer Zeit freigelassen wurde und unversehrt blieb.
Die Bedrohungsszenarien, denen wir uns als Sicherheitsbehörden ebenso wie die Wirtschaft zu stellen haben, sind vielfältig. Dabei haben klassische und neue Bedrohungen eins gemein: die internationale Dimension der Tatbegehung.

Internationale Zusammenarbeit

Innere Sicherheit kann schon lange nicht mehr ausschließlich aus nationaler Perspektive betrachtet werden. Sicherheit ist vielmehr das Ergebnis konsequenten international

abgestimmten Vorgehens. Nach unserer festen Überzeugung müssen wir der erkannten Netzwerkbildung auf Straftäterseite eine Vernetzung des sicherheitsbehördlichen Informationsaustausches und Handelns entgegen setzen. Das gleiche gilt natürlich für die private Organisation von Sicherheit, soweit sie einen internationalen Bezugsrahmen hat.
Die internationale polizeiliche Kooperation vollzieht sich regelmäßig auf den Ebenen bilateraler und multilateraler Zusammenarbeit.
In der bilateralen Zusammenarbeit spielen für Deutschland institutionalisierte Zusammenarbeitsformen, insbesondere mit unseren unmittelbaren Nachbarstaaten, eine tragende Rolle. Die unmittelbare polizeiliche Tätigkeit vor Ort steht dabei im Zentrum. Weitreichende bilaterale Polizeiverträge erlauben uns den wechselseitigen Einsatz von Polizeibeamten und den unkomplizierten zügigen Informationsaustausch, beispielsweise in gemeinsamen Grenzzentren.
In übergeordneterer Ebene genießt die Zusammenarbeit innerhalb der Europäischen Union für Deutschland Priorität. Eine sehr enge, institutionalisierte Kooperation in den Bereichen Justiz und Inneres zwischen mehreren europäischen Staaten sah erstmals das so genannte Schengener Durchführungsübereinkommen„ (SDÜ) vor. Es wurde von der Kerngruppe der „Schengener Vertragspartner„ unterzeichnet, die bereits am 14. Juni 1985 einen völkerrechtlichen Vertrag mit dem Ziel des schrittweisen Abbaus der Grenzkontrollen an den gemeinsamen Grenzen geschlossen hatten (Deutschland, Frankreich, Belgien, Niederlande, Luxemburg). Im SDÜ wurde vereinbart, die Kontrollen an den Binnengrenzen aufzugeben und im Gegenzug zur Aufrechterhaltung der Inneren Sicherheit eine Reihe von Ausgleichsmaßnahmen zu schaffen, u. a. die Einrichtung eines allgemeinen polizeilichen Informationsaustauschs und eines polizeilichen Rechtshilfeverkehrs sowie die Einräumung des Rechts auf grenzüberschreitende Observation und Nacheile. Das Herzstück der Ausgleichsmaßnahmen stellt die Einrichtung eines gemeinsamen elektronischen Fahndungssystems – des so genannten Schengener Informationssystems (SIS) dar. Heute umfasst der so genannte Schengen-Raum 24 Staaten. Der Kerngedanke des SDÜ „Freiheit im Inneren durch rigide Kontrollen an den Außengrenzen„ wird weiterhin mit hohem Engagement konsequent umgesetzt.



Quelle: „Der Schengen-Raum“, Veröffentlichung des BMI

Eine der wichtigsten zukunftsweisenden europäischen Initiativen ist der Vertrag von Prüm. Er wurde am 27. Mai 2005 von Belgien, Frankreich, Luxemburg, den Niederlanden, Österreich, Spanien und Deutschland mit dem Ziel unterzeichnet, den grenzüberschreitenden Fahndungsdruck zu erhöhen. Kernelement dieses Vertrags ist die Vernetzung von nationalen DNA-, Fingerabdruck- und Kraftfahrzeugregistern. Darüber hinaus wurden auch Regelungen zum Datenaustausch zur Bekämpfung des Terrorismus und des Phänomens reisender Gewalttäter (z. B. Hooligans) getroffen. Seit November 2006 ist der Vertrag in

Österreich, Spanien und Deutschland in Kraft, seit Mai 2007 in Luxemburg.
Deutschland, Österreich, Spanien und Luxemburg tauschen auf der Basis des Prümer Vertrags elektronisch DNA-Daten aus. Die Vorteile liegen auf der Hand, wie ein Blick auf erste Ergebnisse zeigt: Ein elektronischer Abgleich von rund 120.000 deutschen DNA-Spuren mit österreichischen, spanischen und luxemburgischen DNA-Spuren aus ungelösten Fällen führte allein auf der deutschen Seite zu über 3.600 Treffern, darunter 24 Fälle von Mord und Totschlag, 16 Sexualstraftaten und 151 Fälle von Raub und Erpressung.
Straftaten, die teils schon Jahre zurückliegen und bislang als unaufgeklärt galten, können so aufgeklärt werden. Der Beschluss der Innen- und Justizminister der EU vom 15. Februar 2007, die wesentlichen Bestimmungen des Vertrags von Prüm in den EU-Rahmen zu überführen, zeigt, in welche Richtung die grenzüberschreitende Zusammenarbeit bei der Kriminalitätsbekämpfung in Europa geht.
Je mehr Europa als einheitlicher kriminalgeografischer Raum an Bedeutung gewinnt, desto stärker müssen wir unsere Kräfte bündeln. So ist das europäische Polizeiamt Europol längst zu einer unverzichtbaren Institution geworden.
Der durch Europol erstellte Terrorism Situation and Trend Report (TE-SAT) ist ein Beispiel dafür, wie Europol die Mitgliedstaaten im Bereich Terrorismus mittlerweile auch mit zukunftsorientierten prognostischen Gefährdungsanalysen unterstützt. Der TE-SAT soll die Mitgliedsstaaten dabei unterstützen, strategischen Handlungsbedarf beim Kampf gegen den internationalen Terrorismus zu erkennen und darauf aufbauende, gemeinsame operative Ziele zu definieren.
In der Bekämpfung der Organisierten Kriminalität leistet Europol als wichtiger Kooperationspartner des BKA einen wesentlichen Beitrag zur Früherkennung im europäischen Kontext. Seit 2006 wird mit dem Organised Crime
Threat Assessment (OCTA) jährlich ein Instrument der strategischen Lageanalyse erstellt, das viel stärker als die bisherigen Lageberichte der Mitgliedstaaten zur Organisierten Kriminalität prognostisch orientiert ist. Bei der Datenerhebung und Lageanalyse werden nicht nur Zulieferungen aus den Mitgliedstaaten berücksichtigt, sondern auch externe Experten aus Wissenschaft und Wirtschaft befragt sowie Recherchen in externen Quellen durchgeführt und international agierende Unternehmen einbezogen.

IKPO-Interpol
Von herausragender Bedeutung für die erfolgreiche Kriminalitätsbekämpfung ist jedoch zudem eine internationale Zusammenarbeit, die weit über den europäischen Raum hinaus geht. Hier hat für uns die IKPO-Interpol die entscheidende Funktion.
Interpol ist nicht nur der älteste, sondern auch der größte multilaterale Kooperationsrahmen für die grenzüberschreitende polizeiliche Zusammenarbeit. Mit seinen 186 Mitgliedstaaten ist Interpol der Global Player der internationalen Verbrechensbekämpfung.
Die IKPO-Interpol gewährleistet, dass allgemeinpolizeiliche und fallbezogene Erkenntnisse schnell und sicher ausgetauscht werden können. Kurz gesagt – Interpol stellt den Geschäftsweg für den weltweiten Austausch polizeilicher Informationen dar.
Eine weitere wichtige Aufgabe von Interpol ist die internationale Fahndung nach Personen und Sachen. Über das Interpol-Fahndungssystem werden Fahndungsnotierungen der Mitgliedstaaten weltweit gesteuert. Am 8. Oktober 2007 wendete sich das Generalsekretaritat der IKPO-Interpol zum ersten Mal in seiner Geschichte mit einem weltweiten Fahndungsaufruf nach einem mutmaßlichen Kinderschänder an die Öffentlichkeit. Experten des Bundeskriminalamts hatten Ende 2004 eine Serie von insgesamt etwa 200 Bilddateien im Internet festgestellt, die den sexuellen Missbrauch mehrerer asiatischer Jungen zeigten. Möglich wurde die Fahndung erst, nachdem es dem Bundeskriminalamt gelungen war, ein Foto des Täters, auf dem dieser sein Gesicht technisch unkenntlich gemacht hatte, zu rekonstruieren. Mehr als 350 Hinweise aus der ganzen Welt führten elf Tage später in Thailand zur Festnahme eines 32jährigen Kanadiers. Der Mann hat sich nunmehr vor einem thailändischen Gericht zu verantworten.

Strategische Früherkennung

Die Polizei hat sich in den letzten Jahren stark gewandelt, von einer noch primär reagierenden zu einer immer stärker proaktiv agierenden Institution der Verbrechensbekämpfung. „Früherkennung„ lautet das Stichwort – gemeint ist das Erkennen künftiger Entwicklungen von Kriminalität.
Effiziente Bekämpfungsstrategien setzen voraus, dass die Polizei frühzeitig im Hinblick auf sich abzeichnende Entwicklungen und deren Auswirkungen planen kann; sie muss „vor die Lage„ kommen.
Die 2005 eingerichtete Abteilung Internationale Koordinierung (IK) des Bundeskriminalamtes hat u. a. die Aufgabe der Informationsanalyse unter prognostischen Gesichtspunkten zur Früherkennung potenzieller Kriminalitäts- und Gefährdungsentwicklungen. So wurde 2007 erstmals eine Umfeldanalyse erstellt, in der in den sechs Themenfeldern Politik, Wirtschaft, Gesellschaft, Technik, Umwelt und Recht mit wissenschaftlicher Methodik Trends herausgearbeitet wurden, die sich auf die Sicherheitslage in Deutschland auswirken können und somit zukünftige Aufgabenstellungen für das BKA erkennen lassen. Daraus können detailliertere Analysen mit entweder kriminologischer oder regionaler Schwerpunktsetzung abgeleitet werden. Die Lagebilder und Strukturanalysen der Gruppe „Strategie und Früherkennung„ der Abteilung IK ermöglichen es uns zunehmend, durch das Erkennen so genannter „schwacher Signale„ Trends auszumachen und Entwicklungen in bestimmten Phänomenbereichen vorherzusagen. Diese Elemente der so genannten strategischen Früherkennung werden durch weitere vorausschauende Analysen der deliktisch-phänomenologischen Früherkennung unserer Fachabteilungen sowie unsere kriminalistisch-kriminologische Forschung ergänzt und machen als Ganzes das Früherkennungssystem BKA aus.

Vorverlagerungsstrategie

Einen weiteren zentralen Ansatz des Bundeskriminalamtes bildet die so genannte Vorverlagerungsstrategie, die bereits zu Beginn der 1980er Jahre insbesondere zur Bekämpfung der international organisierten Rauschgiftkriminalität entwickelt wurde: Der Gedanke ist, Straftaten nicht erst im Inland oder in Westeuropa, sondern bereits in den Herkunfts- und Transitländern zu bekämpfen.

Die Vorverlagerungsstrategie beruht heute auf vier Säulen:

1. Ausbildungs-, Austausch- und besondere Kooperationsprogramme für Polizeibeamte anderer Staaten. So ist das Bundeskriminalamt derzeit unter anderem beim Aufbau der Polizei in Afghanistan beteiligt. Im Rahmen der ersten Säule der Vorverlagerungsstrategie wurden auch Ausbildungsmaßnahmen für irakische Polizeibeamte durchgeführt.
2. Ausstattungshilfe im Rahmen des Unterstützungsprogramms der Bundesregierung zur Steigerung der Leistungsfähigkeit ausländischer Polizeien, die u. a. mit Führungs- und Einsatzmitteln unterstützt werden. So wurde mit diesen Mitteln z. B. eine Polizeischule in Kabul aufgebaut.
3. Das weltweite Netz von Verbindungsbeamten des BKA, das eine strategische und zugleich taktische Beobachtung der Kriminalitätslage in der jeweiligen Region sowie eine umfassende Unterstützung im Rahmen von Ermittlungsverfahren ermöglicht. Derzeit sind 63 Verbindungsbeamte an 53 Standorte in 51 Staaten entsandt.
4. Die gezielte personelle praktische Betreuung und Unterstützung polizeilicher Kräfte vor Ort. Dies geschieht unter anderem durch die Entsendung besonders erfahrener und qualifizierter Mitarbeiter des BKA zu ausgewählten Dienststellen in Gaststaaten. Hierdurch werden die Verbindungen zu unseren Kooperationspartnern in anderen Staaten gestärkt und zusätzliche Erkenntnisse gewonnen. Derzeit führen wir Projekte im Bereich Rauschgiftkriminalität in Tadschikistan und Venezuela durch.

Zusammenarbeit mit der Wirtschaft

Zum Ausbau seiner Früherkennungskompetenz bindet das Bundeskriminalamt auch immer stärker private Akteure ein. Zusätzlich zu den bewährten Formen der Zusammenarbeit mit Vereinen und Verbänden der Wirtschaft – an erster Stelle ist hier die Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW) als strategischer Partner zu nennen – sowie der Informationsübermittlung durch die SECURICON GmbH, befinden wir uns seit 2006 in einem intensiven direkten Dialog mit weltweit tätigen großen deutschen Unternehmen, so genannten Global Playern.
Mittlerweile haben sich 40 Global Player-Unternehmen für die Zusammenarbeit entschieden. Neben zahlreichen gegenseitigen Informationsbesuchen bestehen bilaterale Kooperationen einzelner Fachbereiche (z. B. Finanzermittlungen, Kriminaltechnik, Wirtschaftskriminalität) mit Einzelunternehmen.
Ferner kommt es vermehrt zu Kontakten zwischen Firmenvertretern und BKA-Verbindungsbeamten im Ausland. Die Unternehmen verfügen oftmals über wichtige Informationen, die unsere Erkenntnisse ergänzen und in unsere Früherkennungsstrategien einfließen können. Im Gegenzug können wir Unternehmen für Gefährdungslagen sensibilisieren – diese können dann entsprechende Schutzvorkehrungen ergreifen. Informationen über Gefährdungslagen oder neue Modi Operandi stellen wir regelmäßig Global Playern, ASW und SECURICON zur Verfügung, zuletzt eine Gefährdungsbewertung im Februar 2008 hinsichtlich möglicher Bedrohungen durch eine kurdische Gruppierung im Zusammenhang mit der türkischen Militäroffensive im Nordirak. Ein weiteres Beispiel: Das BKA wurde 2006 durch ein deutsches Unternehmen über Unruhen in Sao Paulo/ Brasilien informiert, in deren Verlauf 94 Menschen getötet wurden. Die Sicherheit des Personals und der Anlagen deutscher Unternehmen war zeitweise akut gefährdet. Durch das BKA wurde – unter Beteiligung des BKA-Verbindungsbeamten in Brasilien – eine aktuelle Gefährdungsbewertung erstellt und wiederum Global Playern, ASW und SECURICON zur Verfügung gestellt.

Sicherheitsforschung

Sicherheitsforschung leistet ebenfalls einen Beitrag im Rahmen der Früherkennungsstrategie und Gefahrenvorsorge. Dem Bundeskriminalamt kommt in diesem Zusammenhang eine doppelte Rolle zu, denn es ist sowohl Nutzer von Sicherheitsforschung als auch Forschungsinstitution.
In Zusammenarbeit mit Verbänden oder gemeinnützigen Vereinen werden durch das Bundeskriminalamt kriminalpräventive Zielsetzungen thematisiert und Strategien entwickelt, um potenziellen Straftätern den Einsatz neuer Technologien für ihre Zwecke zu erschweren und präventive Konzepte zu entwickeln.
Seit 1998 ist das BKA beispielsweise Mitglied im gemeinnützigen Verein TeleTrusT (TTT), dem international tätige Firmen, Behörden und Forschungsinstitute angehören. TeleTrusT treibt richtungsweisende Entwicklungen für die Sicherheitsarchitektur von IuK-Technologien voran und bewertet mögliche Schwachpunkte. Die Polizei kann hier Technologietrends nicht nur beobachten, sondern auch Einfluss auf praktische Problemfelder im Hinblick auf kriminalpräventive Aspekte nehmen. Ein weiteres Beispiel ist das Competence Center for Applied Security Technology (CAST), das die IT-Sicherheit in allen Wirtschaftszweigen und Bereichen der öffentlichen Verwaltung voranbringen will. Der Verein stellt hierfür als nicht-kommerzielle Institution Kompetenz bereit und fördert innovative Sicherheitslösungen mit Wirkung auf den europäischen Wirtschaftsraum. Er wird getragen von zwei Fraunhofer Instituten und dem Darmstädter Zentrum für IT-Sicherheit. Im Bereich

der Sicherheitsforschung gehen inzwischen auch wesentliche Impulse von der Europäischen Kommission aus. Diese stellt bis 2013 im Rahmen des 7. EU-Forschungsrahmenprogramms rund 1,4 Milliarden Euro für entsprechende Projekte zur Verfügung, wobei folgende Ziele verfolgt werden:

> Bestmöglicher Einsatz bestehender und die Entwicklung neuer Technologien zum Schutz der Sicherheit der Bürger vor Bedrohungen wie Terrorismus, Naturkatastrophen und Verbrechen.
>
> Die verbesserte Kooperation zwischen Anbietern und Nutzern ziviler Sicherheitslösungen soll die Wettbewerbsfähigkeit der europäischen Sicherheitsindustrie – und damit die EU als Wirtschaftsstandort – stärken.

Bei der inhaltlichen Schwerpunktsetzung wird die Kommission beraten durch das „European Security Research and Innovation Forum„ (ESRIF), ein rund 70köpfiges Expertengremium mit Vertretern von Industrie, Wissenschaft und den Nutzern von Sicherheitssystemen. Derzeit arbeiten 11 Arbeitsgruppen u. a. an den Themen Sicherheit der Bürger (nicht zuletzt vor Terrorismus und Organisierter Kriminalität), Sicherheit kritischer Infrastrukturen, Grenzsicherheit, Prognosen und Szenarios, CBRNE-Stoffe (chemische, biologische, radiologische, nukleare, explosive Stoffe), Identitätsmanagement von Personen und Sachen. Die Bundesregierung hat 2007 ein korrespondierendes nationales Sicherheitsforschungsprogramm beschlossen und ein eigenes Forschungsprogramm aufgelegt („Forschung für die zivile Sicherheit„). Das deutsche Programm betont als Teil der so genannten Hightech-Strategie für Deutschland ebenso wie das europäische die Notwendigkeit einer multidisziplinär angelegten Sicherheitsforschung, die technische und sozialwissenschaftliche Fragestellungen miteinander verknüpft.
Zusätzlich zu den bereits genanten Zusammenarbeitsformen findet auch eine phänomenbezogene internationale Kooperation statt.

IUK-Kriminalität

So wurden beispielsweise in der Bekämpfung der IuK-Kriminalität international neue Wege beschritten: Die IKPO-Interpol hat ein Netzwerk von so genannten National Central Reference Points (NCRPs) installiert, dem derzeit 110 Staaten angehören. Dieses Netzwerk wird für den wichtigen fachspezifischen Nachrichten- und Informationsaustausch genutzt. Im Rahmen der G8-Kooperation wurde ein 24/7-Netzwerk eingerichtet, das für zeitkritische Anfragen auf dem Gebiet der IuK-Kriminalität genutzt wird und an jedem Tag rund um die Uhr erreichbar ist. Das Netzwerk besteht derzeit aus 50 Staaten, die Ansprechstelle für Deutschland ist beim BKA angesiedelt. Zur Verbesserung der nationalen und internationalen Zusammenarbeit der Strafverfolgungsbehörden mit Internet-Service-Providern hat der Europarat 2007 eine Studie in Auftrag gegeben („Cooperation between service providers and law enforcement against cybercrime: towards common guidelines?„). An der Studie wirken neben dem BKA u. a. Vertreter weiterer europäischer Sicherheitsbehörden, der deutsche Dachverband der Internetwirtschaft (eco), ausländische Provider und Dachverbände sowie Vertreter von Wirtschaftsunternehmen mit. Die Studie beinhaltet neben einer Bestandsaufnahme der Zusammenarbeitspraxis insbesondere die Erarbeitung von Empfehlungen bzw. eines allgemeinen Leitfadens zur Zusammenarbeit zwischen Service-Providern und Strafverfolgungsbehörden in der Europäischen Union.

Produkt- und Markenpiraterie

Die IKPO-Interpol betreibt in den letzten Jahren verstärkt Initiativen zur Bekämpfung des Phänomens der Produkt- und Markenpiraterie. Dabei ist eine verstärkte Zusammenarbeit internationaler Behörden unter der Einbeziehung des privaten Sektors eine notwendige Vorraussetzung, um eine effektive Bekämpfung des Phänomens erreichen zu können. Der zuständige Fachbereich im Interpol-Generalsekretariat hat hierzu eine Interpol Intellectual Property Crime Action Group (IIPCAG) eingerichtet. Die Mitglieder setzen sich aus verschiedenen Strafverfolgungsbehörden (u. a. Zoll und Polizei), internationalen Organisationen - wie der Welt Zoll Organisation (WCO) und der World Intellectual Property Organization (WIPO), sowie Wirtschaftsverbänden und –unternehmen zusammen. Die Gruppe arbeitet u. a. an der Einrichtung einer Interpol-Datenbank „Interpol Database on International Intellectual Property Crime„ (DIIP).
In diese Datenbank sollen sowohl Fälle von Strafverfolgungsbehörden über aktuelle und bereits abgeschlossene Ermittlungsverfahren als auch Informationen, die seitens der Privatwirtschaft an Interpol gemeldet werden, einfließen. Hierbei ist angedacht, dass die mitteilende Strafverfolgungsbehörde im möglichen Trefferfall Zugriff auf die Informationen erhält, die durch die Privatwirtschaft mitgeteilt wurden. Die Herkunft der Daten soll dabei klar gekennzeichnet werden. Für Strafverfolgungsbehörden bestünde somit die Möglichkeit, die Informationen zu prüfen, zu verifizieren und gegebenenfalls in den polizeilichen Datenbestand zu überführen. Die Informationen aus der Privatwirtschaft sollen damit zur Unterstützung der Ermittlungsbehörden in deren Ermittlungsverfahren dienen.
Auf europäischer Ebene wurde im Januar 2008 die Analysearbeitsdatei (Analysis Work File – AWF) „Copy„ bei Europol eingerichtet. Zweck dieser Datei ist es, die zuständigen Behörden der Mitgliedstaaten bei der Verhütung und Bekämpfung der Aktivitäten organisierter krimineller Netze bei der Herstellung von bzw. dem Handel mit Nachahmungen und bei der Produktpiraterie zu unterstützen. An der Analysedatei sind gegenwärtig acht EU-Mitgliedstaaten beteiligt.

Geldwäsche

Auch in der Bekämpfung der Geldwäsche stehen den Sicherheitsbehörden besondere Zusammenarbeitsformen zur Verfügung. Mit der Novellierung des Geldwäschegesetzes (GWG) im Jahr 2002 hat die im BKA eingerichtete Financial Intelligence Unit (FIU), die deutsche Zentralstelle für Geldwäsche-Verdachtsanzeigen, ihre Arbeit aufgenommen. Hier werden alle gemäß § 11 GWG erstatteten Verdachtsanzeigen nach strategischen Gesichtspunkten ausgewertet. Die nach dem GWG Meldeverpflichteten (Banken, Versicherungen etc.) werden regelmäßig über aktuelle Typologien und Methoden der Geldwäsche informiert. Für die internationale Zusammenarbeit in diesem Phänomenbereich sind – neben Interpol – zwei weitere Gremien hervorzuheben: Die Financial Action Task Force (FATF) entwickelt seit 1989 die internationalen Standards der Geldwäschebekämpfung und der Finanzierung des Terrorismus. Sie hat dazu Empfehlungen an die Regierungen und Finanzinstitute der Teilnehmerstaaten gerichtet, deren Umsetzung regelmäßig per Fragebogen und durch Prüfungen vor Ort kontrolliert wird. Ihr gehören aktuell 32 Mitgliedstaaten sowie die Europäische Kommission und der Kooperationsrat der Golfstaaten an. Ein weiteres wichtiges Forum für die internationale Kooperation ist die so genannte Egmont Group, in der sich (derzeit) 107 FIU zusammengeschlossen haben.
Als technische Plattform steht den FIU der Egmont Group für den internationalen Informationsaustausch das Egmont-Secure-Web (ESW) zur Verfügung. Hier werden über gesicherte und verschlüsselte Leitungen im Hinblick auf Geldwäsche Verdachtsanzeigen ausgetauscht. Der Mehrwert gegenüber dem Informationsaustausch über den Interpol-Weg liegt darin, dass auch Informationen von nicht polizeilichen FIU erlangt werden können.



Zügiger Informationsaustausch durch bilaterale Zusammenarbeit
(Foto: Thomas Hofem)

Entführungen und Geiselnahmen im Ausland

Im Rahmen der G8–Kooperation finden seit 2005 regelmäßig Konferenzen zum Thema Entführungen und Geiselnahmen im Ausland statt. An der letzten „International Conference on Kidnapping„ (ICOK) im Dezember 2007 in Washington nahmen 43 Experten aller G8-Staaten von Polizei, Nachrichtendiensten und den Außenministerien, in deren Zuständigkeitsbereich Entführungen und Geisellagen fallen, teil. Deutschland wurde durch das Auswärtige Amt, das Bundesministerium des Innern und das BKA vertreten. Thematische Schwerpunkte der Konferenz waren die Darstellung von Fallstudien, der Stand des Kidnapping-Meldedienstes, der Umgang mit Entführern und Geiselnehmern sowie der Dialog mit Medien zur Verhinderung von Fehlinformationen. Im Rahmen der Konferenz wurde der Termin für den Testlauf zur Einführung eines G8-Meldedienstes mit anschließender Realisierung des Wirkbetriebes festgelegt. Der Testlauf hat im März 2008 begonnen. Ein entsprechender Meldedienst auf EU-Ebene wurde im September 2007 in Betrieb genommen.
Die weltweiten Entwicklungen und die daraus folgenden veränderten Bedrohungslagen werfen neue Fragen auf, die von den Sicherheitsbehörden neue Antworten erfordern. Das Bundeskriminalamt sieht in der Bildung von neuen Allianzen auf allen Ebenen, vor allem aber im Ausbau der internationalen Zusammenarbeit, einen zentralen Ansatz zur Bewältigung dieser Herausforderungen. Sicherheitsbehörden und Privatwirtschaft haben in der Vergangenheit vielfältig auf die veränderten Rahmenbedingungen in der Kriminalitätsbekämpfung reagiert. Sie haben die in Jahrzehnten gewachsene Zusammenarbeit innerhalb der bestehenden Strukturen weiter intensiviert sowie in Teilen neue Kooperationsrahmen und Reaktionsmuster entwickelt. Trotz aller Fortschritte müssen wir jedoch die gemeinsamen Anstrengungen weiterhin ausbauen, um mit dem rasanten Tempo der Kriminalitätsentwicklung Schritt halten zu können.

© Verlag Deutsche Polizeiliteratur