.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Waldbauer-Hable, Peter (2014):

Risikomanagement bei „Law Enforcement Agencies“. Betrachtung bereits bestehender Modelle und Empfehlungen für die Umsetzung eines generellen Risikomanagements

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2), 82-94.

doi: 10.7396/2014_2_G

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Waldbauer-Hable, Peter (2014). Risikomanagement bei „Law Enforcement Agencies“. Betrachtung bereits bestehender Modelle und Empfehlungen für die Umsetzung eines generellen Risikomanagements, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2), 82-94, Online: http://dx.doi.org/10.7396/2014_2_G.

Online publiziert: 9/2014

Risikomanagement bei „Law Enforcement Agencies“

Betrachtung bereits bestehender Modelle und Empfehlungen für die Umsetzung eines generellen Risikomanagements

PETER WALDBAUER-HABLE,
Kriminalhauptkommissar der Kriminalpolizeiinspektion Passau.

Im nachfolgenden Artikel wird die Anwendbarkeit von Risikomanagement bei „Law Enforcement Agencies“ behandelt. Als Basis dienen dafür Betrachtungen des Risikomanagements aus wirtschaftlicher Sicht und Erkenntnisse, die im Zusammenhang mit der Erstellung einer Masterarbeit gewonnen wurden. Insbesondere wurden Grenzpolizeien aus verschiedenen, europäischen Staaten und die Organisationen Europol und FRONTEX einer Betrachtung unterzogen. Dabei wurde festgestellt, dass spezielles Risikomanagement, bezogen auf das Risiko Kriminalität bereits umgesetzt wird. Auf Grund dieser Erkenntnisse werden Empfehlungen ausgesprochen, die als Basis für ein standardisiertes, generelles Risikomanagement dienen können. Absicht ist es, Anregungen für die Einführung eines vereinheitlichten und vereinfachten, generellen Risikomanagements bei Law Enforcement Agencies zu geben, dessen Fokus nicht nur auf ein Risikofeld gerichtet ist, sondern die gesamte Organisation betrachtet. Die dazu gemachten Vorschläge reichen von der Erarbeitung einheitlicher Definitionen bezüglich der im Risikomanagement verwendeten Begriffe, der Entwicklung einer „Risk-Management-Policy“ in Form eines Risiko-Management-Handbuches, bis hin zur Beschreibung eines Hauptrisikokataloges. Des Weiteren werden im Artikel Vergleiche zu anderen, polizeilichen Anwendungen gezogen und Problemfelder angesprochen, die sich bei der Umsetzung ergeben können. Mit der Anwendung eines generellen Risikomanagements soll es möglich gemacht werden, die erzielten Ergebnisse innerhalb einzelner Organisationen vergleichbar zu machen. Im europäischen Kontext betrachtet, könnte dies zu effektiveren und effizienteren Organisationen im Bereich Law Enforcement führen.

I. EINLEITUNG

Law Enforcement Agencies[1] spielen in sicherheitspolitischen Überlegungen von Staaten eine wichtige Rolle. Insbesondere Grenzpolizeiorganisationen erfüllen dabei nicht selten eine Doppelfunktion. Zum einen sind sie für die innere Sicherheit des eigenen Staates verantwortlich, zum anderen für die eines großen Teils des gesamten europäischen Raumes. In diesem europäischen Kontext trifft dies insbesondere auf Länder zu, deren Grenzen sog. Schengen-Außengrenzen darstellen. Insoweit ist es notwendig, diese Organisationen mit innovativen Methoden auszustatten, um sie effektiver und vor allem effizienter zu machen. Eine dieser Methoden, die unter anderem aus dem wirtschaftlichen Bereich kommt, ist Risikomanagement, mit dessen Kernelement Risikoanalyse.

Im Zusammenhang mit der Erstellung einer Masterarbeit[2] wurde in Form einer

vergleichenden Studie[3] dargestellt, wie sich die Umsetzung dieser Methode bei einigen Staaten und Organisationen gestaltet.

Eine der grundsätzlich zu stellenden Fragen ist dabei, ob Risikomanagement überhaupt auf eine Organisation wie die Polizei übertragen werden kann. Eine weitere, wichtige Frage mit Hinblick auf den gesamteuropäischen Kontext ist die, ob ein einheitliches Verständnis über Risikomanagement gegeben ist, ob dies überhaupt notwendig ist und wie es gegebenenfalls erzielt werden könnte.

Zuerst soll jedoch zur Veranschaulichung kurz das Risikomanagement aus wirtschaftlicher Sicht beschrieben werden.

II. GRUNDZÜGE UND BESTANDTEILE DES WIRTSCHAFTLICHEN RISIKOMANAGEMENTS[4]

Im wirtschaftlichen Bereich haben sich in den letzten Jahrzehnten vor allem Banken, Versicherungen und Unternehmen dem Thema zugewandt. Nach wie vor sind jedoch gewisse Unsicherheiten bezüglich der Begrifflichkeiten, der Anwendung und Umsetzung vorhanden. So gibt es bis heute keine eindeutige Definition für den Begriff Risiko, was dazu führt, dass unterschiedliche Definitionen vorherrschen, denen verschiedene Disziplinen zu Grunde liegen. Beispiele hierfür sind die mathematisch/analytische[5], die informationstheoretische[6] oder die psychologische[7] Sichtweise. Trotz dieser Vielschichtigkeit des Risikobegriffes ist festzuhalten, dass auf Branchen bezogen die Verwendung von einheitlichen Definitionen vorzufinden ist. So verwenden z.B. Banken bei der Anwendung des Risikomanagements gleiche Begriffserklärungen, was zu vergleichbaren Ergebnissen führt.

Der wichtigste Teil im Prozess ist die Risikoanalyse, die sich aus der Risikoidentifizierung und der Risikobewertung zusammensetzt.[8] Sie dient dazu, die Risikolage eines Unternehmens, einer Organisation zu erfassen, zu bewerten und dadurch Ansatzpunkte für die Entwicklung und Umsetzung risikopolitischer Maßnahmen (Bewältigungsstrategien) zu liefern. Die schwierigste Aufgabe im Teilprozess Risikoanalyse ist die Risikoidentifizierung. Schwierig deshalb, weil es nicht nur um das Erkennen neuer Risiken geht, sondern auch darum, Veränderungen bei bereits bestehenden wahrzunehmen. Des Weiteren sollen durch sie Risikoquellen, Schadenseintrittszeitpunkte und Schadensursachen erfasst werden (vgl. Voigt 2010, 11). Dies unter Beachtung eines vernünftigen Kosten-Nutzen-Aufwandes.

Um Risiken identifizieren zu können, werden bestimmte Methoden angewandt, von denen nachfolgend einige beispielhaft aufgezählt werden:

- Kollektions- und Suchmethoden (Checklisten, SWOT-Analyse, Self-Assessment),
- Analytische Methoden (Fragenkatalog, Baumanalyse) und
- Kreativitätsmethoden (Brainstorming, Brainwriting, Delphi-Methode, Szenarioanalyse).

Der zweite Teil der Risikoanalyse, die Risikobewertung, ist der logische Schritt nach der Risikoidentifizierung. Dabei werden die Bewertungsparameter Eintrittswahrscheinlichkeit und Schadensausmaß einer Betrachtung mit quantitativen, semiquantitativen und/oder qualitativen Methoden unterzogen. Bei den beiden Erstgenannten werden mathematische Größen, also messbare Zahlen verwendet. Bei der qualitativen Bewertung werden anstatt von Zahlen subjektive und erfahrungsbasierende Einschätzungen vorgenommen. Sie werden oftmals als qualitative Kennwörter bezeichnet und können hoch, niedrig, schwer, gering, vernachlässigbar, katas-

Quelle: in Anlehnung an Voigt 2010, 60

RISIKO WECHSEL-WIRKUNGEN		Folgerisiko durch Wechselwirkung													
		Org.-Bereich A				Org.-Bereich B			Org.-Bereich C			Org.-Bereich D			
Identifiziertes Risiko		Risiko 1	Risiko 2	Risiko 3	Risiko 4	Risiko 1	Risiko 2	Risiko 3	Risiko 1	Risiko 2	Risiko 3	Risiko 1	Risiko 2	Risiko 3	Risiko 4
Org.-Bereich A	Risiko 1			X										X	
	Risiko 2						X	X	X	X				X	
	Risiko 3						X	X	X	X					
	Risiko 4			X			X	X	X	X			X	X	X
Org.-Bereich B	Risiko 1			X			X	X					X		
	Risiko 2			X								X			
	Risiko 3			X								X		X	
Org.-Bereich C	Risiko 1			X									X	X	X
	Risiko 2			X									X	X	X
	Risiko 3														
Org.-Bereich D	Risiko 1			X		X	X	X					X	X	
	Risiko 2			X		X	X								X
	Risiko 3			X											
	Risiko 4			X										X	

Abb. 1: Wechselwirkung von Risiken („Cross-Impact-Matrix")

trophal usw. lauten. Die qualitative Bewertung wird im Speziellen dann empfohlen, wenn für Entscheidungen auf Grund mangelnder Informationen und/oder Daten keine verlässlichen Zahlen, also nicht genügend quantitatives Material vorliegt.

Die Risikobewertung zielt darauf ab, festzustellen, in welchem Ausmaß die identifizierten Risiken die Ziele des Unternehmens, der Organisation gefährden. Im Zusammenhang mit der Bewertung ist anzumerken, dass es oftmals nicht sinnvoll und auf Grund der Komplexität vieler Unternehmen und Organisationen auch nicht möglich ist, alle identifizierten Risiken zu bewerten. Ebenso wird es nicht gelingen, alle Risiken zu identifizieren. Abschließend sei noch darauf hingewiesen, dass sich Risiken gegenseitig beeinflussen können. Dies muss bei der Bewertung ebenfalls berücksichtigt werden. Zum Erkennen dieser Beeinflussung ist eine „Cross-Impact-Analyse" am besten geeignet. Diese wird anhand einer „Cross-Impact-Matrix" visualisiert (siehe Abbildung 1).

Ist die Risikoanalyse in Form der Identifizierung und Bewertung abgeschlossen, werden sog. Bewältigungsstrategien entwickelt, um Risiken entgegen zu wirken. Dabei wird von aktiven und passiven Strategien gesprochen. Die Risikovermeidung und -minderung sind solche der aktiven Vorgehensweise, der Risikotransfer und die Risikovorsorge die der passiven.

Den Abschluss des Risikomanagementprozesses bilden die Überwachung der beschlossenen Bewältigungsstrategien (Risikoüberwachung), das Risikoreporting und die während des gesamten Prozesses laufende Risikokommunikation. Insbesondere die Kommunikation ist ein wichtiger Bestandteil, der den Prozess fortwährend begleitet. Sie ist sowohl zwischen den Beteiligten der einzelnen Prozessebenen (horizontal) als auch Ebenen übergreifend (vertikal), also top-down und bottom-up zu gewährleisten.

Nachfolgend eine grafische Darstellung (siehe Abbildung 2, Seite 85) des Risikomanagementprozesses zur Visualisierung der Ausführungen.

III. DARSTELLUNG DER ANWENDUNG DES RISIKOMANAGEMENTS AM BEISPIEL VERSCHIEDENER GRENZPOLIZEIEN UND DER ORGANISATIONEN EUROPOL UND FRONTEX

1. DATENERHEBUNG

Nach gezielten Recherchen wurde festgestellt, dass wissenschaftlich fundierte, polizeibezogene Fachliteratur kaum vorhanden ist. Im europäischen Kontext finden sich aus dem Jahr 2002 bei EUROPOL

erste Hinweise auf Risikomanagement im Zusammenhang mit der Durchführung des „Strategic Intelligence Analysis Course“. Dabei wurden unter anderem die Begriffe „Risk Assessment“ und „Threat Assessment“ erwähnt. Die EU befasste sich ebenfalls im Jahr 2002 mit dem Thema und ließ durch eine Expertenkommission das CIRAM (Common Integrated Risk Analysis Model) entwickeln. Die Verantwortlichkeit für dieses Dokument wurde später der europäischen Grenzschutzagentur FRONTEX übertragen, welche im Jahr 2011 eine überarbeitete Version, das CIRAM 2.0, vorstellte. Auch in anderen Dokumenten, wie dem EU Schengen Katalog oder den IBMS (Integrated Border Management Strategies) finden sich Hinweise auf Risikomanagement bzw. Risikoanalyse. Sie werden als Hilfsmittel bei der Grenzsicherung beschrieben.

Zusätzliche Daten wurden durch persönlich geführte Interviews im Zusammenhang mit der Erstellung der Masterarbeit erhoben. Anhand eines detaillierten Leitfadens wurden die Interviewpartner (Experten bzw. Leiter von Risikoanalyseeinheiten) einzeln befragt. Als Referenzstaaten wurden Bosnien-Herzegowina, Kroatien, Ungarn und Deutschland (Bayern) herangezogen. Des Weiteren wurden die Organisationen EUROPOL und FRONTEX in der Untersuchung berücksichtigt. Auf diese Weise war es möglich, nicht nur einen Vergleich mit dem wirtschaftlichen Risikomanagement herzustellen, sondern auch die Vorgehensweisen bei den einzelnen Ländern und Organisationen darzustellen.

Die Interviewergebnisse wurden ausgewertet und unter verschiedenen, vorher definierten Kategorien erfasst. Diese sind:

- Anwendung und Anwendbarkeit des Risikomanagements,
- Verständnis des Risikomanagements und Wichtigkeit für die Organisation,
- Begriffe, Begrifflichkeiten und Definitionen,
- Vorgehensweise bei der Umsetzung des Risikomanagements.

Quelle: Hölscher 2002, 13

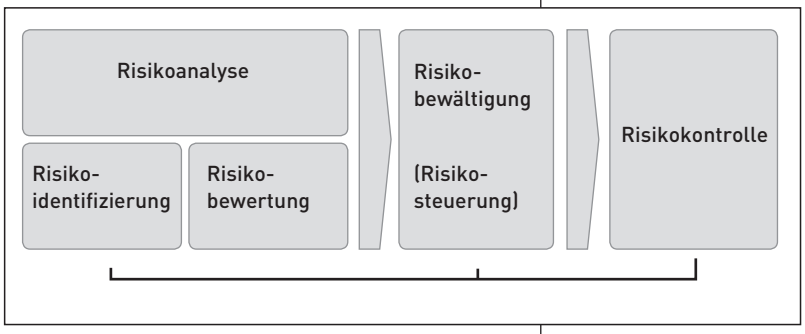

Abb. 2: Risikomanagementprozess

2. ERGEBNISSE DER UNTERSUCHUNG

Grundsätzlich wird Risikomanagement (meistens bezeichnet als Risikoanalyse) von den befragten Experten als Anwendung betrachtet, die auf polizeiliche Organisationen übertragbar ist und sowohl die Arbeit einer Organisation als auch diese selbst verbessern kann. Einschränkend wurde jedoch angemerkt, dass es teilweise nicht verstanden wird, weil eine klare Methodik fehlt.

Ein Regelkreislauf wie im wirtschaftlichen Risikomanagement ist bei den untersuchten Anwendungen nicht ersichtlich. Vielmehr findet man sehr oft den Begriff „assessment“, der mit unterschiedlichen Termini ergänzt wird. Als Beispiel sei CIRAM 2.0 genannt, in welchem die Kombinationen „threat assessment“, „vulnerability assessment“ und „impact assessment“ verwendet werden (vgl. FRONTEX 2011a, 13 ff). Ähnliche Begriffspaare finden sich beim US Department for Homeland Security[9], bei dem vom „threat assessment process“, „vulnerability assessment process“ und „consequence assessment process” gesprochen wird (vgl. US Homeland Security Office 2006, 11 ff). Die Begriffsnähe bei beiden Organisationen ist

insoweit nicht verwunderlich, da sich das von FRONTEX entwickelte CIRAM 2.0 durchaus am Modell des US Department for Homeland Security orientiert. Nichtsdestotrotz kann gesagt werden, dass es sich bei beiden Modellen um eine wiederkehrende, einem Kreislauf ähnliche Abfolge von entsprechenden Maßnahmen handelt.

Als weiteren Aspekt galt es festzustellen, welche Ziele mit Risikomanagement verfolgt werden. Genannt wurden:

- Unterstützung der Führungskräfte und des Entscheidungsprozesses,
- Gleichmachung von unterschiedlichen Lebenssachverhalten, um diese vergleichen zu können,
- Arbeitsverbesserung,
- Herausarbeiten von Handlungsoptionen und/oder Prioritäten.

Besonderes Augenmerk wurde auf Erkenntnisse bezüglich des Verständnisses und der Wichtigkeit der Risikoanalyse gelegt, da diese als Kernelement des Risikomanagements zu verstehen ist. In den bereits erwähnten Schriften wie dem CIRAM und dem EU Schengen Katalog findet man die Unterteilung in „strategic risk analysis", „operational risk analysis" und „tactical risk analysis" (vgl. Europäische Union 2002, 8). Im CIRAM 2.0 wird dies nicht mehr erwähnt. Abgesehen vom neuen CIRAM 2.0 gibt es in keinem anderen Dokument Hinweise darauf, wie Risikoanalyse zu verstehen und durchzuführen ist. Dies gilt auch für die IBMS aus dem Jahr 2007 und die IBM Guidelines aus dem Jahr 2009, in denen „risk analysis" thematisiert wird, ohne genauer darauf einzugehen (vgl. European Commission 2009, 80 f).

Bei den Experten herrscht keine Einigkeit darüber, ob Risikoanalyse ein eigenständiger Prozess oder ein Teilprozess des Risikomanagementprozesses ist. Des Weiteren wurde angemerkt, dass Risikoanalyse und deren Funktion von der Belegschaft nicht oder nur teilweise verstanden wird. Dies wurde damit begründet, dass im Zusammenhang mit der Durchführung der Risikoanalyse ein breiter Raum für Interpretation vorhanden ist und sich deshalb Schwierigkeiten beim Verständnis ergeben.

Bezüglich der Risikoidentifikation ist anzumerken, dass in den Dokumenten mit Ausnahme des CIRAM 2.0 nichts zu finden ist, wobei der Begriff „risk identification" auch hier nicht verwendet wird. Vielmehr spricht man von der Gefahrenidentifizierung und benennt Methoden, die aus der Risikoidentifizierung der Wirtschaft bekannt sind. Dies sind u.a. die Expertenbefragung, die Delphi-Methode und die Szenarioanalyse. In den Guidelines zum CIRAM 2.0 finden sich weitere Methoden, die allerdings der Risikobewertung zuzurechnen sind und als „assessment techniques" bezeichnet werden (vgl. FRONTEX 2011b, 80 ff). Trotzdem sollen einige genannt werden, da sie auch zur Risikoidentifizierung geeignet sind. Dazu zählen:

- field based techniques (Vor-Ort-Besuche, Interviews, Befragungen),
- empirische Techniken (Überprüfung von zurückliegenden Daten, einfache Her- bzw. Ableitungen),
- diagnostic techniques (Checklisten, Betrachtung von Indikatoren, Chronologien).

Bezüglich der Funktion der Risikoidentifizierung gibt es ebenfalls unterschiedliche Ansichten. So sprechen manche vom Sammeln von Daten, einer Themenbestimmung oder davon, verschiedene Modi Operandi zu identifizieren.

Auch die Risikobewertung findet in der Literatur keine explizite Erwähnung. Trotzdem werden die Parameter Wahrscheinlichkeit (likelihood) und (Schadens-)Ausmaß (magnitude) verwendet. Erwähnt werden die Begriffe im CIRAM 2.0 im Zusammenhang mit dem Terminus „threat assessment" (vgl. FRONTEX

2011a, 19). Des Weiteren wird ausgeführt, dass qualitative Methoden zur Bewertung am geeignetsten erscheinen, da in der Regel quantitative Informationen nicht oder nicht ausreichend zur Verfügung stehen. Bei den Interviews wurden verschiedene Erklärungen zur Aufgabe der Risikobewertung abgegeben. Unter anderem wurden diese als Berechnen der Eintrittswahrscheinlichkeit und des Schadensausmaßes bezeichnet, oder als Daten zusammenfassen und einen Report erstellen.

Bei den Risikobewältigungsstrategien findet keine, wie aus dem wirtschaftlichen Risikomanagement bekannte Einteilung in aktive oder passive Methoden statt. Lediglich im CIRAM 2.0 ist der Begriff „recommendations" zu finden, der entfernt auf die Anwendung solcher Steuerungsmethoden hinweist (vgl. FRONTEX 2011a, 79). Die Experten sprachen überwiegend davon, dass die Reduktion und Akzeptanz von Risiken im Vordergrund stehen. Die Risikovermeidung wurde als nicht geeignet bezeichnet.

In der fachbezogenen Literatur finden sich auch kaum Hinweise auf die Themenbereiche Risikoüberwachung und Reporting. Die Risikoüberwachung wird mehr dem Bereich der Risikoidentifizierung zugerechnet. Das Reporting wird auf verschiedene Art und Weise vollzogen. Im CIRAM 2.0 gibt es unter anderem den „weekly analytical brief" oder „weekly analytical report", als auch die „semiannual" und „annual risk reports" (vgl. FRONTEX 2011a, 43). Die Antworten der Interviewpartner ließen jedoch erkennen, dass den Themen keine allzu große Bedeutung beigemessen wird. In einigen Ländern werden diesbezüglich keinerlei Anstrengungen unternommen. Im Zusammenhang mit der Risikoüberwachung wurde auch festgestellt, dass Kommunikation nicht oder nur sehr nachlässig betrieben wird. Dies gilt sowohl für die horizontale als auch vertikale Ebene. Viele der Experten haben dies als Problem erkannt, da es den Informationsfluss nach oben und die Ergebnismitteilung nach unten erschwert.

3. BEGRIFFE, DEFINITIONEN UND DAS PROBLEMFELD SPRACHE

Die Ergebnisse der Untersuchung machen es notwendig, den Themen Begriffe, Definitionen und Sprache ein eigenes Kapitel zu widmen. Grund dafür ist, dass sowohl bei der Prüfung der polizeibezogenen Dokumente als auch bei den Interviews herausgefunden werden konnte, dass es keine einheitlich gültigen Definitionen gibt und Begriffe unterschiedlich gebraucht und auch verstanden werden. Es scheint beinahe so zu sein, dass die einzelnen Anwender das verwenden, was ihnen persönlich am meisten zusagt. Als Beispiel soll die unterschiedliche Auffassung und Verwendung von Begriffen bezüglich des hierarchischen Aufbaus von Law Enforcement Agencies genannt werden, da darin alle oben angesprochenen Probleme aufgezeigt werden können. Grundsätzlich sieht der Aufbau die strategische (höchste), operative (mittlere) und taktische (unterste) Ebene vor. Manche der Interviewten sind jedoch der Meinung, dass die taktische Ebene die mittlere und daraus resultierend, die operative die unterste Ebene ist. Es gibt auch die Ansicht, dass der Ausdruck strategische Ebene nicht angewandt werden darf, weil dadurch der Eindruck entsteht, dass auf den anderen Ebenen keine strategischen Entscheidungen getroffen werden. In manchen Organisationen werden gänzlich andere Bezeichnungen verwendet, die dann „central" als die höchste, „regional" als die mittlere und „local" als die unterste Ebene beschreiben. Im Gegensatz dazu war in einem der untersuchten Staaten die „local" Ebene die höchste Ebene, was die Verwirrung komplett macht. Auch das be-

reits erwähnte CIRAM-Dokument hat sich mit der Einteilung der Ebenen beschäftigt und dabei die strategische als die höchste und die operative als die mittlere Ebene bezeichnet. Die taktische Ebene wurde nicht ausdrücklich erwähnt und als eine Sonder- bzw. Unterform der operativen Ebene bezeichnet (vgl. Euroäische Union 2002, 7). Auch im neu entwickelten CIRAM 2.0 ist eine klare Unterscheidung nicht mehr ersichtlich. Diese vielschichtigen Probleme erwachsen u.a. aus dem Fehlen eines einheitlich definierten Vokabulars, aus der nicht stattfindenden bzw. schlechten Kommunikation, der Tatsache, dass die Arbeitssprache Englisch ist und den daraus resultierenden, unterschiedlichen Übersetzungen in den einzelnen europäischen Sprachen. Dazu kommt, dass Übersetzungen nicht nur Sprachfärbungen unterliegen, sondern damit oft auch eine Bedeutungs- bzw. Verständnisänderung einhergeht. Dass diese Probleme sehr wohl erkannt werden, zeigt die Antwort auf die Frage nach einer Vereinheitlichung und/oder Standardisierung des Risikomanagements, welche von den Experten zu 100 Prozent mit ja beantwortet wurde.

4. ABGRENZUNG DER RISIKOANALYSE ZUR BEURTEILUNG DER LAGE

Die Beurteilung der Lage (BdL) ist eine Methode, die bei fast allen europäischen Polizeieinheiten angewandt wird, um polizeilich relevante Probleme (Lebenssachverhalte) zu erfassen, zu bewerten und Schlussfolgerungen zu ziehen (vgl. Strobl 1996, 29). So wird dem Polizeiführer die Möglichkeit gegeben, einen Entschluss zu fassen. Schon diese kurze Beschreibung könnte den Eindruck vermitteln, dass es sich somit bei beiden Anwendungen um das Gleiche handelt. Deshalb werden die Gemeinsamkeiten, aber vor allem die Unterschiede nachfolgend dargestellt.

Bei beiden Anwendungen handelt es sich zweifelsohne um methodische Ansätze, die gleichzeitig wichtigster Teil eines Gesamtprozesses sind. Bei der BdL ist es der Problemlösungsprozess, bei der Risikoanalyse der Risikomanagementprozess. Auch die Vorgehensweise bei der Durchführung der Anwendungen ist ähnlich. Bei der BdL wird das Problem (Lebenssachverhalt) angesprochen, bewertet und dann gefolgert. Bei der Risikoanalyse wird identifiziert, bewertet und abschließend gesteuert. Wendet man sich nun den Unterschieden zu, kommt man zu dem Ergebnis, dass bei der BdL das Problem bekannt ist. Man weiß, was wann passiert und wo es stattfindet. Es handelt sich um ein einzelnes Problem, das in mehrere, kleinere Probleme zerlegt wird. Bei der Risikoanalyse dagegen ist das Problem nicht, oder nicht genau bekannt. Man weiß nicht ob und, wenn ja, wann und wo genau etwas passiert. Des Weiteren herrscht Unsicherheit über das Ausmaß und darüber, ob es sich lediglich um ein oder um mehrere Probleme handelt. Weitere Unterschiede in den Methoden finden sich in der Zielsetzung. Bei der BdL ist das Ziel, Lösungsmöglichkeiten für den Polizeiführer zu erarbeiten. Daraus leitet dieser einen Entschluss ab, der zur Umsetzung unmittelbarer Maßnahmen führt. Bei der Risikoanalyse dagegen ist das Ziel die Erstellung eines Risikoprofils, mit welchem das Risikopotential eines vorher festgelegten, möglichen Ereignisses beschrieben wird. Die für die Risikosteuerung festgelegten Maßnahmen (Bewältigungsstrategien) müssen nicht unmittelbar umgesetzt werden. Es kann sogar sein, dass die Umsetzung dieser Steuerungsmaßnahmen überhaupt nicht notwendig ist. Zusammenfassend kann gesagt werden, dass die Risikoanalyse das Unbekannte und bislang Ungeschehene beschreibt. Unterschiedliche Lebenssachverhalte können vergleichbar

gemacht werden. Die Beurteilung der Lage beschreibt das Bekannte, bislang noch nicht, aber mit Sicherheit Eintretende, bislang Ungeschehene. Daraus kann gefolgert werden, dass der tatsächliche Eintritt eines bei der Risikoanalyse erkannten Ereignisses die Beurteilung der Lage nach sich zieht.

IV. EMPFEHLUNGEN FÜR EIN GENERELLES RISIKOMANAGEMENT BEI LAW ENFORCEMENT AGENCIES

Wie eingangs dieser Abhandlung bereits erwähnt, ist die grundsätzliche Frage, ob Risikomanagement auf Law Enforcement Agencies übertragen werden kann. Des Weiteren muss die Überlegung angestellt werden, ob dafür eine Vorgehensweise aus der freien Marktwirtschaft als Basis geeignet ist. Ein Fehler wäre es, eine staatliche Organisation, die für Sicherheit verantwortlich zeichnet, mit einem Wirtschaftsunternehmen zu vergleichen. Unternehmen sind auf wirtschaftlichen Erfolg ausgerichtet, was unter Heranziehung des Beispiels einer Grenzpolizeiorganisation nicht der Fall ist. Deshalb würde das Überstülpen einer Anwendung wie Risikomanagement nicht funktionieren, ohne die erforderlichen Anpassungen vorzunehmen. Festgestellt werden konnte auch, dass es sich bei den im polizeilichen Bereich bereits angewandten Modellen um spezielles Risikomanagement handelt, das sich mit dem Risikobereich Kriminalität und den darunter zu subsumierenden Einzelrisiken beschäftigt. Generelles Risikomanagement, welches die gesamte Organisation betrachtet, wird nicht umgesetzt. Auf Grund der Betrachtungen des Risikomanagements im wirtschaftlichen Sinn und den Erkenntnissen aus der Untersuchung könnten nachfolgende Empfehlungen zur Implementierung eines einheitlichen und generellen Risikomanagements beitragen.

1. GRUNDSÄTZLICHE ANFORDERUNGEN

Wichtig erscheint es, dass einfache, allgemeingültige und verbindliche Definitionen der Begrifflichkeiten gefasst werden, welche im Risikomanagement Anwendung finden. Dies gilt für die Begriffe Risikomanagement, Risikomanagementprozess, Risiko, Risikoanalyse, Risikoidentifizierung, Risikobewertung, Risikobewältigung, Risikoüberwachung, Risikoreporting und Risikokommunikation. Diese Vereinheitlichung und Vereinfachung der Begriffe führt dazu, dass Missinterpretationen und Missverständnisse ausgeschlossen werden können. Als „good example" könnte hier der ISO Guide 73[10] (ISO Guide 2009) dienen.

2. KONZEPTIONELLE UMSETZUNG UNTER VERWENDUNG EINES „RISIKO-MANAGEMENT-HANDBUCHES"[11]

Die Einführung und Umsetzung des Risikomanagements sollte unter konzeptioneller und gleicher Vorgehensweise erfolgen. Erreicht werden kann dies durch Zuhilfenahme eines Risiko-Management-Handbuches (auch: Risk-Management-Policy). Dieses Handbuch sollte so gut sein, dass auch bei einem Wechsel von (verantwortlichen) Personen die Fortführung des Prozesses jederzeit und ohne Schwierigkeiten möglich ist (vgl. Romeike/Hager 2009, 117).

Es sollten nach Meinung des Verfassers darin enthalten sein:

- Ziele des Risikomanagements,
- Begriffsdefinitionen,
- Beschreibung der risikopolitischen Grundsätze, insbesondere der Einstellung zum Risiko und zur Risikotragfähigkeit[12],
- Beschreibung der Risikoanalyse (Risikoidentifizierung und Risikobewertung) und der Risikokommunikation,

- Risikostruktur und Risikokatalog,
- Organisatorischer Aufbau (z.B. leitungszentrierter oder prozessorientierter Aufbau),
- Bestimmung der Verantwortlichen und deren Aufgabenbereich,
- Beschreibung der Methoden und Instrumentarien,
- Darstellung des Risikomanagementprozesses,
- Inkrafttreten und Geltungsbereich.

3. GEMEINSAMER HAUPT-RISIKOKATALOG

Um die Ergebnisse des Risikomanagements der verschiedenen Anwender (verschiedene Staaten, Organisationen usw.) vergleichbar zu machen, muss ein gemeinsamer Hauptrisikokatalog entwickelt werden, der Risiken aufzeigt, welche für alle gleichsam Gültigkeit besitzen. Dieser Hauptrisikokatalog kann durch länder- bzw. organisationsspezifische Risiken erweitert werden, damit möglichen, vorliegenden Spezialitäten Rechnung getragen wird. Der gemeinsame Hauptrisikokatalog erfüllt mehrere Funktionen. Im Zuge eines generellen Risikomanagements lenkt er die Aufmerksamkeit der Anwender eines speziellen Risikomanagements weg vom Risikobereich Kriminalität hin zu einer Gesamtbetrachtung der Organisation. Diese generelle Betrachtungsweise hat den Vorteil, dass der Risikobereich Kriminalität automatisch miteinbezogen wird. Des Weiteren werden subjektive Wahrnehmungen der verschiedenen Anwender weitestgehend ausgeblendet, da alle die gleichen Risiken bearbeiten. Ein modularer Aufbau in Form von Risikokategorien, hin zu Risikobereichen, welcher mit der Benennung von Einzelrisiken abgeschlossen wird, erscheint in mehrfacher Hinsicht zielführend. Wie in diesen Ausführungen bereits erwähnt, unterliegen die meisten Law Enforcement Agencies einem dreiteiligen, hierarchischen Aufbau. Mit dem oben genannten, modularen Aufbau ist es möglich, dass sich die einzelnen Prozessebenen die Teile des Risikomanagements aussuchen, welche in ihren Zuständigkeitsbereich gehören. Für die strategische Ebene werden wohl alle Risikokategorien und -bereiche zutreffen. Auf der operativen und taktischen Ebene wird sich der Umfang jedoch reduzieren. Eine mögliche Einteilung im Bereich Risikokategorien könnte sein, dass man von externen und internen Risiken spricht. Diese Einteilung soll zum Ausdruck bringen, dass es Risiken gibt, die einerseits von außen und andererseits von innen auf die Organisation einwirken. Diese Kategorien können anschließend in Risikobereiche unterteilt werden. Im Außenbereich könnten dies z.B. Änderungen der politischen Lage im In- bzw. Ausland, Änderungen der gesetzlichen Lage im In- bzw. Ausland oder das Kriminalitätsrisiko sein. Im Innenbereich könnte man strukturelle Risiken, Finanzrisiken oder Personalrisiken nennen. Die daraus erwachsenden Einzelrisiken würden dann beispielsweise sein, dass sich die Asylpolitik ändert, dass Gesetzesänderungen beschlossen werden, das Risiko der verschiedenen, grenzspezifischen Kriminalitätsformen, eine schlechte Organisationsstruktur, Budgetkürzungen oder fehlende Qualifikation der Mitarbeiter. Der Risikokatalog könnte so gestaltet werden, dass jene Risiken, die im prozessorientierten Ansatz auch von der mittleren und unteren Ebene bearbeitet werden können, zum Schluss genannt werden. Auf diese Weise würde dem Gedanken des modularen Aufbaus Rechnung getragen.

4. VERANKERUNG DES GENERELLEN RISIKOMANAGEMENTS IN DER FÜHRUNGSEBENE

Besondere Bedeutung muss der Verankerung des Risikomanagements in der

Führungsebene beigemessen werden. Sie hat dafür Sorge zu tragen, dass die Verständnisgewinnung und Akzeptanz in den nachfolgenden Ebenen und beim Personal gewährleistet ist. Dies muss von einer umfangreichen, offenen und alle Ebenen (horizontal und vertikal) umfassenden Kommunikation begleitet werden. Die konzeptionelle (gleiche) Vorgehensweise bedingt es auch, dass zuerst die Grundlagen bezüglich der Rahmenbedingungen (Anmerkungen zur Form des Risikomanagements), der Organisation (z.B. Funktion, Verantwortung – „das wer macht was" und Informationsfluss) sowie der Prozessphasen beschlossen und definiert werden (vgl. Romeike/Hager 2009, 114). Um dies in einer funktionalen Form gewährleisten zu können, sollte das bereits erwähnte Risiko-Management-Handbuch herangezogen werden. Zuerst ist es aber wichtig, die Ziele der Organisation und die Ziele des Risikomanagements gegenüberzustellen, bzw. zu vergleichen. Als Ziele der Organisation Grenzpolizei können dabei genannt werden:

- Sicherung der Grenzen,
- Erhöhung und Aufrechterhaltung der öffentlichen Sicherheit und Ordnung,
- Verhinderung von Straftaten und Verwaltungsübertretungen,
- Bekämpfung der Kriminalität,
- Verbesserung der Arbeits- und Organisationseffizienz,
- Mitarbeiterzufriedenheit.

Dem gegenüber stehen als Ziele des Risikomanagements:

- Leistungssteigerung der Organisation,
- Aufdecken von Risiken in allen Bereichen,
- Erkennen von Chancen zur Effizienzsteigerung,
- Unterstützung zum rechtzeitigen Erkennen von zukünftigen Entwicklungen.

Diese Ziele, die sich idealerweise gegenseitig ergänzen, werden, neben anderen Punkten, in Form einer Risiko-Management-Policy definiert und im Risiko-Management-Handbuch schriftlich niedergelegt.

5. VISUALISIERUNG

Um das Risikomanagement, insbesondere die Risikoanalyse und deren Ergebnis, visuell darzustellen, wird empfohlen, Skalen, insbesondere Relevanzskalen, einzusetzen. Sie haben die Funktion, Risikoklassen zu beschreiben (siehe Abbildung 3).

Eine weitere Form der Darstellung ist die Risikomatrix, mit welcher veranschaulicht wird, wie schwerwiegend ein Risiko ist. Auf der Horizontalachse wird die Eintrittswahrscheinlichkeit und auf der Vertikalachse das Schadensausmaß zum Ausdruck gebracht. Das daraus resultierende Risiko wird als sehr hoch, hoch, mittel und niedrig beschrieben (siehe Abbildung 4, Seite 92). Was die jeweilige Beschreibung bedeutet, wird in der Relevanzskala mit Worten erklärt.

Quelle: Waldbauer-Hable

Relevanzskala

Klasse	Risikotragfähigkeit	Beschreibung
1	Niedriges Risiko	Die Organisation kann das Risiko alleine bewältigen.
2	Mittleres Risiko	Die Organisation kann das Risiko alleine bewältigen; Hilfe von Einheiten der gleichen Organisation ist erforderlich.
3	Hohes Risiko	Die Organisation kann das Risiko alleine nicht mehr bewältigen; Hilfe von innerstaatlichen Organisationen ist erforderlich.
4	Sehr hohes Risiko	Die Organisation kann das Risiko alleine nicht mehr bewältigen; Hilfe von internationalen Organisationen ist erforderlich.

Abb. 3: Relevanzskala Risikotragfähigkeit

Quelle: in Anlehnung an Deutsches Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2010, 39

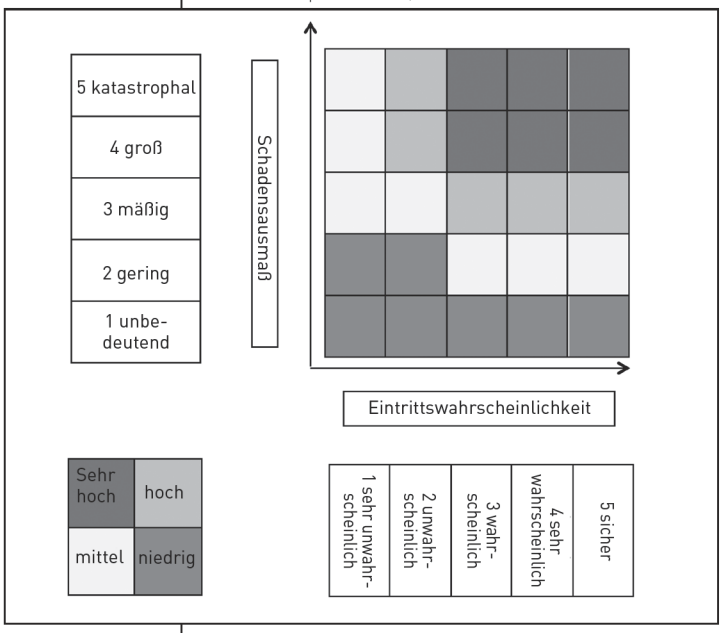

Abb. 4: Risikomatrix

6. DER MENSCHLICHE FAKTOR BEI DER PRAKTISCHEN UMSETZUNG

In der gängigen Literatur wird der Mensch als „das" Hauptrisiko angesehen. Dies resultiert daraus, dass er Entscheider und Risikoeigner zugleich ist. Das trifft sowohl für das Führungspersonal als auch die Mitarbeiter zu. Dies macht es nach Auffassung des Autors notwendig, bei der Umsetzung und Einführung des Risikomanagements besonderes Augenmerk darauf zu richten. Eine besondere Aufgabe besteht hierbei für die Führungsebene, da dort der Prozess vorgelebt werden muss. Sie hat dafür zu sorgen, dass Verständnis für die Einführung geweckt wird und eine Risikokultur entsteht. Des Weiteren besteht ihre Verantwortung darin, das geeignete Personal auszuwählen und für ein geeignetes Arbeitsumfeld zu sorgen. Es ist aber auch zu berücksichtigen, dass jede Änderung mit Ängsten der Mitarbeiter einhergeht. Diese gilt es, durch einen offenen Prozess und umfangreiche Kommunikation zu zerstreuen. Zur Erreichung einer möglichst problemlosen Umsetzung scheint die Anwendung des „Change Managements" am ehesten geeignet.

V. ZUSAMMENFASSUNG UND AUSBLICK

Die Ausführungen in diesem Artikel zeigen, dass die Verantwortlichen der einzelnen Organisationen die Notwendigkeit und den Nutzen von Risikomanagement bzw. Risikoanalyse erkannt haben. Die Übertragung der Anwendung auf Law Enforcement Agencies ist bei entsprechenden Anpassungen möglich. Als Problem kristallisiert sich heraus, dass unterschiedliche Auffassungen und abweichendes Verständnis über Begrifflichkeiten, Definitionen sowie Art und Weise der Implementierung vorherrschen. Dies führt zu Missverständnissen, Missinterpretationen und nicht vergleichbaren Ergebnissen. Nach Meinung des Verfassers, und dies wurde von den Interviewpartnern bestätigt, wäre es aber im Zuge der fortschreitenden, europäischen Einigung wünschenswert, einheitliche Standards beim Risikomanagement festzulegen. Zu bedenken gegeben wurde auch, dass nationale, gesetzliche Bestimmungen genau diese einheitlichen Standards verhindern. Diese Ansicht kann nicht geteilt werden, da in diesen Bestimmungen lediglich festgehalten ist, dass Risikomanagement bzw. -analyse als Hilfsmittel anzuwenden ist. Die Art und Weise des Prozesses bzw. dessen Umsetzung ist nicht gesetzlich geregelt. Dies bedeutet, dass die Verantwortlichen den Freiraum besitzen, Risikomanagement nach ihren Vorstellungen zu implementieren.

Dieser Freiraum wäre der Ansatzpunkt dafür, generelles Risikomanagement unter der Verwendung eines gemeinsamen und standardisierten, europäischen Konzeptes einzuführen. Die dafür in dieser

Abhandlung abgegebenen Empfehlungen bezüglich einheitlicher Definitionen, des Risiko-Management-Handbuches und eines gemeinsamen Risikokataloges sind an die Vorgehensweise der freien Marktwirtschaft angelehnt, jedoch den Erfordernissen von Law Enforcement Agencies angepasst.

Mehrmals kritisch angemerkt wurde, dass die bereits bestehenden Modelle teilweise zu theoretisch seien und deshalb in der Praxis Schwierigkeiten bei der Umsetzung bestünden. Gelingt die Umsetzung, handelt es sich um Anwendungen, die sich bewährt haben. Fest steht aber auch, dass es sich bei diesen Modellen um spezielles Risikomanagement handelt, das auf die Bearbeitung des Risikobereiches Kriminalität fokussiert ist. Im Gegensatz dazu wird beim generellen Risikomanagement die gesamte Organisation einer Betrachtung unterzogen. Ein weiterer Vorteil besteht darin, dass es das spezielle Risikomanagement automatisch beinhaltet. Somit könnten bereits bestehende Modelle mit berücksichtigt werden. Letztendlich wären damit nach Meinung des Verfassers mehrere Ziel erreichbar. Zum einen würde es im Bereich Risikomanagement zu einer Qualitätssicherung und -steigerung bei Law Enforcement Agencies kommen. Zum anderen beruhen die erzielten Ergebnisse auf einer einheitlichen Anwendung und sind somit organisations- und länderübergreifend vergleichbar.

[1] *Als „Law Enforcement Agencies" werden alle Behörden und Organisationen bezeichnet, die Gesetze um- bzw. durchsetzen. Dies können sowohl nationale Staats- oder Bundesbehörden als auch internationale Organisationen (z.B. INTERPOL, EUROPOL) sein.*

[2] *Masterarbeit des Verfassers: „Risikomanagement im Zuge der europäischen Grenzsicherung". Erstellt im Rahmen des Fachhochschul-Masterstudiengangs „Strategisches Sicherheitsmanagement" an der FH Wiener Neustadt, 2013.*

[3] *In die Studie wurden die Länder Bosnien-Herzegowina, Kroatien, Ungarn und Deutschland (Bayern) sowie die Organisationen EUROPOL und FRONTEX miteinbezogen.*

[4] *Die zu Grunde gelegten Erkenntnisse wurden durch Literaturrecherche und Sekundäranalyse im Zusammenhang mit der Erstellung der o.g. Masterarbeit (Waldbauer-Hable 2013) erhoben.*

[5] *Risiko ist der Faktor aus Eintrittswahrscheinlichkeit x Schadensausmaß.*

[6] *Risiko ist ein Informationsdefizit.*

[7] *Risiko = Gefahr.*

[8] *In einigen Dokumenten findet sich auch die Anschauung, dass Risikoanalyse ein eigenständiger Punkt zwischen Risikoidentifizierung und Risikobewertung ist. Diese Sichtweise wird vom Verfasser nicht geteilt.*

[9] *Das US Department for Homeland Security ist ein von der US-Regierung geschaffenes Department, welches die Aufgabe hat, das US-Staatsgebiet und die dazu gehörigen Territorien vor terroristischen Angriffen, Angriffen von Einzeltätern und Naturkatastrophen zu schützen bzw. darauf zu antworten. Die Schaffung gilt als Antwort auf die Erfahrungen des 11. September 2001.*

[10] *Beim ISO Guide 73 (ISO Guide 2009) handelt es sich um ein „Risk Management Vocabulary", mit dem ein gegenseitiges und gleiches Verständnis von Begriffen aus dem Risikomanagement erzielt werden soll.*

[11] *Ein Risiko-Management-Handbuch dient zur Festlegung der einzelnen Schritte bei der Implementierung des Risikomanagements. Auf diese Weise wird gewährleistet, dass Organisationen, die sich an diesem Handbuch orientieren, einheitliche Standards umsetzen.*

[12] *Risikotragfähigkeit ist ein Begriff, der bei den Bewältigungsstrategien verwendet wird und beschreibt, inwieweit eine Organisation in der Lage ist, Risiken zu ertragen. Um das Erreichen speziell der oberen Grenze der Risikotragfähigkeit einer Organisation zu erkennen, werden oftmals Limits eingesetzt.*

Quellenangaben

Deutsches Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2010). Methode für die Risikoanalyse im Bevölkerungsschutz, Bonn.

European Commission/EuropeAid Cooperation Office, Directorate E – Quality of Operations (2009). Guidelines for Integrated Border Management in EC External Cooperation, Brüssel.

Europäische Union (2002). Common Integrated Risk Analysis Model, CIRAM, Expertenkommission der EU Innen- und Justizminister, Brüssel.

FRONTEX (2011a). Common Integrated Risk Analysis Model, CIRAM, a comprehensive update, Version 2.0, Reference number: 16999, Warschau.

FRONTEX (2011b). Guidelines for Risk Analysis Units, Structure and Tools for the application of CRIAM Version 2.0, Reference number: 19232, Warschau.

Hölscher, Reinhold (2002). Von der Versicherung zur integrativen Risikobewältigung: Die Konzeption eines modernen Risikomanagements, in: Hölscher, Reinhold/Elfgen, Ralph (Hg.) Herausforderung Risikomanagement – Identifikation, Steuerung und Bewertung industrieller Risiken, Wiesbaden, 3–31.

ISO GUIDE 73 (2009). Risk Management Vocabulary, First Edition, ISO Guide 73:2009 (E/F), Genf.

Romeike, Frank/Hager, Peter (2009). Erfolgsfaktor Risikomanagement 2.0, Wiesbaden.

Strobl, Josef (1996). Theorie und Praxis des Polizeieinsatzes, Lübeck.

US Homeland Security Office (2006). Homeland Security Risk Assessment, Volume I. Setting, RP05-024-01a.

Voigt, Kai-Ingo (2013). Risikomanagement im Anlagenbau: Konzepte und Fallstudien aus der Praxis, Berlin.

Waldbauer-Hable, Peter (2013). Risikomanagement im Zuge der europäischen Grenzsicherung, Masterarbeit des Fachhochschul-Masterstudiengangs „Strategisches Sicherheitsmanagement", Wiener Neustadt.

Weiterführende Literatur und Links

EUROPOL, Analysis Unit (2002). Strategic Intelligence Analysis Course – reading material, Europol 2002, File No: 2520-47 Rev 1, Den Haag.