



## Strategie Kriminalitätsbekämpfung 2020-2023

### 1. Grundlagen

Mit der Strategie zur Kriminalitätsbekämpfung 2020-2023 bestimmt das EJPD die polizeilichen Schwerpunkte für die entsprechende Legislaturperiode in seinem Zuständigkeitsbereich, namentlich für das Bundesamt für Polizei fedpol als Polizeibehörde des Bundes. Sie ersetzt die Kriminalstrategische Priorisierung 2016–2019<sup>1</sup>, die der Bundesrat mit Informationsnotiz des EJPD vom 27. November 2015 am 4. Dezember 2015 zur Kenntnis genommen hatte.

Ausgehend von der aktuellen Sicherheits- und Polizeilage basiert die Strategie des EJPD auf den sicherheitspolitischen Zielen des Bundesrates und legt allgemeine wie auch deliktsspezifische Aufgabenschwerpunkte der polizeilichen Kriminalitätsbekämpfung des EJPD fest.

Mit Beschluss vom 22. Mai 2019 hat der Bundesrat in seiner Legislaturplanung 2019-2023 folgende sicherheitspolitischen Ziele formuliert:

- Die Schweiz beugt Gewalt, Kriminalität und Terrorismus vor und bekämpft sie wirksam (Ziel 14).
- Die Schweiz kennt die Bedrohungen ihrer Sicherheit und verfügt über die notwendigen Instrumente, um diesen wirksam entgegenzutreten (Ziel 15).

Wie die Erfahrungen der letzten Jahre – v.a. in der Terrorismusbekämpfung – gezeigt haben, stützt sich eine effiziente polizeiliche Kriminalitätsbekämpfung auf folgende drei Säulen:

- Prävention
- Kooperation
- Repression

Diese drei Säulen der polizeilichen Kriminalitätsbekämpfung gelten allgemein und deliktsübergreifend; sie beinhalten jedoch in den einzelnen Aufgabenschwerpunkten jeweils unterschiedliche prioritäre Handlungsfelder. Insgesamt bedingt dieses 3-Säulen-Modell eine umfassende Betrachtungsweise der Kriminalitätsbekämpfung unter Einbezug aller relevanten Partner und Stakeholder.

Die vorliegende Strategie des EJPD ist deshalb mit dem Nachrichtendienst des Bundes (NDB), der Eidgenössischen Zollverwaltung (EZV), dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA), dem Staatssekretariat für internationale Finanzfragen (SIF), der Eidgenössischen Finanzmarktaufsicht (FINMA) und dem Vorstand der Kantonalen Konferenz der Polizeikommandanten (KKPKS) konsolidiert.

Sie ist überdies mit national bedeutenden, konnexen Strategien abgestimmt, so mit derjenigen der Bundesanwaltschaft (BA), der nationalen Strategie zum Schutz der

---

<sup>1</sup> <https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2015/2015-12-043.html>

Schweiz vor Cyberrisiken für die Jahre 2018-2022 (NCS 2.0)<sup>2</sup> sowie der Strategie der Schweiz zur Terrorismusbekämpfung vom 18. September 2015<sup>3</sup>.

Dieses Vorgehen gewährleistet die Kohärenz der Strategien von fedpol und BA als Strafverfolgungsorgane des Bundes mit ihren wichtigsten Partnerbehörden.

## 2. Aufgabenschwerpunkte

### 2.1 Allgemein

Kriminalitätsbekämpfung in einer digitalen und globalisierten Welt stellt die Strafverfolgungsbehörden vor besondere Herausforderungen. Die kriminelle Welt nutzt die technologischen Möglichkeiten (z.B. Big Data, Internet der Dinge, Artificial Intelligence) und setzt sie für die Erreichung ihrer kriminellen Ziele ein. Digitale Kriminalität (Cybercrime) ist kein neuer Tatbestand, keine neue Deliktsform. Vielmehr werden moderne Technologien wie Internetdienste, soziale Medien und Verschlüsselung von den Kriminellen als Mittel zur Ausübung von «altbekannten» Straftaten eingesetzt, insbesondere von Vermögensdelikten.

Polizeiarbeit bedeutet im Wesentlichen Informationsbearbeitung. Herausforderungen stellen sich für die Polizei von der Gewinnung von Informationen, über ihre Auswertung und Analyse, bis hin zum Austausch mit ihren Partnern. Die Flut an Daten und Informationen, die Beliebigkeit von Tatorten, Tatmitteln und -objekten bringen klassische Ermittlungsmethoden und polizeiliche Ressourcen an ihre Grenzen. Grundsätze in der Kriminalitätsbekämpfung wie Territorialität, Sachzuständigkeit, Datenherrschaft und hoheitliches Handeln müssen unter diesen Vorzeichen für einen weiterhin adäquaten Rechtsgüterschutz neu betrachtet werden.

Diese Herausforderungen für die Polizei sind grundsätzlicher Natur. Sie gelten in jedem Deliktsfeld gleichermassen und stellen sich – unabhängig von der Strafverfolgungskompetenz – für jede nationale wie auch internationale Polizeibehörde, wenn auch in unterschiedlicher Ausprägung.

Die Polizeiwelt im In- und Ausland hat auf diese Herausforderungen reagiert. Die Antwort der Polizei auf diese Herausforderungen lässt sich in folgenden drei Leitsätzen beschreiben, welche international in unterschiedlicher Form und Intensität konkretisiert werden:

- *analysebasierte Steuerung der Polizeikräfte - Criminal Intelligence led policing*

Die Polizei erhält nicht zu wenig, sondern zu viel Informationen. Mit dem Grundsatz von *Criminal Intelligence led policing* ist der Fokus auf die zielgerichtete Triagierung, Auswertung und Analyse der Informationen zu setzen. Es soll erreicht werden, dass die richtigen Informationen zeitgerecht zu den richtigen Stellen gelangen und weiterbearbeitet werden. Dafür ist auch erforderlich, dass als Entscheidungsgrundlage für die Anordnung polizeilicher Massnahmen gesamtheitliche polizeiliche Lagebilder bestehen. Die begrenzten Ressourcen für die Beschaffung und Analyse der Informationen in den schwersten Deliktsfeldern sollen dort eingesetzt werden, wo sich am meisten Erkenntnisse für konkrete und effektive polizeiliche (präventive, kooperative oder repressive) Massnahmen gewinnen lassen.

- *Einbezug Privater - public private partnership*

---

<sup>2</sup> [https://www.isb.admin.ch/isb/de/home/themen/cyber\\_risiken\\_ncs/ncs\\_strategie.html](https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/ncs_strategie.html)

<sup>3</sup> <https://www.admin.ch/opc/de/federal-gazette/2015/7487.pdf>

Organisierte Kriminalität, Terrorismus, Korruption, Geldwäscherei, Menschenhandel und Menschenschmuggel sind Delikte, die mehrheitlich im Verborgenen stattfinden. Opfer vermeiden es, mit der Polizei zusammenzuarbeiten. Sei es aus Angst vor Repressalien und Retorsionen (z.B. im Falle von Menschenschmuggel, -handel) oder vor Reputationsschaden (z.B. bei Spyware, Phishing), sei es, weil auch sie vom Delikt profitieren (z.B. bei Geldwäscherei durch Money-mules). Die Herausforderung der Polizei ist es, diese Delikte dennoch zu erkennen.

Die aktuelle Zusammenarbeit mit privaten und polizeifremden Partnern (Unternehmen, NGO, Universitäten u.a.) hat sich bei der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung, Menschenhandel und gegen gewaltextremistische Radikalisierung bereits bewährt. Der Einbezug privater und polizeifremder Partner zwecks Kriminalitätsbekämpfung soll verstärkt werden, v.a. dort, wo die Partner ein eigenes Interesse an der Prävention haben (wie z.B. die Finanzintermediäre aus Reputationsgründen).

- *Erkennen kriminell erworbener Geldflüsse - Follow the money*

Bei gewinnorientierter Kriminalität ergibt es Sinn, zum Erkennen kriminogener Netzwerke vermehrt beim Geld anzusetzen. Die fortgeschrittene Digitalisierung der Finanzströme ermöglicht es, den Weg des Geldes zu verfolgen und damit die Täter und ihre Netzwerke zu erkennen. Nicht immer kann die Täterschaft zur Verantwortung gezogen werden, z.B. mangels Rechtshilfe, aussagebereiter Zeugen oder anderer gerichtlich verwertbarer Beweismittel. Insbesondere in diesen Fällen soll der Täterschaft zumindest soweit wie möglich der Weg zum inkriminierten Geld verwehrt werden.

Alle polizeilichen Ziele und Massnahmen setzen als Grundlage eine polizeiliche Lagebeurteilung in der Schweiz voraus. Diese ist mittels strategischer Analysen in der Schweiz laufend aufzuklären. Aufgrund der Polizeilage Schweiz setzt das EJPD seine polizeilichen Aufgabenschwerpunkte fest und definiert die Ziele. Zum Erreichen dieser Ziele werden Massnahmen in den Säulen Prävention/Kooperation/Repression aufgeführt. Diese Massnahmen orientieren sich an den genannten Leitsätzen in den jeweiligen Deliktsbereichen. Bei einer wesentlichen Änderung der Kriminalitätsslage sind die Massnahmen ebenfalls anzupassen.

Wie oben dargelegt, ist Cyberkriminalität kein eigener Deliktsbereich und wird deshalb nachfolgend nicht separat aufgeführt. Die Bekämpfung digitaler Kriminalität gilt als eine übergreifende Aufgabe mit besonderen Herausforderungen in jedem Deliktsbereich.

## **2.2 Organisierte Kriminalität (OK)**

### **Lage:**

#### *Kriminelle Organisationen mafiöser Art italienischer Herkunft*

Von den italienischen Mafien geht aktuell in der Schweiz eine erhebliche Gefährdung aus. Ihre Mitglieder sind in der Schweiz zum Teil schon über mehrere Generationen hinweg aktiv und das in verschiedenen Deliktbereichen. Mit dieser langjährigen und grossen Präsenz, familiären Bindungen in der Schweiz sowie der sprachlichen Nähe lassen sich die mögliche Infiltration in die Verwaltung und die Wirtschaft erklären, die bislang bei keinen anderen kriminellen Organisationen in diesem Ausmass beobachtet werden konnte. Die italienischen Mafien stellen damit eine Gefährdung der rechtsstaatlichen Institutionen und des Schweizer Finanzplatzes dar.

### *Kriminelle Gruppierungen südosteuropäischer Herkunft*

Es gibt in der Schweiz eine grosse Diaspora aus dem Balkan. Damit hat auch die Gefährdung durch kriminelle Gruppierungen südosteuropäischer Herkunft in der Schweiz in den letzten zwanzig Jahren zugenommen. Diese Gruppierungen dominieren bestimmte Kriminalitätsformen wie den Drogen- und Menschenhandel. Sie zeichnen sich durch eine grosse Gewaltbereitschaft und einen hohen Organisationsgrad aus.

### *Kriminelle Gruppierungen aus den GUS-Staaten*

Die besondere Gefährdung durch kriminelle Gruppierungen aus den GUS-Staaten für die Schweiz rührt u.a. daher, dass deren Mitglieder über ein hohes wirtschaftliches Gewicht und teilweise politischen Rückhalt in ihren Herkunftsstaaten verfügen. Sie sind in Deliktsbereichen aktiv, für welche die Schweiz aufgrund des attraktiven Finanzplatzes besonders anfällig ist (z.B. Geldwäscherei) bzw. welche die Funktion des Staates und seiner Behörden unmittelbar tangieren (z.B. Korruption). Aus der grossen Bedeutung des Schweizer Finanzplatzes für die Machtelite der GUS-Staaten ergeben sich auch aussenpolitische Risiken.

#### **Ziele Deliktsfeld «OK»:**

- Die Schweiz ist für OK unattraktiv – sei es zur Bildung von Strukturen, aber auch als Rückzugsort und Basis, um Gewinne aus kriminellen Aktivitäten zu verstecken oder zu waschen.
- Die Behörden von Bund und Kantonen sind über die Präsenz und die Aktivitäten krimineller Gruppierungen und Organisationen in der Schweiz oder mit Bezügen zur Schweiz laufend informiert (Lageverfolgung), sich der Risiken dieser Präsenz bewusst und entsprechend sensibilisiert.
- Der Auf-, Ausbau und die Tätigkeiten der OK ist verhindert oder erschwert, die Infiltration von Behörden, Wirtschaft und Zivilgesellschaft abgewendet oder minimiert. Die Öffentlichkeit ist über das Phänomen informiert.

#### **Massnahmen:**

##### *Prävention*

- Mit Präventions-, Weiterbildungs- und Sensibilisierungsprogrammen werden Behörden von Bund und Kantonen sowie private Risikogruppen aufgeklärt und instruiert.
- Exponenten der OK werden wegen Gefährdung der inneren oder äusseren Sicherheit von der Schweiz ferngehalten oder ausgewiesen und in den polizeilichen Informationssystemen ausgeschrieben.

##### *Kooperation*

- Die bilaterale Polizeizusammenarbeit mit den relevanten Staaten wird zwecks Beurteilung der Lage und Ermittlungsansätze gestärkt.
- Die operative und strategische Zusammenarbeit in multilateralen und europäischen Gremien, Agenturen und Plattformen wie z.B. Europol wird gestärkt, laufend analysiert und weiterentwickelt. Die Mitwirkung in neuen Zusammenarbeitsprojekten wird unter Berücksichtigung der aktuellen Kriminalitätsslage laufend angepasst.

- Die interdisziplinäre Zusammenarbeit zwischen den Akteuren der Strafverfolgung und anderen Behörden von Bund und Kantonen wird enger koordiniert und konzentriert (Konzept Countering Organised Crime COC<sup>4</sup>).

#### *Repression*

- Geldwäschereiverdachtsmeldungen im Umfeld von OK werden prioritär behandelt.
- Bei entsprechender Verdachtslage werden konsequent polizeiliche Ermittlungsverfahren eröffnet oder Strafanzeigen eingereicht.
- Ermittlungsverfahren bei OK zielen nebst der Strafverfolgung auch auf den Einzug von Vermögenswerten ab.
- Anklagebehörden werden proaktiv auf Instrumente hingewiesen, welche kooperationswilligen Mitgliedern der OK den Ausstieg erleichtern (Zeugenschutzprogramm, Integration).

### 2.3 Terrorismus

#### **Lage:**

Die Terrorbedrohung in der Schweiz ist nach wie vor erhöht. Sie wird weiterhin hauptsächlich durch den «Islamischen Staat», seine Unterstützer und Sympathisanten, geprägt. Auch die Bedrohung durch die «Al-Qaida» besteht fort. Die Schweiz gehört zur westlichen, von Dschihadisten als islamfeindlich eingestuften Welt und stellt damit aus deren Sicht ein legitimes Ziel für Terroranschläge dar. Primär stehen jedoch andere Länder als Ziel für Terrorattacken im Fokus. Anschläge mit geringem logistischem Aufwand, ausgeführt von Einzeltätern oder Kleingruppen, stellen aktuell für die Schweiz die wahrscheinlichste Bedrohung dar. Als Täter kommen in der Schweiz hauptsächlich radikalisierte Personen in Frage, die von der dschihadistischen Propaganda und durch Kontakte im persönlichen Umfeld inspiriert worden sind, aber nicht zwingend in direktem Kontakt mit einer dschihadistischen Gruppierung oder Organisation stehen. Ebenso dürften Rückkehrende aus Kriegsgebieten potenziell als gefährlich einzustufen sein. Die von islamistischen Extremisten ausgehende Terrorgefahr spielt aktuell die bedeutendste Rolle in der Schweiz.

Terroristische Anschläge wie in Christchurch, München, El Paso, Dayton und Halle zeigen jedoch das Nachahmer- und Gewaltpotenzial von links- und vor allem auch rechtsextremistischen Gruppierungen auf.

**Ziele Deliktsfeld «Terrorismus»:** (= Strategie der Schweiz zur Terrorismusbekämpfung vom 18.09.2015<sup>5</sup>)

- Die Schweiz verhindert Terrorismus auf ihrem Territorium.
- Der Export und die Unterstützung von Terrorismus vom Schweizer Territorium aus ist verhindert.
- Die Schweiz lässt sich von Terroristen nicht erpressen.
- Die Schweiz ist darauf vorbereitet, Terroranschläge bewältigen zu können.

<sup>4</sup> *Countering Organised Crime (COC)*: Im Bereich des Terrorismus hat sich mit TETRA die Methode der behördenübergreifenden Zusammenarbeit mit holistischem Ansatz der Kriminalitätsbekämpfung (Prävention/ Kooperation/Repression) bewährt (vgl. hinten). Diese Methode wird auch bei OK eingeführt.

<sup>5</sup> <https://www.admin.ch/opc/de/federal-gazette/2015/7487.pdf>

➤ Die Schweiz ist eine verlässliche, dem Völkerrecht verpflichtete und umsichtige Akteurin auf internationaler Ebene.

### **Massnahmen:**

#### *Allgemein*

- Die Strategie der Schweiz zur Terrorismusbekämpfung wird evaluiert.

#### *Prävention*

- Die Massnahmen des Nationalen Aktionsplans gegen Radikalisierung und gewalttätigen Extremismus<sup>6</sup> werden weiter umgesetzt.
- Terroristische Gefährder sind in einem Bedrohungsmanagement erfasst und präventiv-polizeiliche Massnahmen werden gezielt eingesetzt.
- Von Terrorismus besonders gefährdete Einzelpersonen oder Personengruppen (z. B. Magistratspersonen, völkerrechtlich geschützte Personen, religiöse Minderheiten) sowie Einrichtungen und Objekte werden geschützt.
- Der Zugang zu Stoffen, welche als Sprengstoffe für terroristische Anschläge genutzt werden können (Vorläuferstoffe), ist geregelt.

#### *Kooperation*

- Die interdisziplinäre Zusammenarbeit zwischen den Akteuren der Strafverfolgung von Bund und Kantonen sowie anderen Behörden des Bundes und der Kantone erfolgt koordiniert und konzertiert (Konzept TETRA<sup>7</sup>).
- Die operative und strategische Zusammenarbeit in multilateralen und europäischen Informationssystemen, Gremien, Agenturen und Plattformen (z.B. SIS<sup>8</sup>, API<sup>9</sup>, PNR<sup>10</sup>, Plattformen von INTERPOL, Europol und der Police Working Group on Terrorism PWGT) wird fortgesetzt, laufend analysiert und weiterentwickelt.
- Die Möglichkeiten der Ausschreibungen in den polizeilichen Informationssystemen, namentlich SIS, werden konsequent genutzt.
- Die Zusammenarbeit mit den Finanzintermediären und mit NGO's wird vertieft, um Terrorismusfinanzierung besser zu erkennen und zu verhindern.
- Die bestehenden Krisenmechanismen zur Bewältigung von terroristischen Anschlägen und deren Auswirkungen sind weiterentwickelt, harmonisiert und konsolidiert (z. B. Polizei, Armee, Bevölkerungsschutz, Schutz- und Rettungswesen).

#### *Repression*

- Bei Hinweisen auf Terroraktivitäten wird konsequent polizeilich ermittelt.
- Verdachtsmeldungen wegen Terrorismusfinanzierung werden prioritär bearbeitet.
- Die internationale Zusammenarbeit (insbesondere zwecks Beweisbeschaffung und -verwertung) wird gefördert.

---

<sup>6</sup> <https://www.svs.admin.ch/de/praevention-radikalisierung/Praevention-nap.html>

<sup>7</sup> <https://www.fedpol.admin.ch/fedpol/de/home/terrorismus/terrorismus-aktuelle-lage/schweiz-ist-aktiv.html>

<sup>8</sup> Schenger Informationssystem

<sup>9</sup> Advance Passenger Record

<sup>10</sup> Passenger Name Record



- Ermittlungsdaten werden konsequent analysiert, um Zusammenhänge und Netzwerke zu erkennen.

## 2.4 Übrige transnationale Kriminalität

In den unter 2.2 und 2.3 genannten Deliktsfeldern liegt die Strafverfolgung zum wesentlichen Teil in der Kompetenz der Bundesbehörden. Bei Geldwäscherei und Korruption<sup>11</sup> ist der Bund nur unter bestimmten Voraussetzungen zuständig. Weitere Kriminalitätsbereiche wie Menschenmuggel, Menschenhandel und Vermögensdelikte sind hauptsächlich in der Strafverfolgungskompetenz der Kantone.

Die genannten Delikte sind – wie unter 2.1 ausgeführt – oft schwierig zu erkennen, weisen regelmässig einen Auslandbezug auf und betreffen oft mehrere Kantone (insbesondere bei digital begangenen Vermögensdelikten).

fedpol nimmt bereits seit Jahren in verschiedenen Deliktsbereichen die Rolle als nationale Zentralstelle zur Bekämpfung der organisierten und international tätigen Kriminalität wahr (z.B. Betäubungsmittel, Hooliganismus u.a.). Insbesondere im Menschenhandel/Menschenmuggel fungiert fedpol als Koordinations- und Kompetenzzentrum, erarbeitet Strategien, Massnahmen und Instrumenten, erstellt Analysen, vermittelt Know-how, vernetzt und unterstützt die kantonalen Sicherheits- und andere Partnerbehörden und NGO. Diese Rolle gilt es auch in weiteren Deliktsfeldern transnationaler Kriminalität in kantonaler Strafverfolgungskompetenz zu etablieren bzw. zu konsolidieren.

Das von den Kantonspolizeien und fedpol gemeinsam betriebene «Netzwerk Ermittlungsunterstützung digitale Kriminalität NEDIK» ist ein wichtiges Beispiel dafür. fedpol hat innerhalb NEDIK die Rolle der nationalen Zentralstelle und des nationalen Kompetenz- und Koordinationszentrums NC3. Gerade bei der Bekämpfung der digitalen Kriminalität sind Ausbildung, Bündelung von Expertenwissen, Kooperation sowie Informations- und Erfahrungsaustausch Schlüsselfaktoren für den Erfolg.

### **Lage:**

#### *Korruption und Geldwäscherei*

Internationale Organisationen überprüfen die Massnahmen der Schweiz zur Prävention von Korruption regelmässig und stellen der Schweiz grundsätzlich ein gutes Zeugnis aus. Sie weisen aber weiterhin auf die Notwendigkeit der Stärkung des Präventions- und Bekämpfungsdispositivs hin.

Die Meldungen an die Meldestelle für Geldwäscherei und Terrorismusfinanzierung (MROS) bei fedpol und die Strafverfahren der BA betreffen zunehmend Geldwäscherei mit der Vortat Korruption. Die gestiegenen Zahlen zeigen das erhebliche Geldwäschereirisiko, welches Korruption für den Finanzplatz Schweiz darstellt.<sup>12</sup>

Ausserhalb des kontrollierten Finanzsystems ist Korruption nur schwer zu erkennen, handelt es sich doch dabei um ein sogenanntes «opferloses» Delikt. «Opfer» sind der

<sup>11</sup> Gemäss Artikel 24 Abs. 1 Strafprozessordnung (StPO) wenn die Straftaten:

- a. zu einem wesentlichen Teil im Ausland begangen worden sind;
- b. in mehreren Kantonen begangen worden sind und dabei kein eindeutiger Schwerpunkt in einem Kanton besteht.

Die Strafverfolgung der sogenannten Privatbestechung (Art. 322<sup>octies</sup>-322<sup>decies</sup> StGB) ist in der Kompetenz der Kantone.

<sup>12</sup> <https://www.fedpol.admin.ch/fedpol/de/home/publiservice/publikationen/berichte/geldwaescherei.html>

Rechtsstaat und das Vertrauen in unsere Institutionen. Lediglich dort, wo Strafverfolgungsbehörden bei einem Anfangsverdacht von sich aus aktiv werden, ist mit Anzeigen und Verurteilungen zu rechnen.

#### *Menschenhandel und Menschenschmuggel*

Die Täternetzwerke sind über die ganze Schweiz zerstreut und es gilt, die im Hintergrund tätigen Personen zu identifizieren und strafrechtlich zu verfolgen. Hier sind neue Ansätze zu intensivieren, wie zum Beispiel nicht nur über die Opfer die Hintermänner zu ermitteln, sondern auch über die Geldflüsse (follow the money).

#### *Digitale Vermögensdelikte*

Der grösste Anteil der digital begangenen Delikte betrifft strafbare Handlungen gegen das Vermögen, sog. Cyber-Wirtschaftsdelikte. Darunter fallen mehrheitlich Cyber-Betrugsdelikte, wie falsche Immobilienanzeigen oder Betrug auf Anzeigenplattformen. Den zweitgrössten Anteil nehmen Meldungen zu Verbrechen und Vergehen gegen die Freiheit ein. Darunter fallen beispielsweise Drohungen in sozialen Medien und pädokriminelle Delikte.

#### **Ziele Deliktsfeld «Übrige transnationale Kriminalität»:**

- Den kantonalen Partnerbehörden steht für einzelne Phänomene transnationaler Kriminalität (wie digitale Vermögensdelikte, Menschenhandel, Menschenschmuggel, Korruption und Geldwäscherei) ein polizeiliches Lagebild zur Verfügung.
- Die Kantone kennen die internationalen Entwicklungen und den polizeilichen Handlungsbedarf in den Bereichen Prävention/Kooperation/Repression.
- Sie sind über wirksame Bekämpfungsmassnahmen orientiert und kennen ihre strategischen, taktischen und operativen Partner im In- und Ausland.
- Die Strafverfolgungsbehörden des Bundes führen erste Ermittlungshandlungen durch, wenn Bundesgerichtsbarkeit gegeben ist oder wenn die Zuständigkeit des Bundes oder eines Kantons noch nicht feststeht und koordinieren die kantonalen Verfahren.

#### **Massnahmen:**

##### *Prävention*

- Weiterentwicklung und Durchführung von Aus- und Weiterbildungen an Instituten (z.B. Schweizerisches Polizeiinstitut) und Fachveranstaltungen.
- Mit Präventions- und Sensibilisierungsprogrammen werden Behörden von Bund und Kantonen sowie private Risikogruppen zu einzelnen Phänomenen aufgeklärt und instruiert.
- Erkennen von Trends und Methoden durch Ausbau der strategischen Analyse bei Geldwäscherei.
- Die strategische Koordinationsarbeit in allen vier Säulen der Bekämpfung von Menschenhandel (Prävention, Strafverfolgung, Opferschutz und Zusammenarbeit) wird weitergeführt und die Massnahmen des Nationalen Aktionsplan gegen Menschenhandel<sup>13</sup> werden weiter umgesetzt und weiterentwickelt (z.B. Einbezug der Finanzintermediäre «Follow the money»).

<sup>13</sup> <https://www.fedpol.admin.ch/dam/data/fedpol/aktuell/news/2017/2017-04-13/nap-2017-2020-d.pdf>



- Die Massnahmen gegen Menschenmuggel gemäss dem Vier-Filter-Modell<sup>14</sup> der Integrierten Grenzverwaltungsstrategie<sup>15</sup> werden konsequent weiterverfolgt und entwickelt.

#### *Kooperation*

- Vernetzung und Know-how-Austausch mit internationalen Expertinnen und Experten von Partnerbehörden, internationalen Polizei- und privaten Organisationen.
- Beteiligung an Plattformen von Europol für die Ermittlungszusammenarbeit - sogenannte EMPACT (European Multidisciplinary Platform against Criminal Threats) - zur Bekämpfung der organisierten Kriminalität.
- Operative Fallkoordination mit den zuständigen Partnern des In- und Auslands (vgl. NEDIK, Cyberboard<sup>16</sup> und J-CAT (Joint Cybercrime Action Taskforce) bei der Bekämpfung digitaler Kriminalität).

#### *Repression*

- Durchführung erster kriminalpolizeilicher Ermittlungen im Vorfeld eines Strafverfahrens, wenn Bundesgerichtsbarkeit gegeben ist oder wenn die Zuständigkeit des Bundes oder eines Kantons noch nicht feststeht, insbesondere im Bereich der digitalen Kriminalität.
- Koordination internationaler und interkantonalen Ermittlungen.

---

<sup>14</sup> 1. Massnahmen in Drittstaaten – 2. Massnahmen an der Aussengrenze – 3. Massnahmen im Binnenraum des Schengen-Verbundes – 4. Massnahmen im Binnenraum der Schweiz

<sup>15</sup> <https://www.sem.admin.ch/sem/de/home/themen/einreise/ibm.html>

<sup>16</sup> Im Cyberboard sind sämtliche in der Bekämpfung der Cyberkriminalität tätigen kantonalen und nationalen Strafverfolgungsbehörden als auch Vertreter der Prävention vereint.