Bundesministerium
des Innern

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Herrn
Alexander Ulrich, MdB
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 140, 10557 Berlin
POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-11117
FAX +49 (0)30 18 681-11019
INTERNET www.bmi.bund.de

DATUM 26. April 2016

BETREFF **Schriftliche Frage Monat April 2016**
HIER Arbeitsnummer 4/111

ANLAGE - 1 -

Sehr geehrter Herr Abgeordneter,

auf die mir zur Beantwortung zugewiesene schriftliche Frage übersende ich Ihnen die beigefügte Antwort.

Mit freundlichen Grüßen
in Vertretung

Dr. Günter Krings

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 140, 10557 Berlin
VERKEHRSANBINDUNG S-Bahnhof Berlin Hauptbahnhof
Bushaltestelle Berlin Hauptbahnhof

Schriftliche Frage des Abgeordneten Alexander Ulrich
vom 19. April 2016
(Monat April 2016, Arbeits-Nr. 4/111)

Frage

Was ist der Bundesregierung darüber bekannt, über welche technischen Mittel zum Monitoring von Terrorismusfinanzierung internationale Finanzdienstleister (darunter SWIFT, Western Union, Monreygram, Ria) verfügen, um mit Hilfe einer permanenten Rasterfahndung der Finanzströme jeden verdächtigen Zahlungsverkehr herauszufiltern und die damit in Verbindung stehenden Accounts/Personen anschließend in Anwendungen zur Sozialen Netzwerkanalyse (SNA) darzustellen, und in welcher Form bzw. welchen Formaten werden solche Analysen oder Berichte durch Finanzdienstleister bei den zuständigen deutschen Strafverfolgungsbehörden oder Geheimdiensten angeliefert?

Antwort

Die EDV-gestützten Datenverarbeitungssysteme der Kredit- und Zahlungsinstitute arbeiten regelmäßig dergestalt, dass die Transaktionen des Instituts ausgerichtet an der jeweiligen Geschäfts- und Kundenstruktur mittels individuell festlegbarer Risikoparameter auf Geldwäsche, Terrorismusfinanzierung oder auf sonstige strafbarkeitsrelevante Strukturen hin untersucht werden. Dabei werden die Risikoparameter insbesondere auf Basis der institutsinternen Gefährdungsanalyse sowie national oder international erstellten Typologien über die Methoden der Geldwäsche, der Terrorismusfinanzierung oder sonstiger strafbarer Handlungen erstellt.
Durch das Monitoring werden zweifelhafte oder ungewöhnliche Transaktionen aus der Mehrzahl der nicht-relevanten Transaktionen herausgefiltert. Bei der weiteren Erkenntnisverdichtung zu den tatsächlich zweifelhaften bzw. ungewöhnlichen Transaktionen werden von den Instituten auch frei verfügbare Informationen wie z. B. Daten aus den sozialen Netzwerken genutzt.
Die Pflicht der Institute zur Implementierung solcher Monitoringsysteme basiert auf den Maßgaben des Artikels 8 Absatz 3 und 4 der 4. europäischen Geldwäsche-Richtlinie und der Empfehlung 18 des Standards der Financial Action Task Force.

Der Einsatz dieser Mittel hat dabei keinen Bezug zu einer „Rasterfahndung", da die verpflichteten Institute dadurch nicht etwa als „Hilfsorgan der Ermittlungsbehörden" fungieren, sondern die getroffenen Sicherungsmaßnahmen vielmehr dem Selbstschutz der Institute zur Minimierung von Rechts-, Reputations- oder operationellen Risiken dienen.
Die in diesem Zusammenhang im Wege der Risikoanalyse gewonnenen Informationen verbleiben in den Instituten, werden nach Ablauf der hierfür vorgesehenen Fristen gelöscht und nicht an Strafverfolgungsbehörden oder Nachrichtendienste weitergegeben. Lediglich in Fällen eines meldepflichtigen Verdachts nach § 11 Absatz 1 des Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten werden die gewonnen Erkenntnisse für die Substantiierung der Verdachtsmeldung herangezogen. Abschließend sei darauf hingewiesen, dass SWIFT kein Kredit- oder Zahlungsinstitut, sondern ein technischer Dienstleister ist.