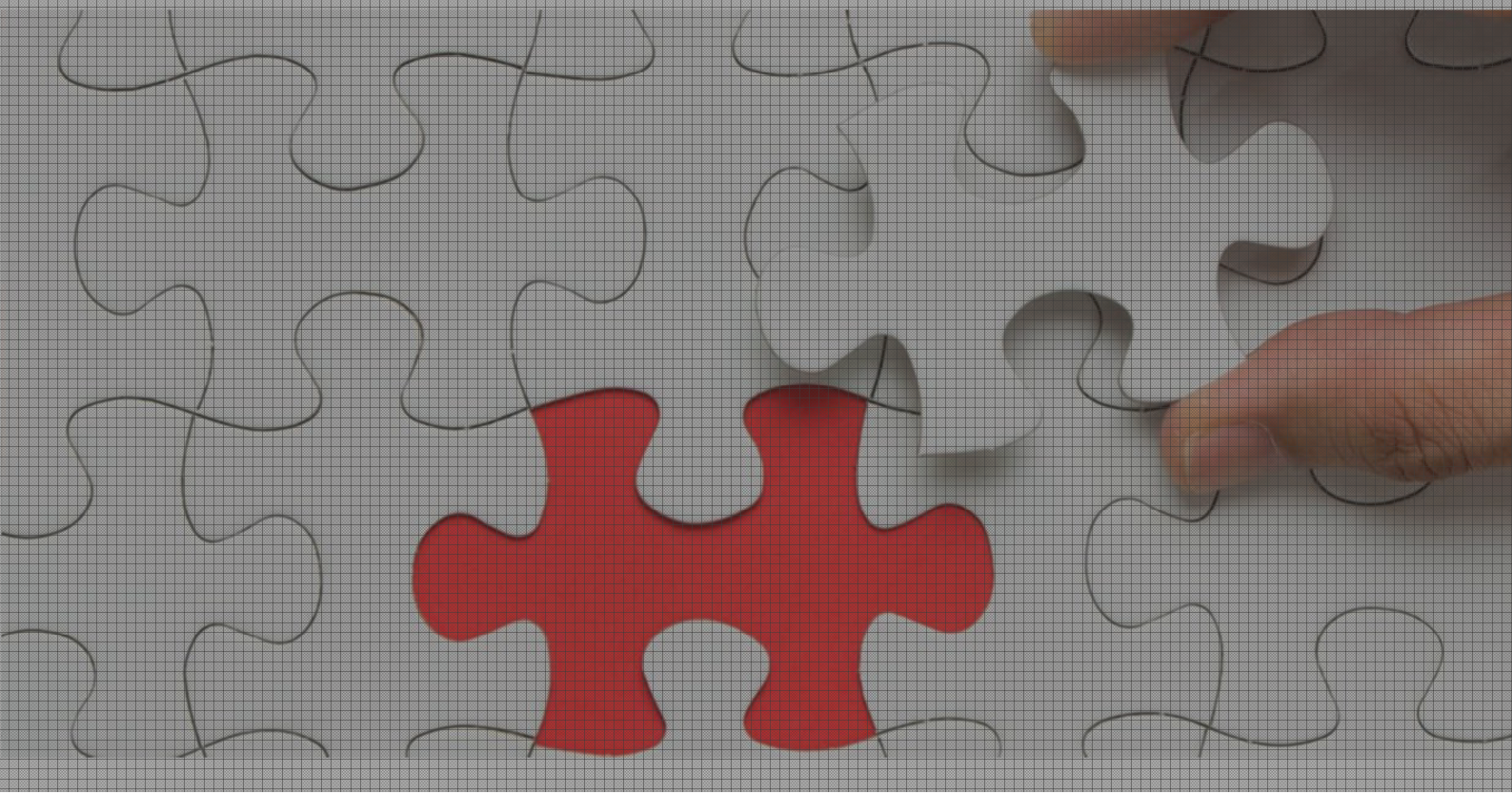
VERTRAULICHER FATF-BERICHT

# Aufdeckung von Terrorismusfinanzierung: *Relevante Risikoindikatoren*

**Juni 2016**



**Arbeitsübersetzung des Bundeskriminalamtes**

# Aufdeckung von Terrorismusfinanzierung (TF): *Relevante Risikoindikatoren*

Die FATF hat die in diesem Bericht genannten Anhaltspunkte erarbeitet, um Regierungsbehörden und ausgewählte Unternehmen des Privatsektors bei der Aufdeckung und Unterbindung der Geldflüsse von Terroristen und Terrororganisationen zu unterstützen. Die FATF hat beschlossen, den vorliegenden Bericht nicht öffentlich zugänglich zu machen, um den Nutzen der Indikatoren und der sonstigen relevanten Informationen zu bewahren.

Die nationalen zuständigen Behörden sind für die Weitergabe des Berichts an die entsprechenden Unternehmen des Privatsektors in ihrem Land verantwortlich. Die Empfänger des Berichts müssen die Informationen vertraulich behandeln und dürfen sie ohne vorherige Genehmigung durch ihre nationale zuständige Behörde nicht vervielfältigen, freigeben oder auf andere Weise an Dritte weitergeben.

© FATF
Juni 2016

© 2016 - **nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt**

## ABKÜRZUNGSVERZEICHNIS

| | |
|---|---|
| **AML/CFT** | Anti-money laundering (Geldwäschebekämpfung)/ countering the financing of terrorism (Bekämpfung der Terrorismusfinanzierung) |
| **ATM** | Automated Teller Machine (Geldautomaten) |
| **CDD** | Customer due diligence (Kundensorgfaltspflichten) |
| **CIFG** | Counter ISIL Finance Group (*Verbund gegen ISIL-Finanzierung*) |
| **FATF** | Financial Action Task Force |
| **FIU** | Financial Intelligence Unit |
| **FTF** | Foreign terrorist fighter (Ausländische Terrorkämpfer) |
| **FTZ** | Free trade zones (Freihandelszonen) |
| **HOSSPs** | Hawala and other similar service providers in money laundering and terrorist financing (Hawala und ähnliche Dienstleister) |
| **ISIL** | Islamic State of Iraq and the Levant (Islamischer Staat im Irak und der Levante) |
| **KFR** | Kidnapping for ransom (erpresserischer Menschenraub) |
| **ML** | Money laundering |
| **MSB** | Money service business (Gelddienstleistungsunternehmen) |
| **MVTS** | Money value transfer systems (Geld-/ Werttransfersysteme) |
| **NPO** | Non-Profit Organisation |
| **STR** | Suspicious transaction reports (Verdachtsmeldungen) |
| **TF** | Terrorist financing (Terrorismusfinanzierung) |
| **TFS** | Targeted financial sanctions (gezielte finanzielle Sanktionen) |
| **TBML** | Trade-based money laundering (handelsbasierte Geldwäsche) |


**nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** - © 2016

## Zusammenfassung

Die Aufdeckung von Terrorismusfinanzierung (TF) ist für die Identifizierung von Netzwerken und Verdächtigen notwendig, nachdem ein Anschlag begangen wurde, ist aber auch entscheidend, um von vornherein zu verhindern, dass solch tragische Ereignisse geschehen. Seit 2001 steht die FATF an vorderster Front bei der Unterstützung des Privatsektors zum besseren Erkennen und Verstehen der Art und des Umfangs von Terrorismusfinanzierungsaktivitäten. Diese Arbeit hat angesichts der größer gewordenen Bedrohungen durch Terrorismusfinanzierung, mit denen wir jetzt weltweit konfrontiert sind, über die letzten zwei Jahre beträchtlich zugenommen. Die zwei im Jahr 2015 veröffentlichten Berichte *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)* und *Emerging Terrorist Financing Risks* haben zu einem besseren Verständnis der Weltgemeinschaft für Terrorismusfinanzierung geführt. Es ist jedoch angesichts der sich dynamisch und konstant weiterentwickelnden Art der Risiken und der Herausforderungen an die Aufdeckung von Terrorismusfinanzierung wichtig, dass die FATF detaillierte Informationen zur Unterstützung der Aufdeckung dieser Aktivitäten zur Verfügung stellt.

Der Bericht ist das Produkt umfangreicher Zulieferungen seitens des öffentlichen und des privaten Sektors. Er soll ein praktisches Werkzeug für beide Bereiche darstellen, um Terrorismusfinanzierung zu erkennen und um letztendlich terroristische Aktivitäten bereits vor Begehung zu verhindern. **Abschnitt I** stellt die verschiedenen Rollen und Verantwortlichkeiten der Bereiche dar; **Abschnitt III** zeigt die wechselseitigen Vorteile für beide Parteien, wenn starke Partnerschaften geschlossen werden. Ferner dient der vorliegende Bericht den zuständigen Behörden (besonders der Strafverfolgung) als Tool für die Zusammenarbeit mit Institutionen des Privatsektors in ihren jeweiligen Ländern. Die zuständigen Behörden werden daher gebeten, einen effizienten Weg des Austauschs der Informationen mit dem Privatsektor zu schaffen, ohne dass hierdurch laufende Ermittlungsverfahren und Anstrengungen im Ermittlungsbereich, auf denen die Anhaltspunkte zum Teil basieren, beeinträchtigt werden.

Ein Risikoindikator zeigt oder suggeriert die Wahrscheinlichkeit des Vorliegens verdächtiger Aktivitäten. Der Bericht beschreibt, wie sowohl der öffentliche als auch der private Sektor die Anhaltspunkte effizient nutzen sollte, da sie weder vollständig noch in jeder Situation anwendbar sind. Die Anhaltspunkte sind häufig nur eines von vielen Elementen, die zu einem besseren Gesamtbild des potentiellen Terrorismus- oder Terrorismusfinanzierungsrisikos beitragen. Wichtig ist, dass die Anhaltspunkte (oder ein einzelner Anhaltspunkt) nicht isoliert betrachtet werden. Sie müssen im Zusammenhang mit Informationen betrachtet werden, die aus der Zusammenarbeit mit den entsprechenden Behörden stammen. Jedes Land sollte seinem Privatsektor daher die Anhaltspunkte und Informationen zur Verfügung stellen, die für das Land von größter Relevanz sind (dies unter Nutzung von bestehenden Tools und Methoden für den sicheren Informationsaustausch). Die zuständigen Behörden sollten auch vermeiden, das vorliegende Dokument als Checkliste bei der Überprüfung von Institutionen des Privatsektors zu nutzen, da nicht alle Anhaltspunkte auf alle Länder oder alle Institutionen anwendbar sind.

Terrorismusfinanzierung ist aufgrund seiner Natur extrem schwer aufzudecken. Nicht nur, weil es häufig um kleinere Geldbeträge und nicht um Geldwäscheaktivitäten geht, sondern weil es sich um Transaktionen handelt, die häufig von rechtmäßigen Alltagsgeschäften nicht zu unterscheiden sind. Es ist daher unmöglich, eine abschließende Liste von Anhaltspunkten zu erstellen oder die "Wunderwaffe" zur Aufdeckung von Terrorismusfinanzierung zu liefern. Daher werden trotz der detaillierten und speziellen Informationen, die dieser Bericht enthält, weiterhin große Wissenslücken bestehen. Diese Lücken können durch einen verbesserten Informationsaustausch, wie in Abschnitt III beschrieben - insbesondere durch Austausch von Hintergrundinformationen zur Verbesserung der Risikoindikatoren - geschlossen werden.

© 2016 - **nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt**

Der Beratungsprozess zu diesem Bericht hat unser Verständnis darüber gestärkt, wie Institutionen des Privatsektors Anhaltspunkte und andere Mechanismen zur Feststellung von Aktivitäten im Zusammenhang mit Terrorismus nutzen. Der vorliegende Bericht soll den Ländern als ein weiterer Katalysator dienen, um ihre Kommunikation und Interaktionen mit dem Privatsektor zu verbessern. Diese laufende Interaktion wird dazu dienen, die Aufdeckung von Terrorismusfinanzierung zu verbessern und wird auch die künftigen Bemühungen der FATF zur Bekämpfung von Terrorismusfinanzierung verbessern.


**nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** - © 2016

# I. EINLEITUNG

## A. ZWECK, UMFANG UND ZIELE

Der Bericht *Emerging Terrorist Financing Risks* (FATF, 2015b) unterstreicht die Wichtigkeit echter Partnerschaften zwischen der öffentlichen Hand und dem Privatsektor zur Schärfung des Bewusstseins für - und Reaktionen auf - neu auftauchende Risiken der Terrorismusfinanzierung (TF). Durch präzise und vorausschauende Handlungsempfehlungen für den Privatsektor werden dessen Monitoring- und Screening-Prozesse sowie die Meldezeit sensibler Transaktionen mit möglichem TF-Bezug verbessert. Diese enge Zusammenarbeit hilft, TF-Risiken festzustellen und zwischen allen beteiligten Parteien zu kommunizieren.

Der vorliegende Bericht ist eine Fortschreibung des Berichts *Emerging Terrorist Financing Risks* und hat das Ziel, Risikoindikatoren zu entwickeln, mit denen der private und der öffentliche Sektor TF-Risiken erkennen und minimieren können soll. Ziel ist es, diese Art von Informationen dem privaten Sektor durch die entsprechenden Behörden zur Verfügung zu stellen. Der Bericht enthält einen Abschnitt zur Verbesserung der Zusammenarbeit mit dem Privatsektor, um eine regelmäßigere und konkretere Sensibilisierung und die Verbreitung der Anleitung zu Risikoindikatoren zu erzielen.

## B. METHODIK, TEILNEHMER UND VERWENDETE DATEN

Dieser Bericht wurde unter der gemeinsamen Leitung von Frankreich und den Vereinigten Staaten (USA) erstellt und beinhaltet Beiträge von einer Vielzahl weiterer Delegationen innerhalb des weltweiten Netzwerks der FATF. Die Delegationen beider Länder und Unternehmen des Privatsektors haben über 30 Indikatoren zu Terrorismusfinanzierung vorgelegt, die in Abschnitt II des Berichts einflossen. Einige der Informationen basieren auf der strategischen Auswertung der Daten der FIUs. In den meisten Fällen **wurden die Informationen in der Absicht übermittelt, sie nicht öffentlich zugänglich zu machen. Daher ist der Bericht vertraulich und nicht zur weiteren Verbreitung bestimmt.** Viele der eingegangenen Anhaltspunkte bezogen sich auf bestimmte Länder oder geographische Bereiche. Der vorliegende Bericht hingegen liefert allgemeinere Anhaltspunkte, die auf individuelle Umstände zugeschnitten werden könnten.

Er basiert auch auf der Erfahrung und dem Wissen, das die Delegationen durch ihre Teilnahme an mehreren Typologie Workshops vermittelt haben, die innerhalb des weltweiten Netzes der FATF abgehalten wurden, sowie auf Diskussionen bei der FATF-Tagung, die im Februar 2016 mit dem privaten Sektor zu Terrorismusfinanzierung veranstaltet wurde. Ziel dieser Tagung waren Gespräche über "Good Practices" für Partnerschaften zwischen den staatlichen Stellen und der Privatwirtschaft zur Feststellung von Risikoindikatoren und zum Informationsaustausch zur Aufdeckung von Terroristen oder Terrorismusfinanzierung. Das auf dieser Tagung erhaltene Feedback ist in den vorliegenden Bericht eingeflossen. Die FATF hat auch eine gemeinsame Sitzung mit der "Counter ISIL Finance Group" (CIFG) zur weiteren Intensivierung der gemeinsamen Arbeit im Kampf gegen die Finanzierung des IS und zum Schutz des internationalen Finanzsystems vor Missbrauch durch die Terrororganisation veranstaltet. Experten der CIFG trugen ebenfalls zu diesem Bericht bei, besonders durch Zulieferung von Anhaltspunkten betreffend IS-Finanzierung (z. B. Abschnitt II (G) - Anhaltspunkte betreffend die Erdöl- und Gasindustrie).

Darüber hinaus hat die FATF weltweit einen Fragebogen zum Thema, wie die zuständigen Behörden Informationen über TF-Risiken mit dem Privatsektor austauschen, verteilt und erhielt über 40

Antworten. Drei Kernprobleme ergaben sich. Sie bezogen sich auf (1) Feedback an Meldestellen, (2) Arten der ausgetauschten Informationen und (3) Mechanismen zur Zusammenarbeit mit dem Privatsektor. Abschnitt III dieses Berichts befasst sich mit diesen Fragen.

## C. Begrifflichkeiten

International hat man große Erfahrung mit Risikoindikatoren oder Anzeichen für Geldwäsche oder illegale Finanzströme. Die FATF hat in einer Reihe ihrer Berichte versucht, Anhaltspunkte zu entwickeln, um dem Finanz- und dem staatlichen Sektor zu helfen, Fälle von Geldwäsche oder Terrorismusfinanzierung zu erkennen. Das Erkennen von konkreten Anhaltspunkten für Terrorismusfinanzierung stellt jedoch aus verschiedenen Gründen eine andere (und schwierigere) Herausforderung dar. Der Begriff Risiko ist weit gefasst und komplex. Im vorliegenden Bericht wird der Begriff "Red Flag" nicht verwendet. Er wird sich auf die Verwendung eines allgemeinen Ausdrucks, ***Risikoindikator,*** beschränken, der helfen soll, Fälle terroristischer Aktivitäten oder TF-Aktivitäten zu erkennen. Ein Risikoindikator zeigt oder suggeriert die Wahrscheinlichkeit des Vorliegens verdächtiger Aktivitäten. Während eine Reihe der festgestellten Faktoren möglicherweise keine direkte Verbindung zu Terrorismus oder Terrorismusfinanzierung zu haben scheinen, sind sie dennoch beim Versuch relevant, diese Art von Aktivität aufzudecken. Ein Anhaltspunkt oder eine Reihe von Anhaltspunkten können einen Hinweis liefern, der genauerer Auswertung bedarf. Die festgestellten Anhaltspunkte sind nur ein Aspekt eines größeren Gesamtbilds möglicher Terrorismus- oder Terrorismusfinanzierungsrisiken.

Durch die FATF wurde im Jahr 2002 die Anleitung *Guidance for Financial Institutions in Detecting Terrorist Financing* veröffentlicht. Die Anleitung unterschied Terrorismusfinanzierungsindikatoren nicht von Geldwäscheindikatoren. Wie oben erwähnt, können viele relevante Risikoindikatoren nicht direkt mit Terrorismusfinanzierung oder Geldwäsche in Verbindung gebracht werden. Durch jüngste Bemühungen konnten konkrete oder spezifische TF-Methoden und -Techniken besser festgestellt und verstanden werden. Mit den jüngsten FATF-Recherchen wurde versucht, bestimmte Transaktionen oder Verhaltensmuster zu erklären, die ausschließlich oder eher wahrscheinlich mit TF-Techniken oder Aktivitäten in Verbindung stehen. Terrorismusfinanzierung betrifft im Vergleich zur Wäsche von Geldern aus Straftaten häufig kleinere Geldbeträge, die lokal generiert werden. Dieser Unterschied macht die Aufdeckung von Geldern, die für den Terrorismus bestimmt sind, schwieriger als die Aufdeckung von Geldwäscheaktivitäten im großen Stil.

## D. Zielgruppe

Die in diesem Bericht genannten Anhaltspunkte sind gleichermaßen für den öffentlichen wie für den privaten Sektor relevant. Nicht alle Anhaltspunkte werden vom privaten Sektor ohne zusätzliche Hintergrundinformationen der zuständigen Behörden erkannt werden (siehe Abschnitt III). Im Privatsektor sollen die Anhaltspunkte von Mitarbeitern genutzt werden, die für Compliance, Transaktionsmonitoring, Ermittlungsarbeit oder sonstige FIU-bezogene Operationen bei den Finanzinstituten und den Gelddienstleistungsunternehmen (Money Services Businesses, MSB) zuständig sind. Die Anhaltspunkte sind für den Banksektor besonders wichtig, könnten aber auch für Finanztransferdienstleister und Wechselstuben gelten. Die meisten Indikatoren - besonders die, die sich auf Verhalten beziehen - gelten für das Privatkundengeschäft, aber es gibt auch einige Anhaltspunkte, die eher für das Firmenkundengeschäft relevant sind, z. B. Abschnitt II.G. Die Anhaltspunkte sollen für eine Vielzahl verschiedener Kunden gelten - von Personen mit bescheidenen Mitteln bis zu Personen mit hohem Nettoeinkommen - und weitestgehend die verschiedenen Aspekte einer Kundenbeziehung umfassen. Die Anhaltspunkte sind auch auf kleine Unternehmen, Mittelständler und große Firmenzusammenschlüsse anwendbar.


**nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** - © 2016

Die Anhaltspunkte sind auch relevant für die zuständigen Behörden, insbesondere die FIUs, Strafverfolgungs- bzw. Sicherheitsbehörden, die für operative und strategische Auswertung von TF-Trends verantwortlich sind. Die Anhaltspunkte können den Behörden auch beim Erkennen von TF-Verhalten aus ihrer jeweiligen Perspektive helfen. Der vorliegende Bericht steht den zuständigen Behörden in der Absicht zur Verfügung, dass sie ihn bzw. die enthaltenen Informationen an Unternehmen des privaten Sektors weitergeben (siehe Abschnitt III zu Weitergabe von Hintergrundinformationen zur Verbesserung der Risikoindikatoren). Die zuständigen Behörden können die in diesem Bericht enthaltenen Informationen auch dafür nutzen, eigene Ratgeber für die Meldestellen zu erstellen. Der Bericht soll jedoch NICHT als Regelwerk für Compliance- und Prüfzwecke genutzt werden. Dies könnte unbeabsichtigt zu einem regelbasierten Ansatz bei der Risikofeststellung führen. Die FATF wird die Weitergabe und Nutzung dieses Berichts beobachten, um einen maximalen Nutzen zu gewährleisten.

## E. Nutzung der Anhaltspunkte

Die festgestellten Anhaltspunkte sind sehr umfassend, sie beschreiben bestimmte Aktivitäten und Situationen, sind aber dennoch allgemein genug, um eine angepasste Anwendung zu ermöglichen. Die Kategorien sind exemplarisch und sollen sensibilisieren, damit weitere Recherchen und Auswertungen durchgeführt werden können zur Feststellung, ob bei bestimmten Transaktionen, Verhalten und Aktivitäten hinreichender Verdacht auf Terrorismusfinanzierung besteht. Dieser Bericht soll nicht als Grundlage für pauschale oder undifferenzierte "De-Risking Practices" oder sonstige Aktivitäten genutzt werden, die zu beträchtlichen unbeabsichtigten Konsequenzen jenseits des Ziels der Verhinderung von Terrorismusfinanzierung führen könnten.

Die vorgelegten Anhaltspunkte stammen aus einer Auswahl der eingegangenen Daten; es handelt sich keinesfalls um eine abschließende Aufstellung. Ein einzelner Anhaltspunkt allein kann nicht den Verdacht der Terrorismusfinanzierung rechtfertigen bzw. einen klaren Hinweis auf solche Aktivitäten liefern. Ferner muss das Vorliegen eines einzelnen Anhaltspunkts nicht notwendigerweise zur Verdachtsschöpfung führen, kann aber ggf. weiteres Monitoring und Überprüfungen auslösen. Ähnlich könnte das Vorliegen mehrerer Anhaltspunkte im Zusammenhang mit einem Kunden oder einer Transaktion Überprüfungen rechtfertigen. Das Feststellen eines oder mehrerer Anhaltspunkte hängt von den Geschäftsfeldern, den Produkten oder den Dienstleistungen ab, die ein Institut anbietet und wie es mit seinen Kunden interagiert, sowie von seinen personellen und technologischen Ressourcen.

Eine Reihe der hier aufgeführten Anhaltspunkte sind zu weit gefasst und bedürfen zur Verdachtsschöpfung eines weiteren Monitoring, einer weiteren Überprüfung oder Hintergrundinformationen über den Kunden oder die Transaktion. Viele der Anhaltspunkte beschreiben normale Alltagsaktivitäten. Es wird betont, dass der Privatsektor Hintergrundinformationen der Strafverfolgungsbehörden und der FIUs benötigen wird, um die Anhaltspunkte bestmöglich nutzen zu können. Angesichts der Tatsache, dass es immer neue TF-Risiken gibt, sind die Anhaltspunkte selbst dynamisch. Bei Nutzung der Anhaltspunkte sollten die Unternehmen die Gesamtheit des Kundenprofils berücksichtigen, einschließlich der Informationen aus dem Customer Due Diligence-Prozess (CDD), sowie sonstiger Risikofaktoren im Kontext. Die Meldestellen werden nicht immer in der Lage sein, eine Verbindung zwischen verdächtigem Kundenverhalten und terroristischen Aktivitäten herzustellen. Dennoch kann jedes Verdachtsmoment, das den FIUs gemeldet wird, ein kleines aber wesentliches Teilchen eines größeren Puzzles sein und kann wesentlich sein für den Erfolg der von den zuständigen Behörden geführten Ermittlungen zu

Aktivitäten der Terrorismusfinanzierung und damit in Zusammenhang stehenden terroristischen Aktivitäten.

Die Anhaltspunkte sollen Monitoring- und Meldesysteme betreffend verdächtige Aktivitäten unterstützen und mittels eines risikobasierten Ansatzes zu tiefergehenden Analysen beitragen. Monitoringsysteme beinhalten normalerweise Mitarbeiteridentifizierung oder -verweise, transaktionsbasierte (manuelle) Systeme, (automatisierte) Überwachungssysteme oder eine Kombination aus diesen. Einige der Anhaltspunkte können beim allgemeinen Transaktionsscreening festgestellt werden, während sich andere erst bei einer eingehenden Analyse oder Prüfung der Fälle zeigen dürften.

Beispielsweise nutzen einige Banken proaktives Data-Mining zur Identifizierung von ausländischen Terrorkämpfern (Foreign Terrorist Fighters - FTF) und mit ihnen in Verbindung stehenden Netzwerken, indem sie die Zahlungsaktivitäten und Kontonutzung ihrer Kunden beobachten (einschl. Debit-/Kreditkartennutzung). Dies umfasst die Überprüfung der Kundendaten von Verdächtigen, wie Anschrift und Zahlungsdaten. Dies geschieht häufig über Warnmeldungen, die von den FIUs unter Angabe von Anhaltspunkten herausgegeben werden. Dieser proaktive Ansatz unterstützt häufig die Erarbeitung des Schwerpunkts für weitere Ermittlungen oder ein verstärktes Monitoring. Der Privatsektor hat auch als Beispiel ein Schaubild mit der Phase des Kundenmonitoring-Prozesses zur Verfügung gestellt, wo diese Indikatoren erkennbar sein könnten. Das Beispiel zeigt, dass einige Anhaltspunkte während des anfänglichen CDD-Verfahrens oder bei automatisierten Überwachungsprozessen festgestellt werden können, aber in vielen Fällen wird es spezielle Tools, weitere Ermittlungen oder Erkenntnisse der Strafverfolgungsbehörden brauchen, um sie festzustellen.

Der größere Teil der Anhaltspunkte könnte zu Problemen bei der Handhabung dieser Informationen führen, besonders für kleinere Institute. Einige Institute könnten die Anhaltspunkte in ihre automatisierten Systeme integrieren wollen (z. B. unter Nutzung von Filterkriterien oder Regeln), wodurch der Ermessensspielraum der Mitarbeiter reduziert, die Möglichkeit zur Feststellung von Unregelmäßigkeiten jedoch gesteigert werden könnte. Systemfilterkriterien, einschl. spezieller Profile und Regeln, sollten darauf basieren, was angemessen und für die jeweiligen Kontoarten zu erwarten ist. Einige Anhaltspunkte, wie z. B. die im Zusammenhang mit Ausgabeaktivitäten, können nicht automatisiert werden, was ihr Monitoring erschweren könnte. Anhaltspunkte, die automatisiert festgestellt werden können, erfordern möglicherweise, dass Meldestellen ihre IT-Kapazitäten oder Management-Informationssysteme (z. B. Standortbestimmung von Internetverbindungen und Abhebungen in Grenzgebieten, Art der Ausgabeaktivitäten) ausbauen.


**nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** - © 2016

# II. RISIKOINDIKATOREN ZUR AUFDECKUNG VON TF-AKTIVITÄTEN

Die FATF-Standards stellen sowohl dem öffentlichen als auch dem privaten Sektor eine Hilfestellung zur Identifizierung von TF-Aktivitäten bereit. Die Standards wurden 2012 überarbeitet, um die Definition der sogenannten „Hoch-Risiko-Bereiche“ zu konkretisieren und damit den o.g. Sektoren einen fokussierteren Ansatz dort zu ermöglichen, wo weiterhin ein hohes Risiko besteht, insbesondere im Zusammenhang mit Terrorismusfinanzierung. Die exakte Bewertung von TF-Risiken erfordert eine vielschichtige Analyse von Kunden, ihren Aktivitäten und den bekannten Risiken, die mit einem Produkt, einem Land oder einem Transaktionstyp in Verbindung stehen.

Kunden-, Produkt- und geographische Risiken sind drei allgemeine Kategorien, die bei der CDD betrachtet werden, und sie können konkrete höhere Risikoindikatoren aufweisen, die weitergehende Maßnahmen erfordern. Angesichts der Besonderheit der Terrorismusfinanzierung wurden im vorliegenden Bericht spezielle TF-Risikokategorien anhand folgender Kriterien erstellt:

A. Kundenverhalten
B. wirtschaftliches Profil
C. geographisches Risiko
D. Ausgabeaktivitäten
E. Produkte / Dienstleistungen
F. Non-Profit Organisationen (NPOs) und
G. Handel und Wirtschaftsunternehmen

Die Einstufung ist flexibel und in vielen Fällen können Anhaltspunkte in mehreren Kategorien

bestehen.

## A. ANHALTSPUNKTE MIT BEZUG ZU KUNDENVERHALTEN

Die Kenntnis über einen Kunden spielt eine wichtige Rolle beim Verständnis des finanziellen Verhaltens eines Kunden in Bezug auf seine nicht-finanziellen Aktivitäten und auf die Gesamtkundenbeziehung. Bei der Entwicklung von Anhaltspunkten sollte der private Sektor Informationen aus einer Reihe von Quellen betrachten, darunter unter anderem die Auswertung interner Transaktionsdaten, die Überprüfung der Internet-Protokoll-Daten (IP), die Analyse verdächtiger Daten, besonders in Bezug auf potentielle TF-Vorkommnisse, sowie alle Erkenntnisse der Strafverfolgungsbehörden. Die Institute führen häufig ein Transaktionsmonitoring, Namensscreening und erweiterte CDD bei Kunden durch, die finanzielle oder subjektive Verbindungen zu Personen/Gruppierungen, Unternehmen (z. B. Industrie, NPOs) oder Ländern mit hohem Risiko haben.

Die FATF hat immer deutlich gemacht, dass Terrorismus und diejenigen, die ihn unterstützen, nie mit einer Religion, Nationalität, Kultur oder Ethnie in Verbindung gebracht werden können. Wo Terroristen, terroristische Gruppierungen oder diejenigen, die Terrorismus unterstützen, behaupten, mit bestimmten Hintergründen in Verbindung zu stehen, kann ein solches Verhalten zum Zwecke der risikobasierten Due Diligence berücksichtigt werden. Dieses Verhalten umfasst radikale, extremistische oder gewalttätige Denkweisen, die vermutlich der Religion, dem Nationalismus oder der Ethnie entstammen. Diesbezüglich sollten Anstrengungen unternommen werden zum Verständnis, was radikalisiertes oder extremistisches Verhalten darstellen könnte, das eine potentielle Terrorgefahr birgt,

© 2016 - **nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** 

im Vergleich zu Verhalten, das eher im üblichen Rahmen der Ausübung des Glaubens und der Überzeugungen innerhalb des Landes oder der Region liegt.

### Aufbau einer Geschäftsbeziehung

Beim Aufbau einer Geschäftsbeziehung mit einem Kunden sollte der Name des potentiellen Kunden mit Personen und Unternehmen abgeglichen werden, die auf Listen gezielter Finanzsanktionen stehen, die entsprechend nationalem oder internationalem Recht und Verfahren erstellt wurden[1]. Die Meldestellen und die zuständigen Behörden sollten auch Personen oder Unternehmen überprüfen, die von anderen Ländern gelistet wurden. Durch die Vereinten Nationen wurden kürzlich alle Sanktionslisten (inkl. TF-Sanktionen (TFS)) zu einer UN-Sanktionsliste zur Erleichterung der Compliance zusammengeführt[2]. Die „Consolidated Sanctions List" enthält alle Personen und Unternehmen, die Gegenstand von Sanktionsmaßnahmen des UN-Sicherheitsrats sind. Während mit gelisteten Personen eindeutig keine Geschäfte gemacht werden sollten, sollte bei Personen, die mit gelisteten Personen in Verbindung stehen - einschließlich Repräsentanten, wirtschaftlich Berechtigten, Mitbewohnern, nahen Verwandten oder anderen Personen im Umfeld einer gelisteten Person - ebenfalls eine erweiterte Sorgfaltspflicht in Betracht gezogen werden. Dies umfasst das Monitoring von Transaktionen, die von einer Person in Auftrag gegeben werden, die einer gelisteten Person bekanntermaßen nahe steht. Zu den Informationen, die beim Abgleich der TFS-Listen zu berücksichtigen sind, gehören die Folgenden:

- Namen, Aliasnamen, Geburtsdaten und sonstige Identifizierungsmerkmale von Personen, die in Terrorismus verstrickt sind und auf nationalen oder internationalen TFS-Listen stehen, können registrierten Kunden, Begünstigten und Unternehmen zugeordnet werden.
- Anschriften von Personen, die in Terrorismus verstrickt sind und auf nationalen oder internationalen TFS-Listen stehen (falls vorhanden), können häufig registrierten Kunden, Begünstigten und Unternehmen zugeordnet werden.
- Geld oder sonstiges Vermögen von an Terrorismus beteiligten Personen, die auf nationalen oder internationalen TFS-Listen stehen, kann anderen Unternehmen oder Kunden zugeordnet werden.

Durch das Monitoring öffentlich zugänglicher in- und ausländischer Medien kann die Aufdeckung neuer Kunden mit hohem Risiko unterstützt werden. Externe Recherche-Tools können auch helfen, ein gutes Verständnis für Personen zu entwickeln, die mit einer Transaktion in Verbindung stehen. Unternehmen sollten Negativpresse oder nachteilige Medienberichte betreffend Kriminalität im Zusammenhang mit Terrorismusfinanzierung, illegale Finanzierung oder sonstige Negativnachrichten zu Kunden mit hohem Risiko, Auftraggebern, Geschäftsoperationen sowie persönlichen oder geschäftlichen Beziehungen berücksichtigen. Informationen auf Seiten sozialer Medien, die von Terrororganisationen oder radikalisierten Personen besucht werden, können bei der Auswertung potentiell verdächtiger Aktivitäten und der Feststellung von Anhaltspunkten für Terrorismusfinanzierung von Nutzen sein.

Meistens ist es schwierig, TF-bezogene Aktivitäten ohne zusätzliche Erkenntnisse der zuständigen Behörden zu erkennen. Die Erkenntnisse der zuständigen Behörden werden oft Typologien oder

[1] Siehe *International Best Practices on Targeted Financial Sanctions for Terrorist Financing* (FATF, 2013a).
[2] *Consolidated United Nations Security Council Sanctions List* (UNSC)


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

Fallstudien enthalten. Obwohl die zuständigen Behörden Hintergrundinformationen mit Finanzinstituten zu Personen, die mit einem TF-Ermittlungsverfahren in Verbindung stehen, oft erst nach dessen Abschluss austauschen können, werden sie in einigen Fällen Erkenntnisse übermitteln, um terroristische Aktivitäten zu verhindern (siehe auch Abschnitt III). Folgende Punkte sind u. a. zu berücksichtigen:

- Personen, denen bereits Terrorismus oder damit in Zusammenhang stehende Straftaten zur Last gelegt wurden.
- Personen, von denen bekannt ist oder die im Verdacht stehen (z. B. Gegenstand von Ermittlungen sind), an terroristischen Aktivitäten beteiligt zu sein oder als ausländische Terrorkämpfer zu agieren.
- Einträge in sozialen Medien, die Radikalisierung oder gewalttätigen Extremismus unterstützen oder fördern.
- Bekannte oder verdächtige Handynummern, die von Terroristen oder Verdächtigen genutzt werden.
- Einzelheiten zu Untergrund-Unterstützern, Sympathisanten oder Helfern.

Nachstehend ein Beispiel für zusätzliche Risikoindikatoren, die für Kundenverhalten bei Aufbau einer Geschäftsbeziehung relevant sind und als relevante Risikoindikatoren für TF in Betracht gezogen werden könnten:

- Widerstand gegen kulturelle Normen des Landes, in dem der Kunde die Transaktion durchführt, wie auffällige Versuche des Kunden, persönlichen Kontakt mit Bankangestellten zu vermeiden (z. B. Verweigerung, das Geschäft mit weiblichen Angestellten durchzuführen).
- Verhalten, das radikale oder extremistische Denkweisen zeigt oder gewalttätige Tendenzen aufweist (z. B. Profile in den sozialen Medien mit zahlreichen Posts von Zeitungsartikeln mit Bezug zu oder sympathisierend mit Terrororganisationen).
- Vorlage von offensichtlich gefälschten oder neuen Ausweispapieren (z. B. totalgefälschter Stempel oder Lichtbild, Lichtbild über Stempel angebracht, Ausstellungsdatum passt nicht zum Zustand des Dokuments bezüglich Abnutzung).
- Neukunden, die den Bankangestellten übermäßig viele Fragen zu Verdachtsmeldungen, Meldeauflagen, Schwellenwerten oder Buchführungsauflagen stellen.
- Neukunden, denen es widerstrebt, Informationen preiszugeben.
- Kunden, die Transaktionen für eine andere Person durchführen oder für diese tätig sind.
- Ein Konto wird für eine juristische Person mit gleicher Anschrift wie die einer anderen natürlichen Person eröffnet, die nicht mit dem Konto in Verbindung gebracht wurde.
- Ein Konto wird gemeinschaftlich von zahlreichen Personen geführt oder genutzt, die weder geschäftlich noch persönlich etwas mit dem Kontoinhaber zu tun haben.
- Eine natürliche Person eröffnet mehrere Konten (z. B. Bankkonten, Prepaid-Karten, E-Wallets etc.) um Überweisungen in kleinen Stückelungen entgegenzunehmen oder zu tätigen.

© 2016 - **nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** 

- Eine natürliche Person eröffnet ein Konto nur zu dem Zweck, eine oder mehrere Überweisungen in Empfang zu nehmen und Geld abzuheben oder an andere Personen zu überweisen.
- Vorübergehende Wohnsitznahme bzw. häufiger Wohnsitzwechsel bzw. scheinbar ohne Bezug zum angegebenen Wohnsitz.
- Wiederholte Nutzung der gleichen Anschriften, Telefonnummern und Referenzen (z. B. Beschäftigung) bei mehreren Konten ohne scheinbaren Bezug, die auf verschiedene Namen eröffnet werden.
- Kontoeröffnung in Gegenden, die nicht im Lebens-/Arbeitsbereich des Kunden liegen, und ohne nachvollziehbaren Grund

## B. ANHALTSPUNKTE MIT BEZUG ZUM WIRTSCHAFTLICHEN PROFIL DES KUNDEN

Die Kundensorgfaltspflichten beginnen vor dem Aufbau einer Geschäftsbeziehung und werden fortgesetzt durch das Monitoring aller Veränderungen des Kundenverhaltens und seines wirtschaftlichen Profils (einschließlich Änderung der Geldquellen und Ausgaben). Verhaltensbezogene Anhaltspunkte für TF können auch im Laufe der Geschäftsbeziehung verifiziert werden. Dementsprechend sollten Anhaltspunkte, die während des laufenden Monitorings festgestellt werden, auf solche ausgeweitet werden, die nach Aufbau der Geschäftsbeziehung verifiziert werden können. Kenntnis über einen Kunden, einschließlich der Finanztransaktionshistorie, die zu dem Kunden festgestellt wurde, kann wichtig sein, wenn ein Verdacht der Terrorismusfinanzierung entsteht. Anzeichen dafür, dass Transaktionen nicht zu den üblichen Aktivitäten des Kunden passen, sind möglicherweise Folgende:

- Eine Person führt mehrere Transaktionen in der gleichen Filiale oder auch in verschiedenen Filialen mit der offensichtlichen Absicht durch, nicht von den gleichen Bankangestellten bedient zu werden.
- Der Kunde verwendet gekennzeichnete Finanzinstrumente (wie z. B. Schecks) mit informellen Notizen, Initialen oder Symbolen, wie z. B. eine Token-Nummer, die zur Identifizierung dienen sollen.
- Geschäftsbeziehung oder Vertrag (z. B. bei Zinskonten) wird ohne Erklärung beendet.
- Unerwartete Einzahlungen, Überweisungen oder Zahlungen aus dem Verkauf von Privatvermögen, Rentenkonten oder persönlichem Eigentum.
- Das Kundenkonto weist eine unerklärliche Zunahme an Einzahlungen und Geldflüssen auf.
- Auf Einzelkonten gehen eine Vielzahl von Überweisungen großer Beträge von Personen ohne Bezug oder aus unbekannten Quellen ein (z. B. angegebener Verwendungszweck "Unterhalt").
- Mehrere natürliche Personen, die nicht mit dem Kontoinhaber verwandt sind, sind Kontobevollmächtigte.
- Kunden, die nur widerwillig Identitätsangaben machen oder ihre jeweiligen Daten aktualisieren, oder dies ganz verweigern.
- Kunden, die jedes Mal andere Ausweispapiere vorlegen, wenn die Finanzinstitute sie dazu auffordern.
- Kunden, die bei ihren Geschäften Aliaspersonalien, Nicknames oder andere alternative oder vereinfachte Namensformen statt ihres eigenen


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

(vollständigen) Namens benutzen. Hierzu kann auch die Umstellung der Namensfolge gehören.

- Kunden, deren Adresse oder Erreichbarkeiten (Telefon, Fax, E-Mail-Adresse etc.) häufig wechseln oder nicht korrekt sind, oder die ständig unerreichbar sind, besonders, wenn die Kontaktversuche des Finanzinstituts kurz nach Aufbau einer Geschäftsbeziehung erfolgen.
- Überweisungen werden von verschiedenen Personen oder Unternehmen, bei denen eine oder mehrere Personalien gleich sind (z. B. Nachname, Anschrift, Arbeitgeber, Telefonnummer etc.), am gleichen Tag oder innerhalb von ein paar Tagen angewiesen.
- Häufigkeit oder Umfang der Transaktion stimmt nicht mit Beruf des Kunden, Einkommen oder Alter etc. überein.
- Plötzliche Abhebung großer Beträge (oft in bar) an Unterstützungszahlungen, die über einen Zeitraum von Monaten aufgelaufen sind.

Fallstudie: **Änderung des wirtschaftlichen Profils eines Kunden**

Eine Privatperson bat das Finanzinstitut um Auflösung seiner Zinskonten, ohne eine Erklärung abzugeben. Das Gesamtguthaben auf den Depotkonten wurde in bar abgehoben.

Der Bankangestellte erklärte, die Person habe sich geweigert, von weiblichen Angestellten der Bank bedient zu werden und hatte offenbar Kleidung und äußeres Erscheinungsbild geändert, was auf eine radikale Denkweise hinweisen könnte. Bei dem Konto wurde dann eine lange Phase der Inaktivität beobachtet.

*Quelle: Frankreich*

## C. ANHALTSPUNKTE MIT BEZUG ZU GEOGRAPHISCHEN RISIKEN

Bei der Bewertung von TF-Risiken sollten immer geographische Risiken, die mit dem Herkunftsland, dem Bestimmungsland und den Transitländern in Verbindung stehen, berücksichtigt werden. Dies umfasst Risiken in Verbindung mit dem Auftraggeber einer Transaktion und dem Begünstigten von Geldern, die mit Hochrisikoländern/-gegenden in Verbindung gebracht werden können. Ein geographisches Risiko könnte auch auf die Staatsangehörigkeit, den Wohnsitz oder den Geschäftssitz anwendbar sein. Der vorliegende Bericht beabsichtigt nicht, eine Liste von Ländern auszuweisen, bei denen ein hohes Terrorismusfinanzierungsrisiko besteht. Die zuständigen Behörden können ihre eigene Liste der Hochrisikoländer und -regionen (einschließlich inländischer Regionen in ihrem Land) anhand dieser Faktoren bestimmen.

### Hochrisikoländer / -regionen

Die Begriffe "Hochrisikoland/-region" sind nicht leicht zu definieren oder zu erklären, da sie für eine Reihe von Umständen gelten und Risiken umfassen, die mit verschiedenen Arten von Straftaten oder mit politischen oder wirtschaftlichen Umständen in Verbindung stehen. Aus Sicht der Terrorismusfinanzierung können diese Begriffe die Länder/Regionen umfassen, in denen es zu terroristischen Aktivitäten kommt (u. a. Anschläge und Anschlagsplanung) oder in denen Terrororganisationen angesiedelt sind, Unterstützer anwerben oder logistische Unterstützung zur

Begehung von Terroranschlägen erhalten. Es folgen einige weitere Beispiele, die auf ein Hochrisikoland deuten könnten:

- Eine Konfliktzone. Dies ist ein Synonym für solche Hochrisiko-Länder/-regionen, die instabil sind, sich im Krieg befinden, in denen bewaffnete Feindseligkeiten vorherrschen oder in denen Terrororganisationen aktiv sind.
- Provinzen/Regionen mit bekannten Verbindungen zu Terrororganisationen oder gemeinsamen Grenzen mit Gebieten, die von Terrororganisationen kontrolliert werden.
- Länder, in denen Gelder und andere Vermögenswerte für terroristische Handlungen oder Terrororganisationen generiert werden (z. B. Auftraggeber des Geldtransfers), unabhängig davon, wo es zu den Handlungen kommt oder die Organisationen ansässig sind.
- Länder/Regionen, die Transitpunkte darstellen oder über die Geldflüsse ausländischer Terrorkämpfer (FTFs) laufen (siehe nachstehende Fallstudie).
- Länder, in denen Defizite bei der Bekämpfung von Geldwäsche/Terrorismusfinanzierung bestehen, Länder mit schwachen institutionellen Rahmenbedingungen, die die FATF-Standards nicht erfüllen (einschließlich der öffentlich durch die FATF identifizierten Länder), oder Länder, die generell bei der Terrorismusbekämpfung nicht kooperativ sind.


**nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** - © 2016

Fallstudie: **Verwendung von Geldtransfers in der Nähe von Ländern, in denen der IS agiert**

Vertraulichen Finanzinformationen zufolge wurden Terrorismusfinanzierungsrisiken betreffend die Nutzung elektronischer Geldtransfers über Banken, aber auch in Bezug auf sonstige Transfers über Geld-/Werttransfersysteme in Gegenden in der Nähe von IS-aktiven Gebieten bzw. an gelistete Personen festgestellt. Die Örtlichkeiten, an die diese Überweisungen gelangten, befanden sich häufig in Gebieten, die ausländischen Terrorkämpfern und Terrororganisationen als Finanz-, Logistik- und Schmuggelbasis dienten. In einigen dieser Fälle wurde in sozialen Medien darauf hingewiesen dass die Begünstigten von Geldtransfers möglicherweise Kontakte zu terroristischen bzw. radikalen Gruppierungen haben. In anderen Fällen wurden sehr hohe Bargeldeinzahlungen in den USA getätigt; anschließend kam es zu elektronischen Überweisungen an Begünstigte in Gebieten unweit der Territorien, in denen der IS operiert. Die erkannten Risiken bezogen sich auch auf den Mangel an Informationen über den Zweck dieser Überweisungen, das Verhältnis zu den Empfängern bzw. den Grund dafür, warum über kurze Zeiträume zahlreiche Transaktionen durchgeführt wurden.

*Quelle: Vereinigte Staaten*

### Grenzüberschreitende Faktoren

Zu dieser Kategorie gehören Transaktionen und Aktivitäten, die mit Reisen, besonders in Bezug auf FTFs, in Verbindung stehen. In diesem Bereich ist bereits viel Arbeit geleistet worden, insbesondere durch die Egmont-Gruppe der FIUs, die sich mit speziellen FTF-Profilen befasst hat. Durch die Egmont-Gruppe wurde ein nicht-öffentliches Bulletin zu FTFs erstellt, das den zuständigen Behörden zur Weitergabe an den Privatsektor zur Verfügung steht. Der vorliegende Bericht möchte die umfangreiche Arbeit der Egmont-Gruppe nicht duplizieren. In Abschnitt II.D ist jedoch eine Reihe von Faktoren genannt, die für FTFs relevant sind.

Darüber hinaus kann zum geographischen Risiko auch die Nutzung von Geldtransferdienstleistungen gehören, die von einem Finanzinstitut parallel zu normalen Zahlungen angeboten werden, sowie Firmen in Familienbesitz, die Onlineüberweisungen über informelle Netzwerke anbieten. Der vorliegende Bericht möchte einige der relevanten Risikoindikatoren im Zusammenhang mit Geld-/Werttransfersystemen untersuchen (siehe auch Bericht *The role of Hawala and other similar service providers in money laundering and terrorist financing* (FATF, 2013b).) Andere Anhaltspunkte betreffend geographische Risiken finden sich in den Kategorien im Zusammenhang mit Ausgabeaktivitäten, Produkten und Dienstleistungen. Nachstehend wird ein Beispiel für Anhaltspunkte mit Bezug auf ein geographisches Risiko aufgezeigt:

- Mehrere Personen schicken dem gleichen Begünstigten in einem Hochrisikoland Geld.
- Der gleiche Kunde schickt mehreren Begünstigten in einem Hochrisikoland Geld.
- Häufige Geldüberweisungen geringer Beträge über Grenzen hinweg von/an Personen ohne Bezug/Verbindung.
- Geldüberweisungen von/an die gleichen Parteien durch Personen, die getrennt zu handeln scheinen (auch "Konsumentennetzwerk" genannt,

welches eine Reihe von Personen repräsentiert, die durch gemeinsame Gegenparteien verbunden sind).

- Eine Zahlung aus dem Ausland, die als Spende, Hilfe, Darlehen etc. angegeben wird und die umgehend in bar abgehoben oder auf ein anderes Konto transferiert wird.
- Hohe Geldbeträge werden von einem Familienangehörigen oder einer Organisation ohne Bezug auf ein Studentenkonto im Ausland gezahlt.
- Kunden mit Wohnsitz in oder Verbindung zu einem Hochrisikoland.
- Kunden greifen von einer IP-Adresse in einer Konfliktzone oder einer Adresse, die nicht mit den CDD-Unterlagen übereinstimmt, auf (Online-) Bankgeschäfte zu.
- Ein kürzlich eröffnetes Konto eines Kunden weist beträchtliche Ausgaben im Ausland aus.
- Längere Aufenthalte (über sechs Wochen) Arbeitsloser im Ausland, die weiterhin Arbeitslosengeld vom Staat erhalten.
- Hinweise darauf, dass der Kunde in Gebiete in Konfliktzonen oder angrenzende Bereiche gereist ist (oder regelmäßig reist) und dabei Bargeld bei sich hat.

Fallstudie: **Beispiel für ein europäisches Netzwerk mit Helfern**

Vier Personen haben 28 Geldüberweisungen über sieben verschiedene Unternehmen in Deutschland und Frankreich durchgeführt. Die Transaktionen hatten 17 verschiedene Begünstigte in 16 verschiedenen Unternehmen in Ägypten, Deutschland, Griechenland, Marokko, Portugal und Tunesien.

Der Auswertung zufolge kam es zu den Transaktionen im Zusammenhang mit dieser Gruppierung zwischen 2006 und 2013, die überwiegende Anzahl fand 2008 statt. Der Begünstigte in Portugal hat die Gelder im Januar 2009 bei drei verschiedenen Unternehmen in Oporto abgehoben. Er hatte in Portugal weder ein Einkommen noch Besitz. Nach Erkenntnissen, die durch internationale Zusammenarbeit gewonnen wurden, soll der Begünstigte in Portugal 2014 über die Türkei nach Syrien gereist sein und hat sich mutmaßlich dem IS angeschlossen. Er wurde später bei seiner Rückkehr nach Europa festgenommen.

*Quelle: Portugal*


**nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** - © 2016

### Erpresserischer Menschenraub

Erpresserischer Menschenraub ist für Terrororganisationen eine Einnahmequelle, auch für den IS.[3] Terrororganisationen bedienen sich Netzwerken von Helfern, um die Erlöse aus erpresserischem Menschenraub durch das weltweite Finanzsystem zu bewegen, darunter alternative Überweisungssysteme, Banken, Geldwechselstuben und andere Finanzinstitute.[4] Bargeld spielt bei erpresserischem Menschenraub häufig eine bedeutende Rolle. Banken werden wahrscheinlich nicht in der Lage sein festzustellen, ob eine Zahlung aus einer Lösegeldforderung stammt, ohne dass konkrete Informationen vorliegen. Einige Anhaltspunkte wurden kürzlich festgestellt:

- Verwandte beschaffen (für das Opfer) Geld durch den Verkauf von Vermögenswerten und Krediten.
- Ein Trust (oder eine andere rechtliche Vereinbarung) wird eingerichtet, um Zuwendungen für Lösegeldzahlungen zu sammeln/verwahren.
- Eine Crowdfunding-Seite wird eingerichtet, um Spenden für ein Opfer entgegenzunehmen.
- Hohe Bargeldbeträge werden über Geld-/Werttransfersysteme (einschließlich Überweisungsdienstleister und Hawalas) in Drittländer geschickt, bei denen es sich nicht um das Land handelt, in dem die Entführung stattfand.
- Internationale Geldüberweisungen für religiöse Gruppen oder Unternehmen. Personen (z. B. Schatzmeister), die Bankkonten im Namen religiöser Organisationen führen, gaben bei Nachfrage seitens der Bank an, der wahre Zweck der Transaktionen seien Lösegeldzahlungen.
- Hohe Bargeldabhebung von Konten, zur Nutzung als Hilfszahlungen getarnt.
- Geldeingänge von einem Versicherer, der mit Entführungs- und Lösegeld-Versicherungsprodukten handelt.
- Kooperation mit Firmen oder Versicherungsgesellschaften, die Verhandlungen bei Geiselnahmen führen.

## D. ANHALTSPUNKTE MIT BEZUG ZU AUSGABEAKTIVITÄTEN

Ausgabeaktivitäten könnten auf viele verschiedene Arten aufgedeckt werden, wobei die Informationen des Kunden, der Zweck der Geldüberweisung und der Geschäftszweig der Gegenparteien zu berücksichtigen sind. Wie in dem Abschnitt zu geographischen Risiken genannt, bezieht sich eine Reihe von Geldausgabeindikatoren konkret auf ausländische Terrorkämpfer. Diese Personen werden eine Reihe von finanziellen und logistischen Vorkehrungen treffen, bevor sie reisen und während sie *auf dem Weg* in die Konfliktzone sind. Ein Anhaltspunkt ist der Kauf eines "E-Visums" außerhalb des Landes, in dem der reisende FTF wohnt, oder eine Ungereimtheit beim ersten angegebenen Ziel des Reisenden. Um Aufdeckung zu vermeiden, legen FTFs häufig Zwischenstopps auf ihren Reisen in Konfliktgebiete ein, indem sie über Zwischenziele reisen. Zur Legitimierung dieser Zwischenziele beschaffen FTFs hierfür Visa. Die Überprüfung der Geldquelle und des Alters des Reisenden (z. B. Teenager) kann auch helfen festzustellen, ob Käufe als ungewöhnlich im Vergleich zu den meisten normalen Urlaubsvorbereitungen gelten.

[3] *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)* (FATF, 2015a).
[4] *Organized Maritime Piracy and Related Kidnapping for Ransom* (FATF, 2011).

© 2016 - **nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt**

Die Anwendung dieser Anhaltspunkte könnte eine Reihe von Herausforderungen für den Privatsektor darstellen. Institute könnten beispielsweise nur unzureichende Informationen über das Produkt, die Dienstleistung oder sogar die Art des Geschäftsbetriebs, der eine Kredit-/Debit Transaktion bearbeitet hat, erhalten. Viele der Indikatoren in diesem Abschnitt sind darüber hinaus harmlos in ihrer Art und deuten nicht sofort auf Terrorismusfinanzierung hin. Die Anhaltspunkte könnten besonders relevant sein bei der Feststellung einer Änderung der üblichen Transaktionsaktivitäten einer Person, die eine Reise in eine Konfliktzone vorbereitet, um ausländischer Kämpfer zu werden (siehe nachstehende Fallstudie), indem sie ein Missverhältnis zwischen Einkommen und Ausgaben aufweisen. Dieser Abschnitt befasst sich mit Szenarien in Bezug auf Reise, Ausgaben von Einzelpersonen/Gruppen für Nicht-Reise-Zwecke und deckt Netzwerke auf.

### Ausgaben im Zusammenhang mit Reisen

- Zahlungen in Outdoor-Stores (wo sie Stiefel, Schlafsäcke, Kleidung, Thermounterwäsche, Zelte und Ausrüstung kaufen können).
- Zahlungen, die auf Termine in Krankenhäusern vor der Reise hindeuten.
- Kauf eines Flugtickets, Busfahrscheins, Pkw-Anmietung, Carpooling-Buchung.
- Buchung von One-Way-Flügen ins Ausland mit Kreditkarte (häufig für Personen ohne erkennbaren direkten Bezug).
- Kauf zahlreicher Flugtickets oder Busfahrscheine nach Eingang mehrerer Bargeldbeträge oder Überweisungen.
- Zahlungen für Visa, insbesondere Onlinezahlungen für E-Visa in Konfliktgebiete.
- Reisende fragen nach einer Bestätigung, dass angegebene Begünstigte von Lebensversicherungspolicen eine Zahlung auch in Fällen erhalten, in denen die Umstände auf Beteiligung an Terrorismus und nicht auf Opfer von Terrorismus deuten. (diese Fälle betreffen potentielle FTFs, die ihre Reisen in Konfliktzonen nicht vor Abreise angeben).
- Junge Leute kaufen Sterbe- oder Lebensversicherungspolicen oder lösen eine Police zur Bezahlung von Flugtickets aus.
- Kauf von Pkw zwecks Ausfuhr in Länder, die an die Konfliktzonen angrenzen.
- Kauf von Pre-Paid Handys oder SIM-Karten.


**nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** - © 2016

Fallstudie: **Transaktionsaktivitäten eines FTF, der eine Reise in eine Konfliktzone vorbereitet**
Bei einer Person ohne regelmäßiges Einkommen, werden zahlreiche Eingänge kleiner Beträge für Reisen (mit dem Zug, öffentlichen Verkehrsmittel) innerhalb von Frankreich verzeichnet. Diese Aktivitäten scheinen auf die Existenz radikalisierter Personen zu deuten, die potentielle ausländische Terrorkämpfer sein könnten.
Die Bankkonten der oben beschriebenen Personen sind auch von erhöhten Ausgaben für Telefonie in den Monaten vor ihrer Abreise gekennzeichnet. Mindestens ein Kauf (für einige hundert Euro) von "Sportartikeln" ist für das einzelne Konto registriert. Der Kauf von "Sportartikeln" erfolgt online, in Sportgeschäften oder in Geschäften, die auf den Verkauf von Waren für Extremklima spezialisiert sind. Solche Käufe können zur Beschaffung militärischer Grundausstattung (z. B. Schlafsäcke, Wanderschuhe, Parkas etc.) genutzt werden.
Schließlich verzeichnen die Konten online-Käufe im Zusammenhang mit Reisekosten (z. B. Zahlungen an Reisebüros, Fluggesellschaften und Fährgesellschaften) außerhalb des Landes.
*Quelle: Frankreich*

Fallstudie: **Helfer für ein Netzwerk potentieller ausländischer Terrorkämpfer**
Eine Person, die mehrere Bankkonten führt, erhält zahlreiche Überweisungen von zahlreichen Personen. Die erhaltenen Gelder werden dann auf das Konto eines anderen überwiesen, der regelmäßig Flugtickets kauft und Versicherungen abschließt. Die Nutzung seiner Kreditkarte weist jedoch keine Reisen ins Ausland auf.
*Quelle: Türkei*

### Reiseunabhängige Geldausgaben

- Kauf von teuren oder qualitativ hochwertigen Kommunikationsmitteln und Informationstechnik (z. B. Satellitentelefone).
- Kauf von Shooter-Games oder Teilnahme an Kampftraining oder Ähnlichem.
- Kauf von Waffen oder Dual-use-Produkten, die für Terroranschläge oder im Kriegskontext genutzt werden können (z. B. Munition, Sprengstoff, Militärbedarf, optisches oder elektronisches Gerät) über elektronische Zahlungskonten.
- Zahlungen an Medien oder Buchläden, die mit Propaganda für Radikalismus, Extremismus oder Gewalt in Verbindung stehen.
- Spenden an NPOs oder religiöse Websites, die mit Propaganda für Radikalismus, Extremismus oder Gewalt in Verbindung stehen.
- Kauf zahlreicher Prepaid-Karten (z. B. Telefon-, Mehrzweckkarten)

### Aufdeckung von Netzwerken

Proaktives Mining wird häufig zur Feststellung von Beziehungen führen, die größere Netzwerke um mutmaßliche FTFs herum aufweisen können. Netzwerke können oft durch Überprüfung der Beziehungen des Hauptverdächtigen über Kundendaten, wie Anschrift und Zahlungsdaten, festgestellt werden. Diese Faktoren könnten zur Feststellung von Netzwerken genutzt werden.

- Gemeinsame Anschriften.

- Gemeinsam genutzte Computer und IP-Adressen.
- Einzahlungen aus gleichen Quellen.
- Person innerhalb eines Netzwerks verteilt Geld an andere.
- Geldflüsse aus dem Ausland zur Finanzierung von Aktivitäten im Inland.

## E. ANHALTSPUNKTE MIT BEZUG ZU PRODUKTEN ODER DIENSTLEISTUNGEN

Wie bei anderen Kategorien von Risikoindikatoren handelt es sich hier um einen weitreichenden, breit gefächerten und nicht leicht zu überschauenden Bereich. Eine relevante Frage ist, wie Produkte und Dienstleistungen, die der Finanzsektor anbietet, für Geldbewegungen genutzt werden. Nützliche Hinweise sind Abschnitt III (B) des Berichts *Emerging Terrorist Financing Risks* aus 2015 (siehe S. 20-23) zu entnehmen. Der Abschnitt gibt einen Überblick über die herkömmlichen TF-Methoden und -techniken, die auch heute noch für Geldbewegungen genutzt werden. Die Beispielindikatoren, die allgemein angegeben wurden, decken die Produkte ab, die in dem oben genannten Bericht festgestellt wurden. Alternativ befasste sich Abschnitt IV (B und C) der *Emerging Terrorist Financing Risks* mit den Schwachstellen, die für die sozialen Medien und für eine Reihe von neuen Produkten und Dienstleistungen von Bedeutung sind.

### Geld-/Werttransfersysteme und Überweisungsdienstleister

Geld-/Werttransfersysteme (MVTS) werden von der FATF als Finanzdienstleistungen definiert, die die Annahme von Bargeld, Schecks, anderen monetären Instrumenten oder anderen Werten sowie die Zahlung einer entsprechenden Summe in bar oder in anderer Form an einen Begünstigten mittels Kommunikation, Nachricht, Überweisung oder über ein Clearing-Netzwerk betreffen, dem das MVTS angehört. An Transaktionen, die von solchen Dienstleistern durchgeführten werden, können ein oder mehrere Vermittler zum Beispiel mit einer Schlusszahlung an einen Dritten beteiligt sein. Hierbei können alle neuen Zahlungsmethoden genutzt werden. Eine Reihe der festgestellten Anhaltspunkte im Abschnitt "geographische Risiken" beziehen sich auf MVTS.

Geldwechselstuben und Geldtransferdienstleister sind nach wie vor eines der wichtigsten Mittel, durch das der IS finanzielle Ressourcen bewegt. Diese Arten von Firmen herrschen im Irak und in Syrien vor, wo nur ein kleiner Teil der Bevölkerung über ein Bankkonto verfügt. Die Geschäfte in der Region sind von diesen Unternehmen abhängig, damit Geld verschickt oder von der ausländischen Partei in Empfang genommen werden kann, und bislang sind sie besonders anfällig für die Nutzung durch den IS. Im Irak sind beispielsweise über 1.900 Geldwechselstuben und 34 Geldüberweisungsunternehmen registriert. Im Januar 2016 wurden durch die Central Bank of Iraq (CBI) fast 150 Geldwechselstuben und Überweisungsdienstleister öffentlich bekannt gemacht, die wissentlich Transaktionen für den IS durchführen oder ihren Standort in vom IS kontrollierten Gebieten haben. Durch die CBI wurde eine Richtlinie herausgegeben, mit der ihnen die Beteiligung an Devisen-/Geldwechselgeschäften mit dem Irak verboten wird.[5]

#### *Geographische Risiken*

- Transaktionen mit/in/aus Regionen mit hohem Risiko an/von Personen ohne scheinbaren Bezug und ohne offensichtliche familiäre Verbindung.
- Geldüberweisungen an Hochrisikoländer/-regionen, die nicht zu den üblichen Auslandsgeschäften des Kunden passen.

[5] Die Liste der verbotenen Geldwechselstuben und Überweisungsdienstleister der Central Bank of Iraq kann unter folgendem Link abgerufen werden: http://www.cbLiq/documents/public%20Blacklist%2016%20March%202016%205th%20april.xlsx


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

- Absender und Begünstigter haben keinen Bezug zu dem Land, in das/aus dem das Geld geschickt wird und können nicht hinreichend erklären, warum das Geld von/nach dort geschickt wird (besonders wenn die Empfänger ausländische Staatsbürger sind).
- Der Absender bittet konkret um Übersendung des Geldes in einer internationalen anstatt in einer örtlichen Währung.
- Transaktionen werden über mehrere Länder gesteuert, durch Hochrisikokorridore oder -regionen.
- Bei Kunden, die web-basierte Systeme nutzen, wurde eine beträchtliche Entfernung zwischen ihrem Wohnort und dem Standort der IP-Adresse festgestellt.
- Der Begünstigte gibt stets die Anschrift eines Hotels in einer Touristengegend als seine Privatadresse an.

### *Identifizierungsprobleme*

- Verschiedene Identifizierungsdokumente, die von einer Person vorgelegt werden und widersprüchliche Angaben enthalten, oder verschiedene Personen nutzen die gleichen Identifizierungsdokumente.
- Kunden, die unstimmige biographische Daten vorlegen (z. B. sind eine zunehmende Anzahl ausländischer Terrorkämpfer aus westlichen Ländern muslimische Konvertiten, die ihre Namen in einen arabischen Namen geändert haben. Transaktionen werden möglicherweise unter dem Anglo-Namen durchgeführt).Beim Aufbau einer Geschäftsbeziehung sollten Kunden mit Finanzsanktionslisten (TFS) abgeglichen werden (siehe Abschnitt Aufbau einer Geschäftsbeziehung).
- Echte Telefonnummern werden durch zufällig generierte Telefonnummern oder durch logische Zahlensequenzen ersetzt, die wie eine inländische Telefonnummer aussehen könnten (z. B. 0123456789).

### *Umfang und Häufigkeit der Transaktionen*

- Hohes Transaktionsvolumen einer einzelnen Person, wobei die Transaktionen an verschiedenen Orten durchgeführt werden.
- Plötzlicher Anstieg des Transaktionsvolumens mehrerer Personen innerhalb eines kurzen Zeitraums an einem einzigen Standort.
- Anstieg des Transaktionsvolumens, das nicht mit einem örtlich bekannten, üblichen Muster in Zusammenhang steht (z. B. Gehaltsüberweisung oder kulturelles Fest).
- Transaktionen in/aus Städten, in denen eine zunehmende Anzahl von Geldüberweisungen bzw. Geldern in der Zeit vor und während eines Konflikts festgestellt wurde.

### *"Many-to-One"- und "One-to-Many"-Kundennetzwerke*

- Eine Person führt zahlreiche Transaktionen mit mehreren Ländern durch.
- Der gleiche Kunde schickt mehreren Begünstigten in einem Hochrisikoland Geld.

- Geldüberweisungen geringer Beträge über Grenzen hinweg von/an Personen ohne Bezug.
- Mehrere Personen schicken Geld an eine einzige Person, die als "Drittempfänger" agiert.
- Die gleiche Person erhält Geld von verschiedenen Geldüberweisungsfirmen oder Standorten von MVTS-Dienstleistern.

### *Andere Faktoren*

- Der Kunde scheint erst zu wissen, welcher Betrag transferiert wird, wenn der Angestellte des Geld-/Werttransfersystems das Bargeld gezählt hat.
- Der Kunde zeigt kein Interesse an den Überweisungsgebühren.
- Die übermittelte Transaktion kommt nie beim Begünstigten an, der vermutlich verstorben ist.

Fallstudie: **Netzwerk von Abholern, die Geld-/Werttransferdienstleister (MVTS) nutzen**

Mehrere Mitglieder (A, B und C) einer Familie haben eine Reihe von Bargeldtransfers über MVTS erhalten, jeder von verschiedenen Personen ohne erkennbaren Bezug (verschiedene Namen und verschiedene Orte über das Land verteilt). Die Personen A, B und C haben immer eine Telefonnummer angegeben, die aus einer Sequenz von Zahlen bestand. Sie haben regelmäßig Bargeldtransfers an die Personen D, E und F in einem Land vorgenommen, das an eine Konfliktzone angrenzt. Die Begünstigten der Transfers gaben stets als Privatadresse ein Hotel in einer Touristengegend an. Empfänger D, E und F haben nie Geld zur gleichen Zeit erhalten und scheinen sukzessive zu agieren. Die Personen A, B und C haben ihr Geld an die einzigen aktiven Personen geschickt, vermutlich im Wissen um die Änderung des Namens des Abholers von D in E und dann von E in F. Eine Person, die mehrere Bankkonten führt, erhält viele Überweisungen von vielen Personen. Die erhaltenen Gelder werden dann auf das Konto einer anderen Person überwiesen, die regelmäßig Flugtickets kauft und Versicherungen abschließt. Die Nutzung der Kreditkarte dieser Person weist jedoch keine Reisen ins Ausland auf.

*Quelle: Frankreich*


**nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** - © 2016

## Hawala und ähnliche Dienstleister

Hawala-Systeme gelten als Untergruppe der Geld-/Werttransferdienstleister (MVTS) und werden als Geldüberweiser (money transmitters) [6] definiert. Sie verfügen insbesondere über Kontakte in bestimmte geographische Regionen oder ethnische Gemeinschaften, die den Transfer und Eingang von Geldern oder Gegenwerten veranlassen und über einen gewissen Zeitraum Handel, Bargeld und Nettoabwicklung abwickeln. Während sie häufig Bankkanäle für die Abwicklung zwischen Einzahlungs- und Auszahlungsagenten nutzen, so unterscheiden sie sich von anderen Dienstleistern durch die Nutzung nicht-bankgeschäftlicher Abwicklungsmethoden, einschließlich der Abwicklung über Handel und in bar sowie verlängerte Abwicklungszeiträume. Die Beschreibung basiert auf den erbrachten Leistungen und nicht auf ihrem Rechtsstatus. Es handelt sich NICHT um globale Geldtransfernetzwerke (einschließlich Agenten), die von großen, multinationalen Geldüberweisern betrieben werden.

Der FATF-Bericht zur Rolle der Hawala und anderer, ähnlicher Dienstleister bei Geldwäsche und Terrorismusfinanzierung (*The role of Hawala and other similar service providers in money laundering and terrorist financing, HOSSPs)* aus dem Jahr 2013 stellt die TF-Schwachstellen dar und dient als Handlungshilfe für Transaktionsmuster, die häufig mit illegalen/nicht unter Aufsicht stehenden Geldtransferunternehmen, einschl. HOSSPs, in Verbindung stehen. Einige dieser Risikoindikatoren zur Feststellung verdächtiger Dienstleister sind nachstehend kurz genannt (siehe auch *Anhaltspunkte mit Bezug zu geographischen Risiken).*

- Umfangreiche Nutzung von Sammelkonten (auf die kleine Beträge eingezahlt oder angesammelt und dann in regelmäßigen Abständen ins Ausland überwiesen werden).
- Überweisungen werden häufig von Händlern in Länder übermittelt, die keine geschäftliche Verbindung mit den Zielländern zu haben scheinen.
- Geschäftskonten werden für Erhalt oder Auszahlung großer Geldbeträge genutzt, weisen jedoch kaum bis gar keine Geschäftsaktivitäten auf, wie Gehaltszahlungen, Rechnungen etc.
- Häufige Einzahlung von Schecks und Zahlungsanweisungen Dritter auf Geschäfts- oder Privatkonten.

Der Bericht *The role of Hawala and other similar service providers in money laundering and terrorist financing (HOSSPs)* hebt auch die Nutzung krimineller Hawala-Netzwerke und die Rolle verschiedener Personen, wie Controller, hervor. Der Controller (in einigen Ländern auch Money Broker genannt) bietet konkrete weltweite Geldwäschedienstleistungen an und bietet Straftätern eine zentrale Anlaufstelle und Koordinierung für ihre Bedürfnisse. Der kriminelle Kunde sagt dem Controller, wer das Geld übergeben wird und wo der Wert zu zahlen ist. In dem Bericht wird eine Reihe von Methoden beschrieben, die als relevante Risikoindikatoren betrachtet werden könnten, wie z. B.:

- Nutzung örtlicher MVTS, die Beihilfe zum Transfer von Geld an Dritte oder auf Konten leisten, die vom Controller geführt werden.
- Einzahlung von Bargeld auf Bankkonten im Namen des Controllers, um separate Weiterüberweisungen durchzuführen.

[6] *The role of Hawala and other similar service providers in money laundering and terrorist financing* (FATF, 2013b)

© 2016 - **nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt**

- Tatsächliche Bewegung von Bargeld (Bargeldschmuggel) durch Kuriere, Fracht oder Ladung.

### Bargeld und Geldautomaten

Während die Verwendung von Bargeld unter der Kategorie *Ausgabeaktivitäten* behandelt wird, handelt es sich bei Bargeld auch um eine *Art von Produkt*, das von denen genutzt wird, die Terrorismus finanzieren. Auch in diesem Bereich wurde an der Entwicklung von Anhaltspunkten betreffend FTFs gearbeitet. Aufgrund der relativ geringen Beträge, um die es bei Terrorismusfinanzierung geht, bietet sich Bargeldschmuggel an. Die Verwendung von Banknoten großer Stückelung (z. B. EUR500) erleichtert dies zuweilen. Der Schmuggel wird von den Kämpfern selbst, die in die Region reisen, durchgeführt, sowie von Freunden und Verwandten, die dorthin reisen, wenn die Kämpfer vor Ort sind.

Es gibt auch Beispiele dafür, dass Bankkonten eingerichtet werden, um Spenden in Form von vielen kleinen Bargeldeinzahlungen zu sammeln, die dann kure Zeit später in verschiedenen Beträgen an Geldautomaten (ATMs) abgehoben werden. Beispielsweise könnte Geld kurz nach Einzahlung auf Konten an einem ATM oder an mehreren in unmittelbarer Nähe wieder abgehoben werden (an aufeinanderfolgenden Tagen oder mehrere Abhebungen mit ein paar Tagen Abstand). Eine Delegation hat jedoch berichtet, dass die Nutzung von Geldautomaten und die Kartentransaktionen kein schlüssiges Anzeichen sind aufgrund der großen Anzahl der Staatsangehörigen ihres Landes, die in Gebieten Urlaub machen, die an Konfliktzonen angrenzen und die familiäre Wurzeln in diesen Grenzgebieten haben sowie aufgrund der vielen legalen Hilfsarbeiter, Journalisten und Diplomaten, die in die Gegend reisen. Einigen Banken könnten auch zu wenige Informationen über den genauen Standort eines genutzten Geldautomaten (z. B. Land oder ATM-Identifizierungscode) vorliegen. Einige allgemeine Anhaltspunkte, die Bargeld und Geldautomaten betreffen und gemeldet wurden, sind die folgenden:

- Plötzliche Geldabhebungen, die ungefähr dem derzeitigen Kontostand entsprechen und mit Ausgaben für Auslandsreisen begründet werden.
- Kunde möchte zuvor überwiesenes Geld von seinem Privatkonto kurz nach der ursprünglichen Transaktion abheben.
- Kunde möchte sich sein ungenutztes Kontoguthaben in bar auszahlen lassen.
- Aufsplittung von Bargeldeinzahlungen in kleinere Beträge, um Anzeigepflichten bei Transaktionen über dem Schwellenwert zu umgehen.
- Aufsplittung von Bargeldabhebungen mit mehrfachen Abhebungen am gleichen Geldautomaten an aufeinanderfolgenden Tagen oder an mehreren Geldautomaten in der Nähe.
- Bargeldabhebungen unter Nutzung von Debitkarten am gleichen Tag oder an aufeinanderfolgenden Tagen in verschiedenen Ländern entlang der Route in Konfliktgebiete.
- Kleine Bargeldbeträge, die häufig an SB-Terminals auf ein Privatkonto eingezahlt werden (Konto wird zum Sammeln von Spenden genutzt), und Abhebung der gesammelten Gelder an SB-Terminals kurze Zeit später.
- Große Bargeldeinzahlungen, auf die internationale Transfers folgen, die unter dem anzeigepflichtigen Schwellenwert liegen.


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

- Aufgesplittete Einzahlungen auf ein Konto von Dritten und umgehende Abhebungen an Geldautomaten im Ausland in Transitbereichen oder Hochrisikoländern.
- Auf Privatkonten ändert sich plötzlich die übliche Aktivität, wie z. B. große Beträge werden über Geldautomaten eingezahlt, dann erfolgen wiederholt Anrufe mit Fragen nach dem Kontostand und anschließend werden große Beträge an Geldautomaten abgehoben.

Fallstudie: **Fortgesetzter Zugriff auf Bankkonten durch ausländische Terrorkämpfer**

Vertraulichen Finanzinformationen zufolge wurden TF-Risiken im Zusammenhang mit Barabhebungen im Ausland entdeckt, und zwar Abhebungen durch unbekannte Personen an Geldautomaten in der Nähe der Gebiete, in denen der IS aktiv ist. Diese Abhebungen erfolgten von Bankkonten in den USA unter Benutzung einer Scheckkarte. Ein weiteres festgestelltes TF-Risiko waren hohe Einzahlungen auf Bankkonten, unmittelbar gefolgt von Barabhebungen im Ausland nahe der Gebiete, in denen der IS aktiv ist. Diese Informationen lassen die TF-Risiken erkennen, die sich daraus ergeben, dass Personen, die vermutlich in vom IS besetzte Gebiete gereist sind, weiterhin auf ihre Bankkonten in ihren Heimatländern zugreifen können.

*Quelle: USA (FATF Report on ISIL Financing, 2015)*

### Kreditkarten

Ähnlich wie Bankkunden werden viele Kreditkartenkunden innerhalb einer mehrstufigen Risikostruktur auf der Grundlage einer Multifaktoranalyse bewertet und klassifiziert. Ein Antragsteller oder Inhaber eines Kreditkartenkontos kann Gegenstand verschiedener Due-Diligence-Ebenen sein, abhängig von der festgelegten Stufe. Ferner können bestimmte Arten von Produkten oder Dienstleistungen genauer kontrolliert werden oder höheren Anforderungen unterliegen, oder in einem bestimmten Land oder einer bestimmten "Kundenstufe" nicht zur Verfügung stehen. Der geographische Standort des Antragstellers oder des Kunden ist der erste Faktor beim Risikobewertungsprozess, aber konkrete Anpassungen können je nach Bewertung anderer, individueller Risikofaktoren vorgenommen werden. Viele der Verhaltensindikatoren, die in Abschnitt II (A) festgestellt wurden, gelten auch für diese Produkte. Zu den festgestellten Anhaltspunkten gehören unter anderem:

- Wiederholte Bargeldauszahlungen in Ländern, die an Konfliktgebiete angrenzen, oder Länder entlang der Routen, die normalerweise in die/aus den Konfliktgebieten führen.
- Zahlungen mit Kreditkarte in verschiedenen Ländern im Transit (z. B. an Tankstellen, an Mautstellen oder in der Nähe von Flughäfen).
- Kundenkonto weist Bargeldauszahlungen großer Beträge bei einer erst kürzlich ausgestellten Kreditkarte auf.
- Bargeldauszahlungen mit Kreditkarten ohne sofortige Rückzahlung.
- Angesichts der Kreditwürdigkeit des Kunden unbegründeter oder ungerechtfertigter Antrag auf maximale Hochsetzung des Kreditrahmens.
- Erreichen des Kreditrahmens vor Abreise.
- Scheinbar keine veränderte Nutzung einer Kreditkarte nach Abreise per Flugzeug in Konfliktgebiete (z. B. Karte wird im Inland von einer dritten Person genutzt) (siehe nachstehende Fallstudie).
- Plötzliche Nutzung von Kreditkarten in Gebieten mit hohem Risiko (z. B. vermehrte Bargeldauszahlungen), wenn die Karte vorher/anschließend mehrere Monate ungenutzt blieb.

- Nutzung von Kreditkarten nur für Transaktionen zwischen Personen, wohingegen Zahlungen für Waren und Dienstleistungen fehlen (z. B. Personen, die als "Strohmänner" agieren).
- Nutzung von Kreditkarten, die für Dritte ausgestellt sind.

Fallstudie: **Inaktivität bei Kreditkartennutzung**

Die Nutzung von Debitkarten im Ausland, gefolgt von Zeiten der Nichtnutzung der Karten, wurde festgestellt. In diesem Fall, nachdem Reisekosten für das Konto registriert wurden, bleibt das Konto für einige Zeit inaktiv, so dass der Eindruck entsteht, der Kontoinhaber brauche kein Geld zur Finanzierung seiner Reise ins Ausland. Wird das Konto wieder genutzt, so erfolgt oft ein Kauf in einem Geschäft in der Nähe eines Flughafens.

Andere Beispiele für Risiken sind u. a. die Nutzung der Kreditkarte einer Person im Inland, während die Person angeblich in ein Konfliktgebiet ausgereist sein soll, um vorzugeben, dass der FTF sein Herkunftsland nie verlassen hat.

*Quelle: Frankreich*

## Darlehen/Privatkredite

Eine sich abzeichnende Entwicklung, die im FATF-Bericht *Emerging Terrorist Financing Risks* festgestellt wurde, betrifft die Beantragung von Kleinkrediten mit kurzer Laufzeit durch ausländische Terrorkämpfer bei verschiedenen Anbietern gleichzeitig, ohne die Absicht zu haben, die Kredite zurückzuzahlen. Nachstehend werden Beispiele für die festgestellten Anhaltspunkte aufgezeigt:

- Kunden, die Kredite in bar aufnehmen und zu Verzug neigen.
- Kunde verwendet Kredite nicht zu angegebenen Zwecken.
- Kunde beantragt einen Kredit und hebt kurz darauf einen beträchtlichen Teil in bar ab.
- Aufnahme von Kleinkrediten bei mehreren Kreditunternehmen ohne Rückzahlung.
- Kredite werden gewährt (z. B. auf der Grundlage gefälschter Einkommensbescheinigungen) und es gibt Anzeichen dafür, dass sich die Person ins Ausland absetzen könnte.
- Häufige Kreditaufnahme unter Angabe hochwertiger Güter als Sicherheit.
- Kreditanträge, die nicht mit der wirtschaftlichen und finanziellen Situation des Antragstellers übereinzustimmen scheinen.
- Dritte ohne Bezug handeln zur Absicherung des Kredits für den Antragsteller.
- Betrügerische Kreditanträge zum Kauf von Ware, die offenbar nicht vom Antragsteller genutzt wird (z. B. Kauf von Fahrzeug oder Haushaltsgeräten).


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

Fallstudie: **Beantragung zahlreicher Kredite mit kurzer Laufzeit**

In zahlreichen Fällen wurden Ermittlungen betreffend kleine Konsumentenkredite (weniger als EUR 2.000) geführt, die alle in bar innerhalb von 24 bis 48 Stunden vom Konto abgehoben wurden. Es ist daher mehr als wahrscheinlich, dass die Kreditbeträge von der ursprünglichen Absicht abweichend umgeleitet wurden, um ein "Sparkonto" zur Finanzierung einer Reise oder logistischer Ware einzurichten.

*Quelle: Frankreich*

Fallstudie: **Nichtrückzahlung eines Privatkredits**

Jemand erhält zwei Privatkredite über insgesamt JOD 7.500. Nachdem er die Ratenzahlungen eingestellt hat, versucht die Bank ihn anzurufen, und erhält von dessen Arbeitgeber die Auskunft, dass die Person schon seit langem nicht mehr zur Arbeit erschienen sei.

Auf Nachfrage erfährt die FIU, dass die Person ins Land (H) und anschließend in ein Land gereist ist, das an eine Konfliktzone angrenzt. Die FIU des Landes (H) hat den Fall wegen des Verdachts der Finanzierung des Terrorismus an den zuständigen Generalstaatsanwalt abgegeben. Durch den zuständigen Generalstaatsanwalt wurde das bewegliche und unbewegliche Vermögen der Person sowie der Familie sichergestellt.

*Quelle: Jordanien*

## Wechselstuben

Durch die FATF wurden die TF-Risiken betreffend Geldwechselgeschäfte nicht umfänglich untersucht. Vor diesem Hintergrund werden einige der Anhaltspunkte, die bisher festgestellt wurden und in diesem Zusammenhang relevant sein könnten, im Folgenden dargestellt:

- Fehlende Informationen betreffend der Absicht der Person und Quelle der Gelder.
- Bankkunde tauscht einen großen Geldbetrag in ausländischer Währung in Inlandswährung und nutzt diesen zur Eröffnung eines neuen Bankkontos in einem an eine Konfliktzone angrenzenden Gebiet.
- Tausch eines beträchtlichen Devisenbetrags in Banknoten großer Stückelung (z. B. EUR 500-Noten).
- Auf Geldtauschgeschäfte folgen innerhalb kurzer Zeit internationale Geldtransfers in Hochrisikoländer.
- Internationales Netzwerk von Wechselstuben - internationaler Handel zwischen mehreren Wechselstuben in Hochrisikoländern.
- Internationales Netzwerk aus Wechselstuben und Handelsunternehmen in Hochrisikoländern: informelles Clearing- und Abwicklungssystem zwischen Bargeld und Waren ohne grenzüberschreitende Bewegungen.
- Wechselstuben im Ausland stehen im Verdacht, Falschgeld anzubieten.
- Nicht registrierte Wechselstuben nutzen Kontenausgleichsmechanismen mit registrierten Wechselstuben, die Beihilfe leisten und Bankkonten führen.
- Wechselstuben beteiligen sich - angesichts des Umfangs ihrer Aktivitäten - häufiger als nötig an Dollar-Auktionen der Zentralbank.

© 2016 - **nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt**

## Neue Zahlungsprodukte und Dienstleistungen

Der Leitfaden *Guidance for a risk-based approach for prepaid cards, mobile payments and Internet-based payment services* (FATF, 2013c) legt eine Reihe von Risikofaktoren dar, die dabei helfen sollen, Geldwäsche-/Terrorismusfinanzierungsrisiken im Zusammenhang mit neuen Zahlungsprodukten und Dienstleistungen zu erkennen. Werte können dabei digital in einer Vielzahl von neuen Zahlungsprodukten verwahrt werden (z. B. E-Wallets, Prepaid-Karten und mobile Zahlungen) und verflochten werden, um Transaktionen durchzuführen. Die Produkte können für Käufe und Handelstransaktionen, aber auch zur Durchführung internationaler Geldüberweisungen zwischen Personen genutzt werden. Die im vorliegenden Bericht genannten Anhaltspunkte betreffend Ausgabeaktivitäten und geographische Risiken könnten für diese Produkte relevant sein.

Die neuen Produkte und Dienstleistungen werden von einer Reihe verschiedener Zahlungsverkehrsdienstleister betrieben. Bei Verwaltung dieser Produkte durch Nicht-Finanzinstitute sind die CDD-Anforderungen möglicherweise nicht so hoch und sie könnten daher eine größere TF-Schwachstelle darstellen.

### *Internet-basierte Zahlungen*

Internet-basierte Zahlungsverkehrsdienstleister stellen Kunden über das Internet, auch über Smartphones, Zugangsmechanismen zu „Pre-funded Accounts“[7] zur Verfügung, die dafür genutzt werden können, elektronisches Geld oder elektronische Werte, die sich auf den Konten befinden, an andere Personen oder Firmen zu überweisen, die ebenfalls Konten beim gleichen Dienstleister führen.

- Eine Person könnte zahlreiche Finanzprofile (z. B. E-Wallets) nutzen, um sich bei verschiedenen Zahlungssystemen zu registrieren.
- E-Wallet-Registrierung aus Hochrisikoland/-region.
- Kontoauffüllung aus Hochrisikoland/-region.
- Remote-Geldtransfer aus einer E-Wallet an Konten Dritter, die in einem anderen Land eröffnet wurden (Person an Person).
- Angabe von Finanzdaten auf Websites und in sozialen Medien mit extremistischem und radikalem Kontext.
- Zahlungen, die darauf deuten, dass das Konto für Wohltätigkeitsspendenaktionen verwendet wird.
- Große und verschiedene Geldquellen (z. B. Banküberweisungen, Kreditkarten und Barfinanzierung von verschiedenen Standorten aus), die für die gleiche E-Wallet genutzt werden.
- Zahlreiche Bankkonten bei Banken in verschiedenen Städten werden zur Einzahlung auf das gleiche Konto genutzt.
- Online-Konten stehen mit Personen, denen Terrorismus zur Last gelegt wird, durch Namen, Kreditkarten, Adressen, E-Mail-Aktivitäten und Computercookies in Verbindung (z. B. wurden die Konten zum online-Kauf von elektronischen Bauteilen und Prepaid-Handy-Karten genutzt).

[7] Konten, auf die ein Mindestbetrag / -wert eingezahlt werden muss, um später Zahlungen / Abbuchungen darüber abwickeln zu können.


for restricted use only, not for publication - © 2016

Fallstudie: **Many-to-one E-Wallet-Zahlungen**

Im Rahmen einer FIU-Initiative zum Monitoring offener Quellen in einem sozialen Netzwerk (und zwar Vkontakte) erregte ein Eintrag die Aufmerksamkeit. Mit diesem wurde zu Spenden zur finanziellen Unterstützung der Familien von Terroristen, des Jihads und der Finanzierung der Ausbildung von Terroristen aufgerufen. Mehrere E-Wallet-Nummern wurden darin genannt. Die Person, der die E-Wallets gehören, erhielt Überweisungen von zahlreichen Personen aus verschiedenen Ländern. Das Geld auf den elektronischen Konten wurde anschließend an ein mobiles Bankkonto geschickt, das einer Telefonnummer zugeordnet werden konnte, die sich in einem Konfliktgebiet befindet.

*Quelle: Russische Föderation*

### *Prepaid-Karten*

Bei Prepaid-Karten handelt es sich um Karten, die mit einem bestimmten Betrag an elektronischer Währung oder Wert aufgeladen werden. Wieder aufladbare Universal-Prepaid-Karten, die mit einem Bankkonto in Verbindung stehen, sind oft Gegenstand der CDD-Compliance. So wie andere Bankprodukte, wie z. B. Debitkarten, können sie zu TF-Zwecken genutzt werden, um Geld an Automaten in einem Hochrisikoland abzuheben (siehe weiter oben zu *Bargeld und Geldautomaten).* Nachstehend werden noch weitere konkrete Anhaltspunkte genannt, die ebenfalls Konto-basierte Prepaid-Karten betreffen könnten:

- Ausländische Prepaid-Karten, die in einem Hochrisikoland ausgestellt wurden.
- Registrierung zahlreicher Prepaid-Karten für Familienangehörige im Zusammenhang mit der Ausreise in Hochrisikoland/-region.
- Karte-an-Karte-Transfers in/aus Hochrisikoland/-region.
- Online Transaktions-Check von einer IP-Adresse in einem Hochrisikokorridor.
- Transaktionsversuch über dem Limit der Prepaid-Aufladung durch jemanden, der offenbar nichts von dem aufgeladenen Betrag weiß, also möglicherweise nicht der ursprüngliche Besitzer der Karte ist.

Zu Prepaid-Karten, die nicht auf Bankkonten basieren und die von Einzelhändlern verkauft werden, wird häufig eine Identifizierung über einer gewissen Schwelle des Maximalbetrags oder der Wiederaufladefrist gefordert. Solche Karten können im Inland über Electronic Cash aufgeladen und unauffällig ins Ausland geschafft werden. Bei Ankunft in einem Hochrisiko- oder Transitland für Terrorismusfinanzierung werden die Gelder dann über zahlreiche Abhebungen an Geldautomaten im Ausland wieder zu Bargeld gemacht.

- Nutzung von Prepaid-Karten, die unter falscher Identität oder unter dem Namen einer anderen Person für Käufe im Internet registriert wurden.
- Karten werden online über anonyme Zahlungsmittel (z. B. Voucher, die bar bezahlt werden, Bargeldbeträge über Geldautomaten, E-Wallets) aufgeladen.

Open-Loop-Prepaid-Karten, die von Einzelhändlern verkauft werden und die nur ein geringes Aufladevolumen haben, für das keine Identifizierung erforderlich ist. Diese Art von Prepaid-Karten bereitet die größten Sorgen.

- Zahlreiche Käufe von Prepaid-Karten, für die keine Identifizierung erforderlich ist, trotz höherer Gebühren als für eine Prepaid-Karte mit höheren Schwellenwerten aber Identifizierungserfordernis.
- Kauf von mehreren Prepaid-Karten in Geldwechselstuben beim Tausch von Devisen.
- Zahlreiche Bargeldeinzahlungen auf eine aufladbare Prepaid-Debitkarte durch eine Person, der Terrorismus zur Last gelegt wird.

Fallstudie: **Nutzung von Prepaid-Karten vor Anschlägen**

Eine aufladbare Open-Loop-Prepaid-Karte, die von einem Finanzinstitut verwaltet wird, wurde in mehreren europäischen Ländern für Bargeldabhebungen und für kleinere Ausgaben im Zusammenhang mit Reisen benutzt: Kauf von Flugtickets, Buchung von Hotels, Anmietung von Fahrzeugen, Zahlung von Kraftstoffrechnungen, Zahlung an Autobahnraststätten. Die Prepaid-Karten wurden auch als Sicherheit bei der Anmietung eines Fahrzeugs oder der Buchung eines Hotelzimmers genutzt. Versuchte Transaktionen, die das aufgeladene Guthaben auf der Karte überstiegen, konnten von der ausgebenden Bank nicht erkannt werden, wurden jedoch von der Firma, die die Zahlungsvorgänge verwaltet, erkannt. Diese Firma, mit Sitz in Land D, hat die FIU von Land D informiert, die ihrerseits die belgische FIU informierte. Es war dann möglich, die Route der Terroristen durch die Auswertung der mit der Prepaid-Karte vorgenommenen Zahlungen zurückzuverfolgen. Die abgelehnten Transaktionen waren auch wichtig, um die Routen der Terroristen zu ermitteln und nachvollziehen zu können. Die Ermittlungen ergaben, dass die Terroristen durch die Zahlungen mit der Prepaid-Karte logistisch unterstützt werden konnten.

*Quelle: Belgien*

### *Mobile Zahlungen*

Es gibt zahlreiche Mobile-Payment-Dienste, die von Finanzinstituten und Mobilfunkbetreibern angeboten werden und die sich zusammengeschlossen haben, um Agentennetzwerke zu schaffen. Mobilfunkbetreiber-Verkaufsstellen und andere Ladengeschäfte bieten Dienstleistungen an, die denen von Bankfilialen mit beschränkter Zweckbestimmung ähnlich sind (z. B. Entgegennahme von Einlagen und Auszahlung von Bargeld zur Abwicklung von Mobile-Payment-Transaktionen).

- Bargeldtransfer über Grenzen hinweg in Hochrisikoland/-region.
- Handykauf, nur um es für Mobile-Payment und nicht zu Kommunikationszwecken zu nutzen.
- Registrierung eines "Einmal"-Handys bei einem Mobile-Payment-Dienstleister.
- Nutzung von bar bezahlten Stored-Value-Telefonkarten (besonders wenn keine Kundenidentifizierung erforderlich ist).
- Der Empfänger kann um Überweisung auf seine Stored-Value-Karte bitten und das Geld an jedem Geldautomaten abheben.


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

### *Crowdfunding-Plattformen*

Crowdfunding-Plattformen können für TF-Zwecke missbräuchlich verwendet werden, indem auf ihnen Gelder im Internet gebündelt und zahlreiche Zahlungsmethoden für internationalen Geldtransfer angeboten werden. Idealerweise könnte, wie in Abschnitt II.A des Berichts angegeben, jeder, der sich zum Sammeln von Geldern bei einer Crowdfunding-Plattform registriert, mit den TF-Sanktionslisten und in den offenen Medien abgeglichen werden.

- Hohe Beträge werden bei wenigen Teilnehmern gesammelt.
- Ein kleines Projekt sammelt Gelder bei Personen, die im realen Leben in Bezug zueinander stehen (z. B. Angehörige einer kleinen örtlichen Non-Profit-Organisation, Leute aus der Nachbarschaft), trotz der hohen Gebühren, die die Crowdfunding-Plattform nimmt.
- Zahlungseingänge aus Hochrisikoland/-region.
- Möglicher Missbrauch einer humanitären Spendenkampagne.
- Projektleiter nutzen Bankkonten ohne geographischen Bezug zum beworbenen Projekt.
- Crowdfunding-Plattformen mit Projekten/Zwecken mit Bezug zu gewalttätigem Extremismus oder Radikalismus

Fallstudie: **Missbrauch einer humanitären Spendenkampagne über eine Crowdfunding-Plattform**

Eine kürzlich gegründete NPO, die mit einer religiösen Gebetsstätte in einem kleinen Wohnviertel in Verbindung steht, richtet *auf einer Crowdfunding-Plattform* eine Spendenkampagne für humanitäre Zwecke ein, die sich auf Schulen im Ausland bezieht. Die meisten Spenden stammen von ein paar dort wohnenden Leuten, vermutlich im Zusammenhang mit dem Besuch der Gebetsstätte. Die Gebühr von 5,5 %, die die Crowdfunding-Plattform berechnet hat - teuer für eine kleine NPO- hätte davon abhalten sollen, solch ein Medium zum Sammeln von Geld innerhalb einer bereits bestehenden Gruppe zu nutzen. Ein Mitglied der Führungsebene der NPO hatte mutmaßlich enge Verbindungen zu FTF.

*Quelle: Frankreich*

## F. ANHALTSPUNKTE MIT BEZUG ZU NON-PROFIT-ORGANISATIONEN (NPOS)

Während nicht alle Non-Profit Organisationen (NPOs) ein hohes Risiko darstellen und von einigen nur ein geringes oder gar kein Risiko ausgeht[8], so wurden im Rahmen der laufenden internationalen Kampagne gegen Terrorismusfinanzierung Fälle festgestellt, in denen Terrororganisationen NPOs ins Visier nehmen, um sich Zugang zu Material und Geldern dieser Organisationen zu verschaffen und sich ihre Netzwerke zu Nutze zu machen, sie also vorsätzlich missbrauchen. Dieses Problem wurde im FATF-Bericht *Emerging Terrorist Financing Risks* angesprochen, dann aber umfassend in der Ausgabe des FATF-Berichts *Risk of terrorist abuse in non-profit organisations* vom Juni 2014 behandelt. In Kapitel 6 des Berichts aus 2014 ist eine umfassende Aufstellung allgemeiner Anhaltspunkte sowie konkreterer Anhaltspunkte für Terrorismusfinanzierung enthalten. Speziell für dieses Projekt wurde auch umfangreiches Material zu Risikoindikatoren vorgelegt. Die beispielhaften Anhaltspunkte, die kürzlich eingegangen sind, können in vier allgemeine Kategorien unterteilt werden: Spenden, Geldausgaben, Transaktionen und NPO-Verantwortliche.

[8] Siehe *Best Practices on Combating the Abuse of Non-Profit Organizations* (FATF, 2015c).

Wie im ersten Abschnitt unter *I. E. Nutzung der Anhaltspunkte* erwähnt, soll der vorliegende Bericht nicht als Grundlage für pauschale und undifferenzierte "De-risking practices" genutzt werden. Die nachstehenden Anhaltspunkte sollten daher nicht als Indiz dafür interpretiert werden, dass etablierte oder seriöse Wohltätigkeitsorganisationen, die in geographischen Räumen mit Präsenz einer Terrororganisation arbeiten, für die Institute nun ein höheres Risiko darstellen. Noch einmal, ein einzelner Anhaltspunkt allein kann nicht den Verdacht der Terrorismusfinanzierung rechtfertigen bzw. einen klaren Hinweis auf solche Aktivitäten liefern. Die FATF hat kürzlich ihre Standards zu NPOs aktualisiert um sicherzustellen, dass sie dem risikobasierten Ansatz entsprechen und keine legalen Wohltätigkeitsaktivitäten stören oder verhindern.

### Spenden

- Große Spendenbeträge werden von ausländischen Unternehmen/Konzernen auf das Konto einer NPO transferiert, besonders ohne erkennbare klare Beziehung.
- Die Anzahl der Überweisungen in kleiner Stückelung auf das Konto einer NPO ist ohne erkennbaren Grund angestiegen.
- Insgesamt große und nicht entsprechend plausible Beträge, besonders überwiegend Bareinzahlungen.
- Mehrere Bareinzahlungen auf ein Privatkonto, die als "Spenden" oder "Beiträge zu humanitärer Hilfe" oder ähnlich ausgewiesen sind (oder Bareinzahlungen mit der Auflage, das Bargeld an eine Person in einem Hochrisikoland zu überweisen).
- Ein großer Prozentsatz der Spenden/Vermögenswerte an NPOs stammt aus oder geht in Länder, die nicht mit dem Finanzstandort des Spenders übereinstimmen.
- Hohe Spendenbeträge einer fiktiven Person an eine NPO.
- Eine Person erhält Spenden auf einem Bankkonto, das für wohltätige Zwecke bestimmt ist, und überweist das Geld an Organisationen, die über elektronische Medien mit Terrorismusfinanzierung in Verbindung gebracht wurden.
- Eine Spende an eine NPO ist nur für sehr wenige Begünstigte bestimmt.
- Einzahlungen mittels monetärer Instrumente, die für eine legale Geschäftstätigkeit untypisch sind.
- NPOs, die in Konfliktgebieten agieren, erhalten Spenden von Unternehmen (die geschäftliche Interessen in diesen Gebieten haben) auf ihren Konten, entweder direkt oder über eine Serie von mehrschichtigen Transaktionen. Solche Gelder könnten mit Terrororganisationen in Zusammenhang stehen, die Unternehmen über NPOs erpressen.


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

Fallstudie: **Abzweigung von Geldern durch NPO-Interne**

Eine Person (Herr A) gründete eine gemeinnützige Stiftung, die vorgeblich Spenden für syrische Flüchtlinge, Personen, die medizinische und finanzielle Hilfe brauchen, und für den Bau von Moscheen, Schulen und Kindergärten sammelte. Herr A stand jedoch an der Spitze eines organisierten Systems, innerhalb dessen Spenden an einen Kreis von Verbündeten (Gruppe A) anstatt auf das Konto der Stiftung geleitet wurden. In den meisten Fällen wurde in der ersten Phase Geld über Geldtransferdienstleister geschickt und dann in bar transportiert. Anschließend wurde es entweder auf Kreditkartenkonten oder auf E-Wallets transferiert. Die Mitglieder der Gruppe A stellten die entsprechende Information (dass Gelder für die angegebenen Zwecke gesammelt werden) ins Internet, aber in Wirklichkeit wurden die Gelder als Hilfe für Terroristen und ihre Familien versandt und waren als finanzielle Unterstützung für terroristische Aktivitäten gedacht.

Dies wurde im Rahmen von Ermittlungen aufgedeckt, die von der FIU auf der Grundlage des regelmäßigen Monitorings von Organisationen auf ihrer nationalen Liste der ausgewiesenen Terrororganisationen und der mit ihnen in Verbindung stehenden Personen oder auf der Grundlage von Erkenntnissen der Strafverfolgungsbehörden geführt wurden. Durch die Analyse der gesammelten Informationen konnte die FIU die Verbindung zwischen verschiedenen Fällen feststellen: gemeinsame Einzahler und Empfänger und ähnlicher Modus Operandi beim Sammeln und Verteilen der Gelder. Im Rahmen der weiteren Zusammenarbeit mit den Strafverfolgungsbehörden konnte die FIU die direkte Verbindung zwischen Herrn A und den Aktivitäten des IS feststellen. Dies führte zu mehreren kriminalpolizeilichen Ermittlungsverfahren gegen Herrn A. Außerdem wurde er auf die interne Liste ausgewiesener Terrororganisationen gesetzt, und es wurde die Vermögenseinfrierung veranlasst. Gemäß Gerichtsbeschlüssen wurde das Vermögen der Mitglieder der Gruppe A eingefroren.

*Quelle: Russische Föderation (FATF-Bericht Financing of the Terrorist Organisation Islamic State in Iraq and the Levant, 2015a)*

### Ausgaben

- Organisationen, die eigentlich keine humanitäre Hilfe leisten, schicken Geld in Hochrisikoländer.
- Unklare Nutzung von Geldern für Ausgaben, die nicht mit den Aktivitäten einer NPO in Verbindung stehen.
- Transaktionen, bei denen als Zweck der Bau einer Einrichtung für eine NPO angegeben wird, besonders wenn der Begünstigte eine Person ist, die keinen Bezug zum Projekt zu haben scheint und keinem Bauunternehmen zugeordnet werden kann.
- Nutzung von Wohltätigkeitsorganisationen zum Verkauf von Ware.
- Bezahlung von Ware durch einen Dritten und nicht durch den Importeur.
- Die Ausgaben der NPOs "auf dem Papier" stehen in keinem Verhältnis zu den Erwartungen (z. B. Risiko, dass Gelder abgeschöpft, einem anderen Zweck zugeführt oder für TF-Zwecke in Anspruch genommen werden).

### Transaktionen

- Transaktionen werden über das Konto einer NPO durchgeführt, die nicht mit dem Muster und dem Rahmen des Zwecks oder der Geschäfte der Organisation übereinstimmen.
- Transaktionen der NPO entsprechen nicht der angegebenen Aktivität des Begünstigten/Unterstützers.

- Transaktionen sind geprägt von großen Geldflüssen über einen kurzen Zeitraum unter Beteiligung mehrerer NPOs, die nicht zu begründende Verbindungen zueinander haben, wie beispielsweise gleiche Adresse, Vertreter oder Mitarbeiter oder mehrere Konten mit wiederkehrenden gleichen Namen.
- Transfer der meisten gesammelten Gelder in geographische Räume, die gewöhnlich von Aktivitäten und Initiativen mit TF-Bezug geprägt sind.
- Transaktionen werden mit Gegenparteien erbeten, die auf Listen ausgewiesen wurden oder mit TF-Aktivitäten in Verbindung stehen.
- Jemand zahlt Geld auf mehrere eigene Konten ein und ersucht um Überweisung an sich selbst auf ausländische Konten mit Überweisungszweck Spende.
- Wiederholte Bareinlagen, die natürliche Personen auf ein NPO-Konto einzahlen, und anschließend wird das Geld auf Konten natürlicher oder juristischer Personen transferiert.
- Auf das Konto einer NPO erfolgen nur Gutschriften und Barabhebungen.

### NPO-Verantwortliche und andere Mitarbeiter

- Mehrere Personen mit Vollmacht für ein Konto, das von einer Person oder einer NPO ohne familiäre oder geschäftliche Beziehungen geführt wird; häufiger Wechsel der Personen, die Vollmacht für ein NPO-Konto haben.
- Konten, auf denen Gelder von neu gegründeten NPOs und Geldbeschaffern eingehen (es fand möglicherweise ein Wechsel oder vor kurzem eine Aktualisierung der Identität statt).
- Hohe Zahlungsanweisungen gehen auf die Konten der NPO-Gründer (oder anderer Personen, die mit den NPOs in Verbindung stehen, wie Verantwortliche oder Schatzmeister) und laufend erfolgen auf den Konten der NPO-Gründer Bargeldabhebungen.
- Gelder von NPOs befinden sich auf den Konten von natürlichen Personen.
- Unvollständige Angaben zum Auftraggeber von Transaktionen zugunsten von NPOs oder Personen mit Bezug zur Organisation.
- Verantwortliche (oder Angestellte) von NPOs, die Gelder unterschlagen, beispielsweise wenn die Gelder vor Abreise in Konfliktzonen abgehoben werden.
- Von Bankkonten von Verantwortlichen oder Kontaktpersonen, die in Konfliktgebieten tätig sind, könnte Lösegeld an Terrororganisationen gezahlt werden, damit sie ihre Geschäftsinteressen weiterführen können, oder Lösegeld könnte für Terrororganisationen kassiert werden.


for restricted use only, not for publication - © 2016

## G. ANHALTSPUNKTE MIT BEZUG ZU HANDEL UND WIRTSCHAFTSUNTERNEHMEN

Das rapide Wachstum der Weltwirtschaft hat Finanztransaktionen im Zusammenhang mit Waren und Dienstleistungen für internationale Bewegungen illegaler Gelder zunehmend attraktiv werden lassen. Die FATF hat die diesbezüglichen Schwachstellen im Zusammenhang mit Handel und Wirtschaftsunternehmen in einer Reihe von Berichten behandelt, unter anderem in den Berichten "Trade Based Money Laundering" (TBML), 2006 und 2012,[9] "Proliferation Finance", 2008[10], und "Free Trade Zones" (FTZs), 2010[11]. In einigen der Berichte wurden konkrete Risikoindikatoren ("Red flags") festgestellt. Obwohl nicht alle mit Terrorismusfinanzierung in Zusammenhang stehen, sind einige für den vorliegenden Bericht von Bedeutung und wurden aufgenommen.

Da größere Geschäftsbanken üblicherweise die Arten von Finanzprodukten und Dienstleistungen anbieten, die innerstaatlichen und internationalen Handel und kommerzielle Aktivitäten betreffen, sind sie mit hoher Wahrscheinlichkeit Zielscheibe handelsbasierter TF-Aktivitäten. Die Arten der Produkte und Dienstleistungen reichen von Geldüberweisungen vom Importeur zum Exporteur bis hin zu komplexeren Finanzprodukten wie Akkreditiven, Dokumenteninkassos und Sicherheiten/Bürgschaften. Der Finanzsektor stellt auch Exportfinanzierung bereit, um die Zeitspanne zwischen dem Geldbedarf zur Herstellung und zum Transport etc. bis zur Bezahlung der Produkte durch den Importeur zu überbrücken. Banken und andere Ausfuhrkreditagenturen gewähren Händlern Darlehen und Kredite, damit sie Ware oder Geräte kaufen und weiterverkaufen können. Alle Finanzinstitute, die an Handelsfinanzierung beteiligt sind, egal in welchem Geschäftsbereich, haben sowohl kommerzielle Anreize wie auch rechtliche Verpflichtungen zur Durchführung von CDD und potentieller Kontoüberwachung. Die Art und Intensität der CDD und wie sie organisiert ist, kann zwischen den Finanzinstituten, von Transaktion zu Transaktion und aufgrund der Bestimmungen in dem jeweiligen Land jedoch erheblich variieren. Mögliche Risikoindikatoren mit Bezug zu Handel:

- Natürliche Personen, die mit Handel und Herstellung von Waren und Technologie befasst sind, sind national oder international gelistet oder Gegenstand von TF-Sanktionen.
- Eine Geschäftsbeziehung wurde von natürlichen oder juristischen Personen begründet, die mit einer Terrororganisation in Verbindung stehen könnten.
- Kurz nach Listung wird eine in Zusammenhang stehende Firma angemeldet und ein neues Konto eröffnet.
- Zahlreiche Personen sind berechtigt, Geschäfte im Namen der juristischen Person oder Organisation zu führen.
- Geldtransfers in Hochrisikoländer unmittelbar nach Gründung einer juristischen Person, wenn noch keine Geschäftsbeziehung aufgebaut wurde.
- Bargeldintensive Geschäfte werden über MVTS anstatt per Überweisung durchgeführt.
- Transaktionsaktivitäten zwischen Privatpersonen oder Unternehmen und neu angemeldeten Firmen ohne scheinbare Geschäftsbeziehungen oder
- Firmen, die scheinbar nicht geschäftstätig sind (z. B. generische Import-Export-Aktivitäten, keine Website etc.).

[9] *Trade-based money laundering* (APG, 2012)
[10] *Typologies report on Proliferation Financing* (FATF, 2008)
[11] *Money laundering vulnerabilities of Free Trade Zones* (FATF, 2010)

© 2016 - **nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt**

- Zahlreiche eingehende Barschecks werden ohne ersichtliche rechtmäßige Zwecke auf Geschäftskonten eingezahlt.
- Reisebüros organisieren religiöse Pilgerreisen in Hochrisikoländer und das zu Preisen, die weit unter denen anderer Reisebüros liegen.
- Zahlung für Warenlieferungen, die nicht mit dem Servicegrad in Einklang stehen oder der geographischen Struktur des Landes, in das die Ware geliefert wird.
- Der Käufer (natürliche Person) einer Ware wohnt an einem Ort, der sich in einem anderen Land befindet als der Endempfänger der bestellten Ware.
- Die angemeldete Geschäftsbranche einer juristischen Person stimmt nicht mit den tatsächlichen Geschäften überein, oder der tatsächliche Begünstigte der bestellten Ware erscheint nicht als Endbegünstigter.
- Zahlreiche Geldeingänge auf Geschäftskonten ohne ersichtliche rechtmäßige Zwecke.
- Plötzliche Zunahme von Transaktionen auf einem MVTS-Geschäftskonto.
- Wirtschaftsunternehmen mit Geschäften in Hochrisikoländern handeln mit Ware, die als Dual use-Ware gilt oder bei terroristischen Aktivitäten genutzt werden könnte.
- Wirtschaftsunternehmen führen Geschäfte in Hochrisikogebieten durch, die anfällig für Missbrauch und Nötigung sind (z. B. Zahlungen, um Zugang zu Häfen und Handelsplätzen, die von Terrororganisationen kontrolliert werden, zu erhalten).
- Investitionen in Transportunternehmen, die die intensive Nutzung von Bargeld erlauben und auf Routen und in Zonen tätig sind, die mit illegalen Aktivitäten in Verbindung stehen.
- Anlage von Geldern in Gründung/Betrieb von Firmen, die Fahrzeuge in Hochrisiko-Konfliktzonen an- und verkaufen.
- Ungewöhnliches Handelsvolumen in bargeldintensiven Geschäftszweigen in Gebieten, die an Konfliktzonen angrenzen.


for restricted use only, not for publication - © 2016

Fallstudie: **Handelsbasierte Terrorismusfinanzierung**

Nach Listung von Firma A als unerlaubte Vereinigung in Israel konnte die Firma keine Ware über israelische Häfen importieren. Trotz dieser Restriktionen kooperierte Firma B, eine örtliche Firma, die Grundnahrungsmittel importiert und vermarktet, mit Firma A, um die Beschränkungen zu umgehen. Firma B importierte zunächst Ware nach Israel, und anschließend löste ein Mittäter, Firma C, die Ware im Hafen aus und lagerte sie. Später transferierte Firma B die Ware an Firma A in ein Hochrisikogebiet für TF. Im Rahmen der Zahlungsabwicklung überwies Firma A Gelder von ihren Konten an Firma B. Der Wert der Waren und der Überweisungen wurde auf mehrere Millionen israelische neue Shekel (NIS) geschätzt.

*Quelle: Israel (Emerging Terrorist Financing Risks (FATF, 2015))*

Fallstudie: **Handel mit Ware, die zu Terrorismusfinanzierungszwecken geschmuggelt wird**

Es wurden Unstimmigkeiten bei einer Handelsrechnung festgestellt, bei der der Käufer einen anderen Namen hatte als der Begünstigte der Überweisung, bei dem es sich um eine Spedition handelte und der daher möglicherweise nicht der Endempfänger der Ware war. Hinzu kam, dass der Verwendungszweck der Überweisung als Bezahlung von Nahrungsmitteln angegeben wurde, auf der Rechnung jedoch medizinische Geräte genannt wurden und keine Lieferadresse angegeben war. Die Erkenntnisse der Strafverfolgungsbehörden ergaben eine Verbindung zwischen der Firma für medizinisches Gerät und einer Terrororganisation.

*Quelle: Frankreich*

### Illegaler Handel mit Antiquitäten/Kulturerbe

Mit Resolution 2199 des UN-Sicherheitsrats (UNSCR) wurde ein weltweites Moratorium für den Handel mit Kulturgütern aus Syrien (seit dem 15. März 2011) und aus dem Irak (seit dem 6. August 1990) verhängt. Laut *Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat* ist es angesichts des Ausmaßes der Plünderungen und ihres beträchtlichen wirtschaftlichen Wertes wahrscheinlich, dass zahlreiche Güter von kriminellen Netzwerken verwahrt werden. Nimmt die Aufmerksamkeit ab, werden Personen und Gruppierungen, die an internationalen kriminellen Netzwerken beteiligt sind, anfangen, weitere „gewaschene" Güter auf den Markt zu bringen.

Der IS scheint hauptsächlich im Anfangsstadium von diesem illegalen Handel zu profitieren, indem er Ausgrabungsgenehmigungen an einheimische Bürger und Unternehmer verkauft, den Verkauf von Münzen, kleinen Skulpturen, Keramik und Mosaiken, die Einheimische und Unternehmer ausgraben, mit Steuern belegt und Steuern auf Antiquitäten erhebt, die außer Landes geschmuggelt werden. Die Vereinten Nationen stellen fest, dass, während die Gewinnspannen für Antiquitäten aus Plünderungen am ersten Verkaufsort potentiell gering sind, Handel mit Antiquitäten in beträchtlichem Umfang betrieben werden muss, wenn beträchtliche Gelder generiert werden sollen[12]. Es läuft eine Initiative für die Strafverfolgungsbehörden, Kunsthändler, Auktionshäuser, Museen und den Antiquitätenmarkt, um für den Verkauf geplünderter kultureller Artefakte zu sensibilisieren, diese aufzuspüren und den Verkauf zu stoppen, es ist jedoch nicht klar, inwiefern diesbezügliche Transaktionen den offiziellen Finanzsektor berühren. Alle Finanztransaktionen, die mit Kulturgütern in Zusammenhang stehen, die aus Syrien, dem Irak oder Libyen stammen könnten, sollten Gegenstand einer eingehenden Überprüfung und entsprechender Vorsichtsmaßnahmen sein. Die Länder sind auch verpflichtet, ein Verbot von Antiquitäten in ihrem Land zu melden, die vom oder an den IS transferiert werden (siehe Absatz 15 UNSCR 2253 (2015) und Absatz 12 UNSCR 2199 (2015)).

[12] *Challenges business entities face in implementing Security Council resolution 2199 (2015).* (UN SC, 2016).

- Finanztransaktionen mit Bezug zu Kulturgütern ähnlich denen, die in UN-Resolution UNSCR 2199 und vom Internationalen Museumsrat (International Council of Museums, ICOM) auf den Listen "Emergency Red List of Iraqi Antiquities at Risk" (2003), "Emergency Red List of Syrian Cultural Objects at Risk" (2013) und "Emergency Red List of Libyan Cultural Objects at Risk" (2015) genannt werden.
- Finanztransaktionen im Zusammenhang mit Antiquitäten aus dem Irak und aus Syrien (auch kleine Stücke, wie Münzen und kleine Statuen), die im Internet und den sozialen Medien zum Verkauf angeboten werden.
- Finanztransaktionen im Zusammenhang mit Lieferungen von Geräten zum Boden-Monitoring/-Scanning, wie Metalldetektoren, die von Plünderern zur Ausgrabung antiker Artefakte und Kulturgüter benutzt werden.
- Falsche Einfuhrerklärungen, in denen Artefakte vorgeblich aus Ländern stammen, die an Syrien und den Irak angrenzen.

### Erdöl- und Gassektor

Gemäß Input der relevanten Akteure und des Privatsektors wurden Anhaltspunkte speziell mit Bezug zum IS gewünscht. Während zahlreiche Anhaltspunkte im vorliegenden Bericht für die konkrete Bedrohung in Bezug auf den IS von Bedeutung sind, liegt der Schwerpunkt dieses Abschnitts ausdrücklich auf den Anhaltspunkten, die mit Erdölförderung und Raffinationsarbeiten in Zusammenhang stehen, darunter auch Kauf, Lieferung oder Handel mit Ölförderungs- und Raffineriegerät.

Mit Resolution des UN-Sicherheitsrats (UNSCR) 2199 werden alle Staaten aufgefordert, jeglichen direkten oder indirekten Handel mit dem IS mit Erdöl und Erdölprodukten, modularem Raffineriegerät und entsprechenden Materialien zu verhindern und zu unterbinden. Die Resolution betont auch, dass alle Staaten alle Vermögenswerte von Gruppierungen mit IS-Bezug sowie die Vermögenswerte von Personen, Gruppen, Unternehmen und Organisationen, die mit diesen in Verbindung gebracht werden, einzufrieren haben. Dies gilt auch für Erdöl, Ölprodukte, modulare Raffinerien und entsprechendes Material. Die Institute sollten daher die allgemeinen Arten von Bohr- und Raffineriegeräten sowie Ersatzteilen der Kohlenwasserstoffindustrie kennen, für deren Kauf sich der IS interessieren könnte. Folgende Anhaltspunkte könnten von Bedeutung sein:

- Finanzielle Verbindungen zu Erdölfirmen, Maklern und Zulieferfirmen in Hochrisikogebieten.
- Privatpersonen oder Unternehmen liefern/verschiffen plötzlich Erdöl nach Syrien, in den Irak oder in angrenzende Staaten, und die Aktivitäten passen nicht zum Geschäftszweig des Kunden.
- Strohfirmen werden zur Verschleierung des Handels und Verkaufs von Erdölprodukten und den entsprechenden Teilen genutzt.
- An den Transaktionen sind möglicherweise Firmenmäntel beteiligt (z. B. verfügen die Firmen nicht über ein hohes Niveau an Kapitalisierung oder es gibt andere Anhaltspunkte für einen Firmenmantel).
- Eine Spedition ist als Endempfänger des Produkts angegeben.
- Telegraphische Anweisungen oder Zahlung durch oder aufgrund von Parteien, deren Identität auf dem Original-Akkreditiv oder in anderen Papieren nicht ausgewiesen ist.


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

- Ein Neukunde beantragt eine Akkreditiv-Transaktion während das neue Konto noch nicht genehmigt ist.
- Die Transaktion betrifft die Verwendung von mehrfach geänderten bzw. verlängerten Akkreditiven.

Zur Beschränkung der Fähigkeit des IS, finanziell vom Erdöl zu profitieren, das in seinen Gebieten gefördert wird, hat die CFIG mit der internationalen Erdölindustrie zusammengearbeitet, um eine erläuternde Liste von Erdölförder- und Raffineriegeräten[13] zu erstellen, die der IS vermutlich benötigt, um seine Erdölproduktion und Raffinationstätigkeiten weiterführen zu können. Die Liste kann zur Feststellung von Geräten verwendet werden, um die Lieferung oder den Umschlag von Bohr- und Raffineriegerät in Gebiete zu verhindern, die vom IS kontrolliert werden. Die Liste kann an Vertreter der Erdölindustrie, Logistikunternehmen, Grenzkontrollbehörden und an Hersteller von Bohr- und Raffineriegerät weitergegeben werden. Die Liste kann schließlich auch für große Geschäftsbanken und für den Finanzsektor im Rahmen von Handelsfinanzierungen von Nutzen sein.

[13] *Illustrative List of Oil Drilling and Refinery Equipment* (US DOS, 2016)

© 2016 - **nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt**

## III. AUSTAUSCH VON HINTERGRUNDINFORMATIONEN ZUR VERBESSERUNG DER RISIKOINDIKATOREN

Auch wenn Risikoindikatoren ein nützliches Werkzeug sind, so sind sie kein Ersatz für enge Beziehungen zwischen dem privaten und dem öffentlichen Sektor beim Austausch von Informationen über TF-Risiken. Durch die FATF-Standards sind die Länder gehalten, robuste rechtliche und operative Rahmen zu entwickeln, um den Privatsektor über Geldwäsche-/Terrorismusfinanzierungsrisiken zu informieren und sicherzustellen, dass der Privatsektor diese Risiken bei der Durchführung seiner Geschäfte berücksichtigt. Im FATF-Bericht *Emerging Terrorist Financing Risks* wurde die Notwendigkeit unterstrichen, Daten der Meldestellen mit Hintergrundinformationen und bereinigten Daten der Behörden zu kombinieren. Aufgrund der Dringlichkeit dieser Problematik ist die Fähigkeit zum schnellen und sicheren Austausch von Information im Zusammenhang mit Terrorismusfinanzierung von wesentlicher Bedeutung. Dieser Abschnitt konzentriert sich nur auf nationale Mechanismen zur Verbesserung des Informationsaustauschs zwischen dem öffentlichen und dem privaten Sektor und zur Verbesserung der Risikoindikatoren.

Als Reaktion auf die derzeitigen TF-Risiken unternimmt die FATF erhebliche Anstrengungen beim Informationsaustausch zwischen dem öffentlichen und privaten Sektor und innerhalb beider. Die Diskussionen zum vorliegenden Bericht ergaben eine Reihe von nützlichen Schritten zur Verbesserung der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor und gemeinsame Bemühungen zur Feststellung und zum Kommunizieren von Risiken sowie zur Entwicklung von Risikoindikatoren. Dieser Abschnitt liefert eine erste Einschätzung der Tools.

Es wurde auch eine Reihe von Faktoren festgestellt, die den Informationsaustausch im Zusammenhang mit TF sowohl national als auch multilateral verhindern oder einschränken. Terrorismus und Terrorismusfinanzierung sind naturgemäß höchst vertraulich zu behandeln und erfordern Schutz, sogar zwischen den zuständigen Behörden. Ein Mangel an Vertrauen zwischen den zuständigen Behörden und dem Privatsektor könnte den Austausch sensibler Daten hemmen. Der öffentliche Sektor hat die schwierige Aufgabe, die Balance zwischen Geheimhaltung sensibler, operativer Informationen und Sensibilisierung für TF-Risiken bei den betroffenen Stellen zu finden. Beziehungen sollten aufgebaut werden, um durch die Schaffung einer Community aus Experten die Fähigkeiten beider Seiten wirkungsvoll zu nutzen. Es muss sich hier um einen laufenden Prozess handeln, da der Privatsektor ein präzises Verständnis für die sich ständig verändernde Risikoumgebung haben muss.

### A. FEEDBACK AN MELDESTELLEN

Risikoindikatoren helfen dem Privatsektor (und den FIUs) bei der Feststellung bestimmter verdächtiger Verhalten, die mit Terrorismusfinanzierung in Zusammenhang stehen könnten. Der Privatsektor ist allerdings immer auf der Suche nach stärkerer und zeitnaher Orientierungshilfe und Feedback vom öffentlichen Sektor hinsichtlich der Qualität und der Zweckmäßigkeit seiner Verdachtsmeldungen (STRs), um die Identifizierungs- und Analysemethoden verbessern zu können. Orientierungshilfe, Feedback und Sensibilisierung sind ein sehr taktisches Element, da den Meldestellen aussagekräftige und "gezielte" Informationen mit dem expliziten Zweck zur Verfügung gestellt werden, dem Privatsektor zu helfen, sein Meldeverhalten zu verdächtigen Aktivitäten zu verbessern. Diese Interaktion führt schließlich zu einer noch besseren Sensibilisierung der Meldeinstitute durch die zuständigen Behörden, was das Meldeverhalten weiter verbessert.


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

Der Privatsektor findet es zudem hilfreich, Entwürfe von Risikoprofilen und Anhaltspunkten betreffend den Privatsektor, wenn möglich, zu prüfen und den öffentlichen Behörden ein Feedback zu geben, bevor diese veröffentlicht werden, um so das effektivste Produkt zu erhalten.

Fallstudie: **Niederlande**

Die Niederlande haben ein Beispiel vorgelegt, wie ihre Behörden Anhaltspunkte beim Privatsektor testen, um ihre Umsetzbarkeit und ihren Nutzen zu bewerten. Entwürfe von Risikoprofilen werden aufgrund von ersten Ergebnissen der Meldestellen überarbeitet. In der endgültigen Version werden Risikoprofile von der zuständigen Behörde in Form einer Orientierungshilfe an die Meldestellen weitergegeben. In diesem Fall steigern eine fortgesetzte Orientierungshilfe und Feedback die Effektivität der Entwicklung der TF-Indikatoren.

Fallstudie: **Australien**

Australien hat ein Beispiel vorgelegt, wie dort Orientierungshilfe und Feedback zu STRs regelmäßig einer Reihe von zentralen Stakeholdern gegeben wird. Vierteljährlich treffen sich FIU und Strafverfolgungsbehörden mit den vier größten Banken, um Compliance-Fragen zu besprechen und STR-Feedbacks zu geben. Die Treffen haben zu einem 300-prozentigen Anstieg der Verdachtsmeldungen geführt.

### B. Arten der ausgetauschten Informationen

In einem ersten Feedback zu diesem Bericht betonte der Privatsektor, dass Risikoindikatoren zwar nützlich seien, sie jedoch um detaillierte Hintergrundinformationen ergänzt werden müssten. Während es schwierig ist, die Informationen in diesem Bericht weiterzugeben, haben die Teilnehmer eine Reihe von Wegen festgestellt, über welche die Behörden dem Privatsektor die benötigten Informationen zur Verfügung stellen können - über allgemeine und gezielte Öffentlichkeitsarbeit, ohne die Vertraulichkeit der Informationen zu beeinträchtigen.

Die Behörden müssen richtig verstehen, welche Art von Informationen und Erkenntnissen für den Privatsektor bei der Feststellung terroristischer Aktivitäten wertvoll sind. Die Reaktionen zeigen, dass die meisten zuständigen Behörden den Meldestellen bereinigte Fallstudien und Typologien zu Terrorismusfinanzierung zur Verfügung stellen können, ohne dass rechtliche Hindernisse über diese Art der Daten bestehen. Diese Informationen werden häufig von der FIU in Jahresberichten, Newslettern oder E-Bulletins vorgelegt. Oftmals können detailliertere Versionen von Fallstudien auf entsprechenden Wegen mit bestimmten Unternehmen ausgetauscht werden.

Nationale Risikoanalysen sind ein weiterer nützlicher Mechanismus bei der Verbreitung von Fallstudien und Typologien. Diese Einschätzungen sind für eine frühzeitige Zusammenarbeit mit dem Privatsektor und eine erhöhte Sensibilisierung für bestimmte Risiken nützlich. Eine festgestellte Herausforderung betrifft die Länder, in denen keine Fallstudien oder Typologien in Bezug auf Terrorismusfinanzierung vorliegen, und sie Fallstudien nur ein anderes Land betreffend vorlegen können.

Um die vorliegenden Daten interpretieren zu können, benötigt der Privatsektor häufig Unterstützung und detailliertere Hintergrundinformationen des öffentlichen Sektors, die geheimhaltungsbedürftig sein könnten. Einige Unternehmen des Privatsektors haben betont, wie wichtig es ist, eine Liste relevanter Personen (z. B. Personen, die Gegenstand von Monitoring, Observationen oder Ermittlungen sind) zu bekommen. Solche listenbasierten Ansätze könnten die Feststellung bestimmter Transaktionen unterstützen und das Netzwerk der Personen, die mit den Gelisteten in Zusammenhang stehen,

aufdecken. Die Weitergabe von Personenlisten ist jedoch ein großes Problem, da die Wahrung der Geheimhaltung von laufenden Ermittlungen und Operationen für die Strafverfolgungsbehörden Priorität hat. Einige Teilnehmer des Privatsektors, besonders die mit größeren Datensätzen, betonen, dass es ihnen - auch wenn es nicht möglich ist, einen speziellen Sachverhalt zu übermitteln - schon helfen würde, einen allgemeinen Hinweis auf die Art der auftretenden Aktivität zu bekommen, um weitere Finanzerkenntnisse liefern zu können.

Der Privatsektor kann Daten über einen Kunden zu CDD-Zwecken vorhalten, wie z. B. IP-Adressen, Handynummern und Standortdaten. In Kombination mit Informationen der zuständigen Behörden können solche CDD-Informationen zur Aufdeckung möglicher TF-Aktivitäten wichtig werden. Durch die zuständigen Behörden wurden spezielle Länder hervorgehoben, die ein höheres Risiko der Terrorismusfinanzierung darstellen oder in denen bestimmte Geschäfte festgestellt wurden, die ein höheres Sicherheitsrisiko darstellen könnten. Die Strafverfolgungsbehörden haben beispielsweise Erkenntnisse zu bestimmten Städten oder Gegenden weitergegeben, in denen bekannte Vermittler und Helfer von ausländischen Terrorkämpfern wohnen. In einigen Fällen werden Behörden eine detaillierte Datenauswertung zu geographischen Gegenden betreffend Grenzen, Logistik und Transitbereiche übermitteln. In anderen Fällen haben Strafverfolgungsbehörden Finanzinformationen an Banken weitergegeben, die sie durch große Sicherstellungen erlangt haben (z. B. Lieferscheine, Quittungen etc.), und die Banken gleichen sie mit ihren Systemen ab, um relevante Informationen zu verdächtigen Transaktionen festzustellen.

Informationen zu Echtzeitereignissen sollten detaillierter und konkreter sein, damit der Privatsektor umgehende Maßnahmen ergreifen kann. Wie oben erwähnt unterliegen jedoch Informationen zu konkreten Personen und Ereignissen häufig Einschränkungen. Diese praktischen Herausforderungen liegen auch bei laufenden oder aktiven Ermittlungsverfahren zu Terrorismus oder Terrorismusfinanzierung vor. In diesen Fällen ist der Erkenntnisaustausch, auch über eine bereinigte Fallstudie, oft schwierig. Behörden und Unternehmen können daher aufgrund rechtlicher Beschränkungen, Schutz der Privatsphäre und Haftungsfragen nicht in gutem Glauben handeln. Die Festsetzung von Ausnahmen oder Protokollen könnte es Behörden ermöglichen, Informationen mit dem Privatsektor auszutauschen, die dringend benötigt werden, wenn ein Echtzeitereignis vorliegt, bei dem es um Leben und Tod geht oder gehen könnte.


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

Fallstudie: **Vereinigte Staaten**

Der USA PATRIOT Act - § 314(a) - erlaubt es FinCEN, dem US-Financial Crimes Enforcement Network, an mehr als 43.000 Ansprechpartner bei über 22.000 Finanzinstituten heranzutreten, um Konten und Transaktionen von Personen zu ermitteln, die an Terrorismus oder Geldwäsche beteiligt sein könnten. Die FinCEN stellt diese Anfragen zu eigenen analytischen und Ermittlungszwecken und im Namen von Bundes-, bundesstaatlichen, lokalen und bestimmten ausländischen (z. B. EU) Strafverfolgungsbehörden. § 314 (a) liefert lediglich Ermittlungsansätze (Finanzerkenntnisse) und ist kein Ersatz für eine „Subpoena" oder andere rechtliche Verfügung, die üblicherweise auf die Feststellung relevanter Informationen folgt, um Erkenntnisse zu weiteren Ermittlungs- oder Beweiszwecken zu beschaffen.

Über ein beschleunigtes Kommunikationssystem kann ein Ermittler unter Anwendung von § 314(a) vertraulich zu behandelnde Hinweise direkt an die Meldestellen steuern. FinCEN verfügt über ein sicheres E-Mail-System zur Übermittlung geheimhaltungsbedürftiger Informationen. Anhand der Erstinformation, die die Finanzinstitute liefern, kann der Ermittlungsfokus schnell auf relevante Orte und Aktivitäten konzentriert werden. Ferner veranstaltet FinCEN hinsichtlich der Stellung von Erkenntnisanfragen nach § 314(a) Diskussionsrunden zum Informationsaustausch mit den entsprechenden Finanzinstituten. Diese kooperative Partnerschaft zwischen der Finanzgemeinschaft und den Strafverfolgungsbehörden ermöglicht es, verschiedene Teilinformationen festzustellen, zusammenzuführen und schnell auszuwerten.

Konkrete und gezielte Orientierungshilfen, Warnhinweise und Mitteilungen werden vom Privatsektor als nützlichste Informationsart angesehen. Diese Warnhinweise werden manchmal über sichere Kanäle, abhängig von der Vertraulichkeit der Daten, übermittelt. Sie liefern belastbare Hintergrundinformationen über die betreffenden TF-Aktivitäten, weisen den Privatsektor auf die Risikofelder hin und erklären nicht nur die möglichen Anhaltspunkte für die Aktivitäten sondern auch, wie der Privatsektor ihnen im Rahmen seiner Geschäfte begegnen kann. In einigen Fällen umfasst die Orientierungshilfe eine Liste von Hochrisikopersonen oder juristischen Personen, die mit der Aktivität in Verbindung stehen. Damit diese Informationen für den Privatsektor so effizient wie möglich sind, sollten die Behörden des öffentlichen Sektors jedoch konkrete Informationen, Personendaten (Name, Geburtsdatum) zu diesen Hochrisikopersonen/-unternehmen übermitteln. Gezielte nationale und internationale Finanzsanktionen gegen Personen und Unternehmen sollten Finanzinstituten proaktiv zur Verfügung gestellt werden, und zwar kurz vor der offiziellen Veröffentlichung, um ein besseres Screening und die Vereitlung von Versuchen zu gewährleisten, Gelder vor Einfrieren zu bewegen.

Fallstudie: **Russische Föderation**

Die russische FIU (Rosfinmonitoring) hat ein mehrschichtiges Anhaltspunktesystem für die russischen Finanzinstitute zur Bekämpfung der Terrorismusfinanzierung entwickelt. Diese Anhaltspunkte sind in drei Gruppen unterteilt:

1) ein regionales Merkmal (das die Transaktion mit einem bestimmten Gebiet in Verbindung bringt);

2) initiierende Kriterien;

3) unterstützende (Hilfs-) Kriterien.

Um ein bestimmtes Gebiet als Zone einer zunehmenden terroristischen Bedrohung identifizieren zu können, sollten die offiziell vorliegenden Erkenntnisse verwendet werden, die von internationalen (zwischenstaatlichen) Organisationen veröffentlicht wurden, darunter auch die FIU-Zusammenschlüsse. Transaktionen, die unter die Anhaltspunkte der Gruppe 1 fallen, werden als initiierend bezeichnet, d.h. Transaktionen, die einer Prüfung unterliegen, zusammen mit einer Betrachtung unterstützender (Hilfs-) Transaktionen, die unter die Gruppe 2 fallen.

Einige Anhaltspunkte werden dann als thematische Punkte entwickelt, wie z. B.:

FTF-Anhaltspunkte werden in zwei weitere Kategorien unterteilt:

- Anhaltspunkte einer externen Kategorie, die das Verhaltensmodell und die speziellen Charakteristika von Transaktionen mit Geldern aufweisen, die von FTF in Hochrisikoländern durchgeführt werden, sowie
- Anhaltspunkte einer internen Kategorie, die das Verhaltensmodell und die Charakteristika von Transaktionen mit Geldern aufweisen, die von FTF in ihren Heimatländern begangen werden.

Anhaltspunkte für "radikale Zentren" und "Geschäftsstrukturen" bestehen aus den Kategorien "initiierende" und "unterstützende" (Hilfs-) Kriterien. Im Ergebnis sollte erwähnt werden, dass durch die Nutzung dieses mehrschichtigen Indikatorensystems sowohl Kreditinstitute als auch FIUs in die Lage versetzt werden, überflüssige "Interferenzen" (irrelevante Daten) bei den gemeldeten Operationen zu vermeiden und sich auf spezielle Gruppen von Transaktionen zu konzentrieren, die im Verdacht der Terrorismusfinanzierung stehen.

## C. MECHANISMEN ZUR ZUSAMMENARBEIT MIT DEM PRIVATSEKTOR

Die Beteiligten an diesem Projekt betonten die Bedeutung einer zwei-Wege-Beziehung zwischen dem privaten und dem öffentlichen Sektor. Die Behörden haben eine Vielzahl von Mechanismen entwickelt, um dies zu realisieren. Zu den Mechanismen können formelle Tagungen und informelle Besprechungen gehören, sowohl auf bilateraler Ebene als auch mit mehreren Unternehmen. Die meisten Länder haben angegeben, mindestens einmal jährlich ein Forum oder Seminar mit dem Privatsektor abzuhalten, um TF-Risiken und -Trends zu besprechen. Der Schwerpunkt dieser Treffen unterscheidet sich, abhängig von der zuständigen Behörde, die beteiligt ist (z. B. Strafverfolgungsbehörde, FIU oder Aufsichtsbehörde). Unabhängig von der ausrichtenden Behörde werden operative Organisationen, wie Strafverfolgungs- oder Sicherheitsbehörden, häufig beteiligt, um praktische Fallbeispiele oder konkrete Informationen zu Risiken zu liefern. In anderen Fällen finden Seminare zu TF-Risiken als Teil der Konferenzen, Seminare und Schulungen für die Meldestellen statt. Ferner kann eine Sensibilisierung auf Initiative des Privatsektors anstatt auf Initiative der Regierung erfolgen, damit eine ausführlichere Diskussion über die potentiellen TF-Aktivitäten geführt werden kann.

Regelmäßige, zeitnahe "one-to-one"-Treffen mit ausgewählten, sicherheitsüberprüften Stakeholdern sind ein nützlicher Mechanismus zum Besprechen konkreter Feedbacks. Die zuständigen Behörden (besonders FIU oder Strafverfolgungsbehörden) können oft ein Feedback darüber geben, ob ein gemeldeter Verdacht begründet war, indem sie Beispiele dafür geben, wie die Information letztendlich von Strafverfolgungs- und Justizbehörden genutzt wurde. In den Zulieferungen wurde auch darauf


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

hingewiesen, dass sich Vertreter der Strafverfolgungsbehörden oder anderer Behörden direkt mit den Compliance-Mitarbeitern treffen sollten, die für die Feststellung verdächtiger Aktivitäten in Bezug auf Terrorismusfinanzierung verantwortlich sind, wenn ein konkretes Feedback abgegeben wird. Die Behörden können den Inhalt einer STR häufig mit einer Meldestelle besprechen. Hierdurch können diese ihre Risikomonitoringsysteme besser verstehen und feststellen, ob Anpassungen vorgenommen werden müssen. Wie oben erwähnt kann ein Feedback aufgrund sensibler Informationen bei Ermittlungsverfahren mit Terrorismusbezug möglicherweise nicht gegeben werden.

Hier könnte unter dem Dach erklärten Rechtsschutzes, geschützter Foren oder unterzeichneter Vertraulichkeitsvereinbarungen agiert werden. Einige Länder erklärten, dass ein effektiver Mechanismus zur Unterstützung des Austauschs sensibler oder die nationale Sicherheit betreffender Daten darin besteht, Angestellte in Schlüsselpositionen des Privatsektors sicherheitsüberprüfen, bevollmächtigen und zur Entgegennahme solcher Informationen berechtigen zu lassen. In solchen Fällen werden die Strafverfolgungs-, Sicherheitsbehörden und Nachrichtendienste bilaterale Treffen mit ausgewählten Firmen im Finanzbereich abhalten, bei denen Angestellte in Schlüsselpositionen für die Zwecke des Treffens berechtigt wurden. Dann werden vertraulich zu behandelnde oder eingestufte Informationen mit TF-Bezug auch zu laufenden Verfahren ausgetauscht. Ein weiterer Mechanismus ist ein rechtlich geschütztes Diskussionsforum, in dem alle relevanten Behörden des öffentlichen und des privaten Sektors Trends, Fälle und Fragen mit TF-Bezug auf vertrauliche, aber nicht eingestufte Art ansprechen können.

In einigen Fällen wurden spezielle TF-Arbeitsgruppen oder Task Forces aus dem öffentlichen und privaten Sektor eingerichtet. Beispiele hierfür sind die Joint Money Laundering Intelligence Taskforce (OMLIT)des Vereinigten Königreichs[14], Australiens Major Reporters Forum und der Domestic Security Alliance Council (DSAC) der USA[15]. Diese Arten von Task Forces stellen ein Forum für operative Zusammenarbeit als ein Instrument zur Verbesserung der Analyse- und Ermittlungsfunktionen aller Beteiligten.

Die Schweiz liefert ebenfalls ein gutes Beispiel solcher Interaktion, an der weitere Stakeholder aus Branchen beteiligt sind, die keine Meldepflichten haben, um Diskussionen voranzutreiben und das Verständnis für Risiken zu verbessern.

Fallstudie: **Ägypten**

Die Federation of Egyptian Banks(FEB) wurde als unabhängige, Non-Profit-Organisation gegründet. Sie verbindet alle ägyptischen und ausländischen Banken, die in Ägypten arbeiten. Ziele der FEB sind Diskussionen und Austausch zu gemeinsamen Themen zwischen den Mitgliedern des Bundes. Dies erfolgt zusätzlich zur Abgabe von Stellungnahmen zu Gesetzesentwürfen und Vorschlägen von Änderungen der derzeitigen Gesetzgebung in Bezug auf den Bankensektor.

Als eine Initiative der FEB wurde 2003 eine Compliance Officer Association geschaffen. Alle Compliance-Officers der in Ägypten tätigen Banken sind Mitglieder dieser Vereinigung. Es werden regelmäßige Treffen veranstaltet, um Vorschläge oder Probleme hinsichtlich der Bekämpfung von Terrorismusfinanzierung und Geldwäsche zu besprechen. Die ägyptische Zentralbank und die ägyptische FIU (EMLCU) werden zur Teilnahme an den Treffen eingeladen, um Feedback zu geben und technische Unterstützung zu leisten bei Problemen, die die Compliance-Officers ansprechen.

[14] Joint Money Laundering Intelligence Taskforce (NCA)
[15] www.dsac.gov

Es bedarf auch landesintern eines Mechanismus oder Prozesses für den Privatsektor, den Strafverfolgungs-/Sicherheitsbehörden in beinahe Echtzeit potentielle TF-Transaktionen zu melden, oder zumindest solche, die darauf zu deuten scheinen, dass ein Terrorakt bevorstehen könnte. Dies setzt voraus, dass die zuständige Behörde über einen Kanal verfügt, diese Art von Informationen entgegenzunehmen, und sie entsprechend reagieren kann, beispielsweise über spezielle Telefon- "Hotlines".


nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016

## IV. SCHLUSSFOLGERUNGEN

Der vorliegende Bericht stellt einen bedeutsamen Fortschritt dar, wie die FATF Risikoindikatoren entwickelt, die helfen, terroristische Aktivitäten und Terrorismusfinanzierungsaktivitäten aufzudecken. Der Bericht macht bewusst, dass das Erkennen von Terrorismusfinanzierungsaktivitäten ein facettenreicher Prozess ist und nicht auf einzelnen, isolierten Anhaltspunkten beruhen kann, die in automatisierte Systeme eingespeist werden können. Die FATF arbeitet mit einer Reihe von Unternehmen des Privatsektors zusammen, um sicherzustellen, dass der vorliegende Bericht für deren tägliche Arbeit relevant und nützlich ist und mit Methoden der Banken und Finanzinstitute operationalisiert und koordiniert werden könnte. Diese Art der Zusammenarbeit dient als Modell für die zukünftigen Bemühungen der FATF, Risiken in Bezug auf Geldwäsche oder Terrorismusfinanzierung zu erkennen.

Risikoindikatoren für Terrorismusfinanzierung sollten mehreren Monitoring-Aktivitäten Rechnung tragen, wie z. B.:

Namensüberprüfung

Transaktionsmonitoring

Überprüfung von Zahlungen und

verhaltensbezogene Due Diligence in der Schulungsumgebung

Diese Anhaltspunkte sollten auch in einschlägige Data-Mining- und Mapping-Tools Eingang finden sowie als Auslöser für interne weitere Ermittlungen dienen.

Während die festgestellten Anhaltspunkte weitreichend sind und sich ständig verändern, werden sie am besten im Zusammenhang mit Hintergrundinformationen nationaler Strafverfolgungsbehörden und anderen Informationen aus öffentlichen Quellen angewandt. Ein regelbasierter Ansatz kann keine Terrorismusfinanzierungsrisiken aufdecken, aber ein risikobasierter Ansatz kann mit einem dynamischen Zwei-Wege-Dialog zwischen Finanzinstituten und öffentlichen Stellen umgesetzt werden.

Eine Verbesserung des Informationsaustauschs ist ein komplexes Thema sowohl national als auch auf multilateraler Ebene. Der vorliegende Bericht zielt auf die Feststellung praktischer nationaler Mechanismen zur Verbesserung des Informationsaustausches zu Terrorismusrisiken und Risiken der Terrorismusfinanzierung ab, in dem Maße, wie sie sich auf die festgestellten Anhaltspunkte beziehen. Abschnitt III dieses Berichts stellt nur ein kleines Stück der Arbeit dar, die die FATF zum Thema Informationsaustausch leisten will. Der vorliegende Bericht kann hoffentlich in andere Arbeitsabläufe auf internationaler Ebene einfließen.

Er ist nicht als Compliance-Monitoring-Tool für Aufsichtsbehörden gedacht. Auf nationaler Ebene sollten die zuständigen Behörden die Gelegenheit ergreifen, den Bericht selbst als Katalysator zu nutzen für die

- Zusammenarbeit mit dem Privatsektor,
- Umsetzung spezieller Feedbacks zu Verdachtsmeldungen mit Bezug zu Terrorismusfinanzierung und Unterstützung der Finanzinstitute bei der Feinabstimmung ihrer Monitoringprozesse,
- sowie zum Austausch von Hintergrundinformationen zu Terrorismus und Terrorismusfinanzierung, die zur präventiven Aufdeckung potentieller Terroristen führen könnten.

© 2016 - **nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt** 

Zur Bewertung der Effektivität des vorliegenden Berichts wird die FATF beobachten, wie die Behörden die Anhaltspunkte und die Maßnahmen verbreiten, die getroffen wurden, um die Partnerschaften mit dem Privatsektor auf der Grundlage der Nutzung der Risikoindikatoren zu verbessern.


**nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016**

## BIBLIOGRAPHIE UND QUELLEN

FATF (2015a) *Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html

FATF (2015b) *Emerging Terrorist Financing Risks*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

FATF (2015c), *Best Practices on Combating the Abuse of Non-Profit Organizations*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html

FATF (2014), *Risk of terrorist abuse in non-profit organizations*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/risk-terrorist-abuse-non-profits.html

FATF (2013a), *International Best Practices on Targeted Financial Sanctions for Terrorist Financing*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-finsanctions-tf-r6.html

FATF (2013b) *The role of Hawala and other similar service providers in money laundering and terrorist financing*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/role-hawalas-in-ml-tf.html

FATF (2013c) *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html

FATF (2011) *Organized Maritime Piracy and Related Kidnapping for Ransom*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/organisedmatitimepiracyandrelatedkidnappingforransom.html

FATF (2010) *Money laundering vulnerabilities of Free Trade Zones*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaundetingvulnerabilitiesoffreetradezones.html

FATF (2008) *Typologies report on Proliferation Financing*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html

FATF (2002) *Guidance for Financial Institutions in Detecting Terrorist Financing*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/guidanceforfinancialinstitutionsindetectingterroristfinancing.html

APG (2012) *Trade-based money laundering*, APG, Sydney, www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaunderingtypologies.html

NCA *(nd) Joint Money Laundering Intelligence Taskforce*, National Crime Agency, London www.nationalcrimeagency.gov.uldabout-us/what-we-do/economic-ctime/joint-money-laundering-intelligence-taskforce-jmlit, accessed May 2016.

© 2016 - **for restricted use only, not for publication**

UNSC (2016) *Challenges business entities face in implementing Security Council resolution 2199 (2015),* United Nations Security Council, New York, https://www.un.org/sc/suborg/en/sanctions/1267/monitoring-team/reports. See Document S/2016/213. (UN SC, 2016)

UNSC (nd) *Consolidated United Nations Security Council Sanctions List,* United Nations Security Council, New York https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

US DOS (2016) *Illustrative List of Oil Drilling and Refinery Equipment,* US Department of State, Washington, www.state.gov/e/enr/c71196.htm


**nur für den Dienstgebrauch, nicht zur Veröffentlichung bestimmt - © 2016**

www.fatf-gafi.org

Juni 2016

# Aufdeckung von Terrorismusfinanzierung *Relevante Risikoindikatoren*

**Die FATF hat die in diesem Bericht genannten Anhaltspunkte erarbeitet, um Regierungsbehörden und ausgewählte Unternehmen des Privatsektors bei der Aufdeckung und Unterbindung der Geldflüsse von Terroristen und Terrororganisationen zu unterstützen. Die FATF hat beschlossen, den vorliegenden Bericht nicht öffentlich zugänglich zu machen, um den Nutzen der Indikatoren und der sonstigen relevanten Informationen zu bewahren. Die nationalen zuständigen Behörden sind für die Weitergabe des Berichts an die entsprechenden Unternehmen des Privatsektors in ihrem Land verantwortlich. Die Empfänger des Berichts müssen die Informationen vertraulich behandeln und dürfen sie ohne vorherige Genehmigung durch ihre nationale zuständige Behörde nicht vervielfältigen, freigeben oder auf andere Weise an Dritte weitergeben.**