SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Strukturen unkonventionell organisierter Kriminalität aufdecken

Zur Umsetzung von Strategien gegen grenzüberschreitende kriminelle Netzwerke

Simona Autolitano / Verena Zoppei

Immer wieder wird das traditionelle Verständnis von Organisierter Kriminalität (OK) in Frage gestellt. Das Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC), das EU-Polizeiamt Europol und auch deutsche Behörden wie Bundeskriminalamt, Bundesinnenministerium und Bundesjustizministerium betonen, dass neben hierarchischen kriminellen Vereinigungen neue Formen krimineller Netzwerke existieren, die sich mit alten überlappen. Es handelt sich um weltweit agierende Zusammenschlüsse, die eher einer Marktlogik folgen, statt sich in gewaltsame Konflikte zu verstricken. Für die Strafverfolgungsbehörden sind sie schwer zu fassen, weil sie locker und flexibel organisiert sind. Alarmierend sind vor allem ihre Fähigkeit, die legale Wirtschaft zu infiltrieren, und das enorme Maß an Geldwäsche, welches das UNODC auf zwei bis fünf Prozent des weltweiten Bruttoinlandsprodukts schätzt. Deshalb sollten nicht nur Strafverfolgungsbehörden und Politiker, sondern auch der Privatsektor besonders wachsam sein. Oft treibt nationale Strafverfolgung kriminelle Aktivitäten nur über die nächste Grenze. Um erfolgreich zu sein, sollten Gegenstrategien daher an globalen Marktdynamiken ansetzen.

In immer mehr wichtigen Strategiepapieren wird Organisierte Kriminalität als ernsthafte Bedrohung für die legale Wirtschaft bezeichnet. So hat die EU in ihrer Sicherheitsagenda 2015 und ihrer Globalen Strategie 2016 die OK als eines der schwerwiegendsten Sicherheitsprobleme gebrandmarkt. Zwar ist seit langem bekannt, dass kriminelle Netzwerke gravierende soziale, wirtschaftliche und politische Auswirkungen haben. Da diese neuen Formen der OK aber ein äußerst diffuses Erscheinungsbild aufweisen, sind Ermittlungen und Strafverfolgung kompliziert und mühsam.

Die Analyse von Ermittlungsakten, Berichten und Urteilen dreier bedeutender Verfahren gegen die OK, die deutsche Behörden in den letzten Jahren abgeschlossen haben, versprach Erkenntnisse über Stärken und Schwächen gegenwärtiger Strafverfolgungspraxis. Die Verfahren betrafen Menschenschmuggel, Cyberkriminalität und Geldwäsche. Drei Problembereiche kristallisierten sich heraus: Erstens wirken nicht-

Simona Autolitano war im Rahmen ihres Praktikums in der SWP-Forschungsgruppe Sicherheitspolitik am MORE-Projekt beteiligt.
Dr. Verena Zoppei ist Wissenschaftlerin in der SWP-Forschungsgruppe Sicherheitspolitik und Leiterin des MORE-Projekts.

hierarchische Formen vernetzter Kriminalität bei flüchtiger Betrachtung fälschlich wie das Handeln zahlreicher Einzeltäter. Zweitens hat die »Follow the money«-Strategie (also der Versuch, über Finanzströme an die Täter zu gelangen) auch Nachteile, denn bei der Geldwäschebekämpfung lassen sich Strafverfolgungsinteresse und wirtschaftliche Interessen nur schwer ausbalancieren. Drittens schließlich haben die untersuchten Fälle gezeigt, dass die Zusammenarbeit innerhalb und über die EU hinaus weiter ausgebaut werden muss, da kriminelle Netzwerke grenzübergreifend operieren.

Strukturen erkennbar machen

Oft sind Täter, die scheinbar selbständig agieren, Teil eines zusammenhängenden kriminellen Netzwerks. Deshalb ist der traditionelle Ansatz, der sich auf »Intensivtäter« konzentriert, kaum dazu geeignet, horizontale kriminelle Strukturen zu zerschlagen. Kriminelle Netzwerke sind sehr anpassungsfähig, wenn es darum geht, »Personalausfall« zu kompensieren. Aussichtsreicher ist eine Strafverfolgung, die Netzwerke aufzulösen sucht, indem sie gegen sogenannte Crime Enabler vorgeht, also diejenigen, die in einer Grauzone operieren und Verbrechen ermöglichen. Diese Methode ist allerdings kostspielig und bindet erhebliche Ressourcen.

Im Zuge des erwähnten Verfahrens wegen Menschenschmuggels wurde in großem Stil bei Banken, Steuerbehörden und Arbeitsagenturen ermittelt. Auf diese Weise wurde eine komplexe transnationale Struktur erkennbar, in der »Schmuggel-Dienstleistungen« in verschiedenen Bereichen angeboten wurden. Beteiligt war eine Anzahl Crime Enabler, die vom Menschenschmuggel profitierten. Gegen Geld hatten sie zahlreiche falsche Dokumente zur Verfügung gestellt, etwa Einladungsbriefe, Heiratsurkunden, Nachweise über Familienzusammenführungen, Ausweise, Urkunden über Universitätsabschlüsse und Sprachzertifikate.

Mit solchen Finanzermittlungen lässt sich zwar immer wieder die Existenz unrechtmäßig erworbener Vermögenswerte offenbaren. Weitaus komplizierter ist es jedoch, Taten nachzuweisen, die Einzelpersonen in der Grauzone zuvor begangen haben. Der Bundestag diskutiert zurzeit einen Gesetzentwurf der Bundesregierung zur Reform der strafrechtlichen Vermögensabschöpfung. Dem Entwurf zufolge soll es künftig möglich sein, im Zusammenhang mit Ermittlungen zur OK Vermögenswerte einzuziehen, deren rechtmäßige Herkunft nicht nachgewiesen werden kann und bei denen begründeter Verdacht besteht, dass sie illegal erworben wurden. Die Verabschiedung dieses Gesetzes wäre ein wichtiger Schritt, um Probleme bei Finanzermittlungen zu überwinden und das deutsche Recht mit Standards in Einklang zu bringen, die in vielen anderen Ländern schon gelten.

Für die Auflösung krimineller Netzwerke hat es sich als effektiv erwiesen, mehrere offensichtlich zusammengehörende Täter gemeinsam vor Gericht zu stellen. Ein gutes Beispiel dafür ist das oben genannte Verfahren gegen cyberkriminelle Netzwerke. Staatsanwaltschaften in ganz Deutschland hatten jeweils eigene Ermittlungen gegen einzelne Verdächtige wegen Computerbetrugs in die Wege geleitet. Intensive Ermittlungen brachten ans Licht, dass ein weitverzweigtes, transnational aktives cyberkriminelles Netzwerk existierte. Nachdem die Fälle zusammengelegt worden waren, stellte sich heraus, dass die Täter hochqualifizierte professionelle Hacker waren. Sie gehörten einer internationalen, gut organisierten illegalen Firma an, die gestohlene Daten an Dritte verkaufte und damit einen Schaden von mindestens 1,3 Millionen Euro verursachte. Mit Hilfe von Schadsoftware waren sie in Online-Banking-Systeme eingedrungen und hatten Daten an OK-Gruppierungen veräußert, die vornehmlich Geldwäsche betrieben. Hätten die Behörden sich damit begnügt, gegen Einzelne zu ermitteln, wären das Netzwerk, die Verbindung zu anderen OK-Gruppierungen und die Geldwäsche unentdeckt geblieben.

Zu resümieren ist also, dass sich die gemeinsame Vorgehensweise trotz hohen Zeit- und Kostenaufwands auszahlt.

Die »Follow the money«-Strategie

Zumindest in der Theorie spricht vieles dafür, dass die »Follow the money«-Strategie sinnvoll zur OK-Bekämpfung beiträgt. Die Realität aber zeigt, dass diese Strategie nicht immer effektiv ist. Früher galt die Geldwäsche als Achillesferse der OK, da das Risiko, entdeckt zu werden, groß war. Mittlerweile nutzen Geldwäscher jedoch legale Wirtschafts- und Finanzinstrumente zu ihrem Vorteil. Schränkt man deren Nutzung ein, um Missbrauch zu verhindern, kann dies gegen verbriefte wirtschaftliche Rechte und Bürgerrechte verstoßen. Berechtigte Klagen können die Folge sein.

Beim dritten ausgewählten Beispiel geht es um ein in Deutschland angesiedeltes kriminelles Netzwerk, das weltweit Geldwäsche-Dienstleistungen anbot. Mit Hilfe einer Kombination aus älteren und neueren Transaktionsmethoden konnte es lange ungestört operieren. Vor allem nutzte das Verbrechersyndikat mit dem sogenannten Cuckoo Smurfing eine ausgefeilte Methode, die auf dem informellen Geldtransfersystem Hawala beruht. Bei diesem System werden Geldbeträge nicht per Bank, sondern mit Hilfe vertrauenswürdiger Vermittler überwiesen. Täter, die als legitime Hawala-Boten fungierten, betrogen Kunden, indem sie deren legales Geld durch unrechtmäßig erworbenes ersetzten. Gleichzeitig wurde im Zielland derselbe Betrag illegalen Bargelds an den angegebenen Empfänger ausgezahlt. Das »gewaschene« Bargeld wurde dann über fiktive Rechnungen zwischen Import-Export-Unternehmen hin- und hergeschoben. Auch hier erlaubte es der Einsatz von Tarnfirmen den Kriminellen, ihre Identität zu verbergen.

Sollen Regulierungen gegen Geldwäsche alle hierzu genutzten Mechanismen einschließen, lässt es sich nicht vermeiden, dass auch grundsätzlich legale Aktivitäten beschränkt werden. Häufig muss die Politik hier einen Kompromiss zwischen Strafverfolgung und Wirtschaftsinteressen finden. Ein Paradebeispiel dafür liefert die derzeitige Debatte über die Einschränkung von Bargeldtransaktionen. Wie Europol 2015 feststellte, ist die Verwendung von Bargeld in einer bestimmten Phase des Geldwäscheprozesses fast unumgänglich, selbst wenn virtuelle Währungen oder komplexe finanzielle Manöver genutzt werden. Dennoch ist und bleibt Bargeld ein legales Zahlungsmittel. Auch im Hinblick auf informelle Vermögenstransfersysteme muss die Politik einen Mittelweg finden: Werden sie aus den Bestimmungen ausgenommen, öffnet dies dem Missbrauch Tür und Tor. Verbietet man sie aber, werden legale Transaktionen auch dort verhindert, wo es keine formalen Finanzstrukturen gibt.

Ebenso umstritten ist der Umgang mit Instrumenten, die Geheimhaltung gewährleisten, wie Treuhandgesellschaften, Tarnfirmen, Bitcoins und Bankschließfächer. Ursprünglich dienten sie dazu, die Vermögen Verfolgter zu schützen, wurden aber von Kriminellen missbraucht, die ihre Identität verschleiern wollten. Um gesetzestreue von kriminellen Firmen unterscheiden zu können, sollten in einem ersten Schritt die Eigentümer und wirtschaftlich Berechtigten von Unternehmen namentlich bekannt gemacht werden. Darüber hinaus sollten Aufsichts- und Ermittlungsbehörden bei der Auswertung gesammelter Daten unterstützt werden. Seit langem sind Datenlieferanten wie Banken und Immobilienmakler in die Geldwäscheprävention eingebunden. Sie sollten noch nachdrücklicher auf die Risiken hingewiesen werden, welche die Einschleusung illegaler Gelder in die legale Wirtschaft birgt. Auf diese Weise soll der verbreiteten Haltung *pecunia non olet* entgegengewirkt werden.

Internationale Zusammenarbeit

Angesichts der grenzüberschreitenden Natur krimineller Netzwerke, die sich auch in den drei untersuchten Verfahren offenbart hat, ist es unabdingbar, dass die Straf-

verfolgungsbehörden der EU-Mitgliedstaaten intensiver zusammenarbeiten. Die Strategie der EU gegen die OK beinhaltet verstärkte Kooperation und einheitlicheres Vorgehen auf europäischer Ebene. So hat sich die EU dafür stark gemacht, dass die Justizbehörden ihrer Mitgliedstaaten eine Reihe von Regelungen harmonisieren. Zu nennen sind hier die Beweiserhebung in Strafverfahren, die Einrichtung gemeinsamer Ermittlungsgruppen, die Vereinheitlichung von Gesetzen zur Sicherstellung oder Einziehung von Tatwerkzeugen und Erträgen aus Straftaten sowie die Gesetze zur Geldwäscheprävention. Die Umsetzung dieser Maßnahmen lässt allerdings auf sich warten. Nicht einmal auf eine gemeinsame Definition Organisierter Kriminalität dürften sich die Mitgliedstaaten in absehbarer Zeit einigen können. Weitere Hindernisse sind der beträchtliche Ermessensspielraum, der den nationalen Regierungen zugestanden wird, und die Option, Richtlinien nicht zu übernehmen. Das eröffnet Straftätern die Möglichkeit, sich den für ihre Aktivitäten vorteilhaftesten Ort auszusuchen. Die uneinheitlichen Gesetze in den EU-Mitgliedstaaten, etwa zur Erhebung digitaler Beweise, erschweren die Zusammenarbeit. Im Falle von Computerkriminalität sind digitale Beweise oft das einzige Mittel, um die wahre Identität der Hacker sowie Standorte und Verbindungen zu anderen OK-Gruppierungen aufzudecken. Wie das oben skizzierte Verfahren zur Cyberkriminalität veranschaulicht, war es alles andere als einfach, die Täter zu verurteilen, obwohl die nationalen Behörden umfangreiche Datenmengen zusammengetragen hatten. Der Grund dafür liegt in den unterschiedlichen nationalen Standards für die Zulässigkeit digitalen Beweismaterials. Da Überwachung stark umstritten ist, weil sie mit Datenschutz und Persönlichkeitsrechten kollidiert, ist ein klarer und umfassender internationaler (oder zumindest europäischer) gesetzlicher Rahmen zu digitalen Beweisen vonnöten, der sicherstellt, dass die Grundrechte gewahrt bleiben.

Wirkungsvolle Bestimmungen auf europäischer Ebene hätten auch Ausstrahlungseffekte über die EU-Grenzen hinaus. Das wird aber nicht genügen, um der Organisierten Kriminalität das Handwerk zu legen. Deshalb sollte sich die EU um weitere internationale Zusammenarbeit bemühen und zum Vorreiter für eine entschiedenere Kriminalitätsbekämpfung werden, ohne dabei Drittländern ihre eigenen Standards und Definitionen aufzuzwingen.

Locker organisiert, aber nicht weniger gefährlich

Berichte über weniger gewaltsame und nicht sehr straff organisierte kriminelle Netzwerke sollten nicht dazu verleiten, die gravierenden Folgen dieser Formen Organisierter Kriminalität zu unterschätzen. Zwar versuchen viele professionelle Straftäter heute, die Anwendung von Gewalt zu minimieren, um nicht ungewollt Aufmerksamkeit auf sich zu ziehen. Dennoch ist ihre Fähigkeit, die legale Welt zu infiltrieren, als Sicherheitsbedrohung einzustufen. Strafrechtliche Lösungen allein reichen nicht aus. Immer mehr setzt sich die Erkenntnis durch, dass die Bestimmungen im Wirtschafts- und Finanzsystem erweitert werden müssen, um den Missbrauch prinzipiell legaler Instrumente zu verhindern. Das erfordert einen politischen Willen, der stärker ist als die unterschiedlichen Interessen.

© Stiftung Wissenschaft und Politik, 2016
Alle Rechte vorbehalten

Das Aktuell gibt die Auffassung der Autorinnen wieder

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-200
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6364

(Aktualisierte und leicht gekürzte deutsche Übersetzung von SWP Comments 44/2016; Übersetzerin: Ina Goertz)

Dieses SWP-Aktuell entstand im Rahmen des MORE-Projekts (Modelling and Mapping the Risk of Serious and Organised Crime Infiltration in Legitimate Businesses across European Territories and Sectors). Siehe www.transcrime.it/more/.