Bern,

Wie fit sind die Kantone in der Cyber-Strafverfolgung?

Bericht des Bundesrates in Erfüllung der Postulate 22.3145, Andri Silberschmidt, 16. März 2022, und 22.3017, Sicherheitspolitische Kommission des Nationalrates, 15. Februar 2022

Inhaltsverzeichnis

Zusammenfassung

Diesen Bericht veröffentlicht der Bundesrat in Erfüllung der Postulate 22.3145 Silberschmidt «Wie fit sind die Kantone in der Cyber-Strafverfolgung?» und 22.3017 der Sicherheitspolitischen Kommission des Nationalrates «Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen». Fedpol und der Sicherheitsverbund Schweiz (SVS) haben zwei Begleitgruppen eingesetzt, eine strategische und eine fachliche, die sich aus Vertretungen der zuständigen Strafverfolgungsbehörden zusammensetzten. Da sich der Bericht hauptsächlich mit den Aktivitäten der Kantone im Bereich der Bekämpfung von Cyberkriminalität befasst, hat fedpol zwei Umfragen durchgeführt, um die relevanten Informationen zu erheben.
Der Bericht bietet einen Gesamtüberblick über die Bekämpfung der Cyberkriminalität in der Schweiz. Die Cyberkriminalität nimmt konstant zu, sowohl was die Anzahl der Delikte als auch die Schwere der verursachten Schäden anbelangt. Die überwiegende Mehrheit der Kantone hat Anpassungen vorgenommen, um dieser Zunahme der Cyberkriminalität zu begegnen. So wurden in den Kantonspolizeien spezifische Einheiten zur Bekämpfung von Cyberkriminalität aufgebaut sowie neue Ermittler-, IT-Forensiker- und Analytikerstellen geschaffen. Auch in den nächsten zehn Jahren dürften weitere Stellen geschaffen werden. Die meisten kantonalen Staatsanwaltschaften und die BA verfügen über Staatsanwältinnen und Staatsanwälte, die teilweise oder ausschliesslich auf die Bekämpfung von Cyberkriminalität spezialisiert sind. Zahlreiche Umfrageteilnehmende sind jedoch der Auffassung, dass die aktuell in der Bekämpfung der Cyberkriminalität eingesetzten Personalbestände absolut nicht ausreichend sind und keine vertiefte Bearbeitung der eingegangenen Anzeigen erlauben. Der Bundesrat empfiehlt den Kantonen daher, auf individueller Ebene eine Selbstevaluation vorzunehmen, um zu überprüfen, ob die eingesetzten Mittel der Lage im Bereich Cyberkriminalität entsprechen.

Zwei grosse Hindernisse stehen einer Verbesserung der Bekämpfung der Cyberkriminalität im Weg: zum einen das Fehlen von gesetzlichen Grundlagen, welche den automatischen Austausch von polizeilichen Informationen zwischen den Kantonen sowie mit dem Bund ermöglichen, und zum anderen das Regime der internationalen Rechtshilfe in Strafsachen. Ohne den automatischen Austausch von polizeilichen Informationen ist es sehr kompliziert, Verbindungen zwischen Verfahren herzustellen, die in verschiedenen Kantonen zu den gleichen Tätern im Gang sind. Dies führt zu einer Ressourcenverschwendung und schwächt die Erfolgschancen der Ermittlungen. Auch verhindert es die Weiterentwicklung der taktischen Kriminalanalyse zu Cyberkriminalität auf nationaler Ebene. Diese ist jedoch entscheidend, wenn es darum geht, technische Präventionsmassnahmen, Massnahmen zur Sensibilisierung der Bevölkerung oder auch kohärente Strategien zur Bekämpfung der Cyberkriminalität zu entwickeln. Ohne diesen automatischen Austausch ist es zudem kompliziert, Verfahren, welche dieselben Täter betreffen, zu konsolidieren, sei es auf kantonaler oder auf Bundesebene. Mit der Umsetzung der Motion 18.3592 Eichenberger wird diese Lücke bald geschlossen. Auch die internationale Rechtshilfe kann für Ermittlungen ein grosse Herausforderung darstellen. Ihre Grenzen (Langsamkeit, administrative Komplexität) können Cyberkriminellen zum Vorteil gereichen und deren Chancen vergrössern, der Justiz zu entwischen. Selbst wenn Ermittlungen erfolgreich sind, zeigt sich, dass zahlreiche Täter in Ländern Unterschlupf finden, mit denen die Rechtshilfe sehr kompliziert ist oder nicht funktioniert. Die Bundesverwaltung verfolgt die internationalen Entwicklungen in diesem Bereich aufmerksam und wird demnächst evaluieren, was die besten Optionen sind.

Die meisten der in diesem Bericht präsentierten Empfehlungen sind bereits in der Nationalen Cyberstrategie (NCS) zu finden, in deren Ausarbeitung die Strafverfolgungsbehörden eng eingebunden waren. Die Verbesserung der Voraussetzungen für die Bekämpfung der Cyberkriminalität kann daher mit den von der NCS – beziehungsweise deren Steuerungsausschuss – vorgesehenen Umsetzungsmechanismen sichergestellt werden.

1 Einführung

Dieser Bericht erläutert in Zusammenfassung der Postulate 22.3017 «Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen» und 22.3145 «Wie fit sind die Kantone in der Cyber-Strafverfolgung?» Herausforderungen in der schweizerischen Strafverfolgung bei Cyberdelikten und digitalisierter Kriminalität. Das folgende einleitende anonymisierte Fallbeispiel illustriert einige dieser Herausforderungen.

Ein junger Mann Mitte 20 lebt noch bei seinen Eltern. Als Digital Native chattet er auf diversen Social-Media-Plattformen mit Jugendlichen aus der ganzen Welt. Oft mit sexuellen Hintergedanken. Der Mann verstrickt die 12- bis 18-Jährigen zunächst in eine persönliche Online-Freundschaft. So bringt er sie mit der Zeit dazu, ihm anzügliche, teilweise pornografische Bilder von sich zu schicken. Er sammelt die Bilder auf seiner Festplatte. Sobald er genügend kompromittierendes Material gesammelt hat, schlägt er zu: Er fordert Geld und droht, die Bilder zu veröffentlichen. Diese Masche funktioniert in sehr vielen Fällen. Insbesondere, weil er auch einige Bilder tatsächlich öffentlich ins Internet stellt, als er keine Zahlung erhält.

Mit dem Vorgehen begeht der junge Mann eine Erpressung, und er nutzt dafür digitale Mittel. Die Tat an sich wäre auch ohne digitale Mittel möglich – aber sie machen die Tat um ein Vielfaches einfacher: Dies ist «digitalisierte Kriminalität». Straftaten, die aufgrund der Digitalisierung immer einfacher und schneller begangen werden, nehmen zu – während die Strafverfolgung immer noch an die vor der weit verbreiteten Digitalisierung festgelegten Rahmenbedingungen gebunden ist. «Digitalisierte Kriminalität» ist nicht das gleiche wie «Cybercrime». So bezeichnet sind Delikte, die überhaupt erst durch digitale Mittel möglich wurden und sich gegen Computer und Daten richten – etwa Phishing oder Hackerangriffe.

Der junge Mann streut die Bilder auf verschiedenen Plattformen. Die Community reagiert: Empörte und angewiderte Nutzer melden die verbotenen Inhalte dem Betreiber. Betreiber von Internetplattformen geben solche Meldungen mit Angabe der Benutzerkonten an das amerikanische «National Center for Missing and Exploited Children» (NCMEC) weiter. Das NCMEC triagiert die Hinweise und gibt sie den in jedem Land definierten Ansprechpartnern für die Prüfung der Strafverfolgung weiter. In der Schweiz ist das fedpol. Fedpol prüft die eingehende Meldung auf einen Tatverdacht nach Schweizer Gesetz und stellt fest: Die gemeldeten Bilder sind verbotene Pornografie, weil darauf Minderjährige zu sehen sind. Weil der Jugendliche in unserem Beispiel gleich mehrere Posts erstellte, sind es auch mehrere Meldungen, die fedpol nun an die Kantonspolizei weitergibt. Doch die Kantonspolizeien müssen ihre Fälle priorisieren, können nicht jedem Hinweis sofort nachgehen. So erpresst der junge Mann während Monaten weiter Jugendliche, bewegt sie zur Herstellung verbotener Pornografie und publiziert weiterhin verbotene Bilder, wenn die Erpressten nicht mitmachen. Weitere NCMEC-Meldungen treffen ein.

Auch diese NCMEC-Meldungen prüft fedpol und leitet sie wiederum an den für die Strafverfolgung zuständigen Kanton weiter. Fedpol erkennt das Muster und den immer gleichen Täter – hat aber keine rechtliche Grundlage, um selber Ermittlungen aufzunehmen. Der Fall liegt – wie die grosse Mehrheit der Fälle digitalisierter Kriminalität – in kantonaler Strafverfolgungskompetenz. Im Bereich der Cyberkriminalität besteht nur bei hochkomplexen und seriell begangenen Delikten (zum Beispiel Ransomware und Phishing) eine Bundeszuständigkeit. Jeder einzelne dieser Fälle erfordert Ressourcen: Ermittlerinnen und Ermittler für Befragungen, Hausdurchsuchungen und Rapporte sowie IT-Fachleute und Analysten für die Sicherung und Auswertung von Geräten, Online-Daten und IT-Protokollen für die lückenlose Beweisführung. Der Fall erhält vorläufig noch immer keine Priorität.

Doch dann macht der junge Mann etwas, das ihn durch Zufall in den Fokus der Strafverfolgung rücken lässt. Er geht ins Ausland in die Ferien und macht von dort aus weiter. Das generiert NCMEC-Meldungen, die aufgrund seines Ferienstandortes an die Strafverfolgungsbehörden seiner

Feriendestination gehen. Auch dort dauert es einige Zeit, bis die Strafverfolgung aktiv wird. Schliesslich führen die Strafverfolger am Standort, der in der NCMEC-Meldung enthalten war, eine Hausdurchsuchung durch und stellen Daten sicher. Doch der Täter ist längst zurück in der Schweiz. Ein internationales Rechtshilfeersuchen an den zuständigen Kanton macht die zuständige Kantonspolizei auf den Täter aufmerksam – und der Fall rutscht in der Prioritätenliste nach oben. Ermittler und Analysten nehmen sich des Falles an. Jetzt zeigen die kantonalen polizeilichen Vorermittlungen das Ausmass. Die kantonale Staatsanwaltschaft eröffnet nun auch in der Schweiz ein Strafverfahren gegen den jungen Mann.

Die Opfer des Fallbeispiels sind Jugendliche aus der ganzen Welt. Ihre Identifikation ist aber unerlässlich für die Beweisführung. Die internationale Polizeikooperation ist aufwändig, da alle Länder separat angefragt werden müssen und Antworten teilweise auf sich warten lassen oder ganz ausbleiben. Fedpol unterstützt die Kantonspolizei bei den zahlreichen Anfragen bei den ausländischen Behörden. Mit der Zeit kennt man Opfer aus den USA, Deutschland, Grossbritannien und Norwegen – woher die Unidentifizierten kommen, bleibt unklar.
Auch innerhalb der Schweiz generiert die Polizeizusammenarbeit viel Aufwand. Damit die Ermittlerinnen und Ermittler in Erfahrung bringen können, ob der junge Mann bereits bei anderen Kantonspolizeien in ähnlichem Kontext aufgefallen ist, müssen sie in jedem der 25 anderen Kantone separat anfragen – rechtliche und technische Hürden verhindern eine automatisierte Anfrage bei allen Kantonspolizeien.

Das Strafverfahren läuft, das kriminelle Verhalten des jungen Mannes ist gestoppt. Das Verfahren wird sich aber noch eine Weile hinziehen.

Der Fall zeigt exemplarisch, was im vorliegenden Bericht ausgeführt wird: Digitalisierte Kriminalität und Cyberdelikte bringen Herausforderungen in der territorialen Zuständigkeit, in der nationalen und internationalen Zusammenarbeit, in der zunehmenden Menge an Meldungen und Daten und im personellen und technischen Ressourcenbedarf mit sich.

1.1 Politischer Auftrag

1.1.1 Postulat 22.3017 «Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen»

Am 8. Juni 2022 hat der Nationalrat das Postulat 22.3017 der Sicherheitspolitischen Kommission des Nationalrats «Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen»[1] angenommen. Das Postulat hat folgenden Inhalt:

«Der Bundesrat wird beauftragt zu prüfen, wie sichergestellt werden kann, dass die Strafverfolgungsbehörden des Bundes sich in enger Zusammenarbeit mit den kantonalen Behörden die Technologie beschaffen, die notwendig ist, um Kryptowährungen zu analysieren und Transaktionen in Blockchain-Systemen zurückzuverfolgen, z. B. bei Lösegeldzahlungen oder bei anderen Betrugsfällen, bei denen diese Technologie eingesetzt wird. Der Bericht führt auch aus, ob dazu die Rechtsgrundlagen angepasst werden müssen und wenn ja, wie diese anzupassen sind.»

Der Bundesrat hatte am 27. April 2022 die Ablehnung des Postulates beantragt, da die Einrichtung eines zentralisierten, gemeinsamen Analysezentrums der Strafverfolgungsbehörden von Bund und Kantonen einen massiven zusätzlichen Personalbedarf zur Folge hätte und die Analyse der Geldflüsse in Kryptowährung bei den Ermittlungen der Kantone und des Bundes bereits zum Alltag gehören. Die Strafverfolgungsbehörden müssen ihre Kompetenzen in diesem Bereich weiterentwickeln. Eine

[1] 22.3017 | Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen | Geschäft | Das Schweizer Parlament

Zentralisierung würde nur dann einen Sinn ergeben, wenn das gesamte Strafverfolgungssystem in der Schweiz überdacht würde. Zudem bestehen bereits Koordinationsstellen zwischen dem Bund und den Kantonen sowie zwischen den Kantonen.

1.1.2 Postulat 22.3145 «Wie fit sind die Kantone in der Cyber-Strafverfolgung?»

Am 17. Juni 2022 hat der Nationalrat das Postulat 22.3145 Silberschmidt Andri «Wie fit sind die Kantone in der Cyber-Strafverfolgung»[2] angenommen. Das Postulat hat folgenden Inhalt:

«Der Bundesrat wird beauftragt, in Zusammenarbeit mit dem Sicherheitsverbund Schweiz (SVS) eine Auslegeordnung über den Zustand der kantonalen Cyber-Strafverfolgung zu erarbeiten. Der vollständige Bericht mit den Ergebnissen der einzelnen Kantone wird nicht veröffentlicht. Es soll ein Bericht mit Inhalten veröffentlicht werden, der weder die Polizeitaktik der einzelnen Kantonspolizeien noch die Reputation einzelner Kantone gefährdet.»

Das Postulat soll ausserdem prüfen, ob die Kantone über die notwendigen gesetzlichen Grundlagen für den automatisierten Austausch von polizeilichen Informationen verfügen, ob die Organisation der Strafverfolgungsbehörden angepasst wurde und ob Anstrengungen zur Bündelung der Ressourcen notwendig sind. Der Bundesrat hatte am 18. Mai 2022 die Annahme des Postulates beantragt. Er hält eine Bestandesaufnahme für angezeigt, welche namentlich dazu beitragen kann, das Dispositiv zur Bekämpfung der Cyberkriminalität zu ergänzen und zu optimieren.

1.2 Inhalt des Berichts

Dieser Bericht präsentiert die Bestandesaufnahme im Bereich der Bekämpfung von Cyberkriminalität in der Schweiz. Das hierzu verwendete methodische Vorgehen ist in Ziffer 1.3 erläutert. Ziffer 1.4 enthält die wichtigsten Begriffsbestimmungen.
Kapitel 2 beschreibt die in der Schweiz in die Bekämpfung von Cyberkriminalität involvierten Akteure und ihre Zuständigkeiten. Zudem werden die verfügbaren Statistiken zur Cyberkriminalität analysiert, was einen ersten Überblick über die Tendenzen in diesem Bereich gibt. Das Kapitel benennt ausserdem die grössten Herausforderungen in der Bekämpfung der Cyberkriminalität.
Kapitel 3 gibt Antwort auf die mit den Postulaten aufgeworfenen Fragen und stellt somit dar, wie sich die Strafverfolgungsbehörden angepasst haben, um gegen Cyberkriminalität vorzugehen. Betrachtet werden dabei verschiedene Bereiche, wie die Ausbildung, die Organisation, die gesetzlichen Grundlagen und die Bündelung von Ressourcen.
Kapitel 4 zeigt auf, in welchen Bereichen anhand der Umfrage Verbesserungspotenzial eruiert wurde, und legt die Basis für die in Kapitel 5 ausgeführten Bereiche, in denen Handlungsbedarf besteht. Schliesslich werden in Kapitel 6 die wichtigsten Ergebnisse des Berichts präsentiert.

1.3 Methodik

Mit der Erstellung des Berichts wurde das Eidgenössische Justiz- und Polizeidepartement (EJPD) beziehungsweise das Bundesamt für Polizei (fedpol) betraut. Im Sinne des Postulats hat fedpol während des ganzen Prozesses der Berichterstellung eng mit dem SVS zusammengearbeitet. Dank der Mitwirkung des SVS stand ein neutraler Ansprechpartner zur Verfügung und konnte gewährleistet werden, dass die Rückmeldungen der kantonalen Akteure in den Bericht einflossen.

[2] 22.3145 | Wie fit sind die Kantone in der Cyber-Strafverfolgung? | Geschäft | Das Schweizer Parlament (parlament.ch)

Die Nachverfolgung von Kryptowährungen stellt einen wichtigen Teil der Strafverfolgung bei Cyberkriminalität dar. Die damit verbundenen Schwierigkeiten sind aber nur eine von vielen Herausforderungen, mit denen die Strafverfolgung in der Cyberkriminalität befasst ist, weshalb die Beantwortung des Postulates der Sicherheitspolitischen Kommission des Nationalrates in vorliegendem Bericht erfüllt wird.
Kryptowährungen werden im Kontext dieses Berichts wie folgt definiert: Bei kryptobasierten Vermögenswerten (Virtual Assets) handelt es sich um digitale Vermögenswerte, die üblicherweise auf einer Blockchain abgebildet werden. Sie unterscheiden sich von anderen Vermögenswerten, da nur mithilfe eines kryptobasierten Zugangsverfahrens über sie verfügt werden kann, dafür aber auch nicht zwingend ein klassischer Finanzintermediär involviert sein muss. In der Regel wird für die Übertragung ein Schlüsselpaar verwendet, bestehend aus einem geheim zu haltenden privaten (Private Key) und einem öffentlichen Schlüssel (Public Key).[3] Die FINMA unterscheidet Virtual Assets in drei Kategorien, nämlich Zahlungs-, Nutzungs- und Anlage-Token, wobei auch Mischformen vorkommen können, sogenannte hybride Token. Aufgrund ihrer (zumindest teilweisen) Anonymität werden insbesondere Zahlungstoken oder eben Kryptowährungen für kriminelle Zwecke und Geldwäscherei missbraucht.[4]

1.3.1 Modalitäten des Berichts

Um den Auftrag der Postulate zu erfüllen, wurden die folgenden Elemente umgesetzt:

- Bei den relevanten Schweizer Behörden wurde eine Umfrage durchgeführt, anhand derer die Bestandesaufnahme, auf der dieser Bericht basiert, und das Benchmarking vorgenommen wurden. Fast alle Kantonspolizeien und Staatsanwaltschaften sowie 17 kantonale Gerichte haben die Umfrage vollständig ausgefüllt. Die Kapitel 3–5 dieses Berichts basieren auf den mittels Umfrage erhobenen Daten.
- Mit den aggregierten quantitativen Daten aus der Umfrage wurden verschiedene Grafiken erstellt. Diese wurden der Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS) abgegeben.

1.3.2 Projektorganisation

Das Postulat Silberschmidt verlangt explizit, dass der Bericht in Zusammenarbeit mit dem SVS erstellt wird. In der konkreten Umsetzung hat fedpol das Projekt geleitet und den SVS in jeder Etappe eng eingebunden. Der Auftrag des SVS wurde von dessen Politischer Plattform genehmigt und bestand darin, den Einbezug der relevanten kantonalen Behörden zu koordinieren sowie sicherzustellen, dass diesen alle Informationen rund um die Erarbeitung des Berichts zur Verfügung gestellt wurden. Zur Gewährleistung der Koordination wurden mehrere Arbeitsgruppen eingesetzt:

- Die strategische Begleitgruppe unter der Leitung des SVS stellte während der Erarbeitung des Berichts den Einbezug und die Information der zuständigen Akteure der Kantone in adäquater Form sicher. Sie setzte sich aus Vertretungen folgender Stellen zusammen: Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS), Schweizerische Kriminalprävention (SKP), Schweizerische Staatsanwaltschaftskonferenz (SSK), Schweizerische Vereinigung der Richterinnen und Richter (SVR-ASM), Netzwerk digitale Ermittlungsunterstützung Internetkriminalität (NEDIK), Bundesamt für Cybersicherheit (BACS).
- Die Fachgruppe unter der Leitung von fedpol bestand aus Fachleuten von Bund und Kantonen. In der Gruppe vertreten waren NEDIK, die SKP, die Bundesanwaltschaft (BA), eine kantonale Staatsanwaltschaft sowie die Vereinigung der Schweizerischen Kriminalpolizeichefs (VSKC). Die Fachgruppe hatte die Aufgabe, sicherzustellen, dass die fachliche Expertise in den Arbeiten

[3] Faktenblatt (Eidgenössische Finanzmarktaufsicht (FINMA), 2022)
[4] Am 28. Februar 2024 wurde die zweite sektorielle Risikoanalyse zu Virtual Assets der Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT) veröffentlicht (nachfolgend KGGT-Bericht): National Risk Assessment (NRA) Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets. Diesem können in den Ziff. 4.1 und 4.2 weiterführende Angaben zu «Virtual Assets» und «Virtual Asset Providers» entnommen werden.

berücksichtigt wird, und sorgte dafür, dass die für die Erstellung des Berichts notwendigen Informationen erhoben und ausgewertet wurden.

– Ausserdem hat fedpol das Centre for Security Studies der Eidgenössischen Hochschule Zürich (ETH CSS) mit einem Beratungsmandat betraut. Das CSS unterstützte fedpol namentlich mit Empfehlungen zum Bericht und Diskussionen zu den Modalitäten der grafischen Darstellung der Daten.

1.4 Begriffe

Von der Cyberkriminalität abzugrenzen, sind die Begriffe der Cybersicherheit und der Cyberdefence. Die Cybersicherheit umfasst die Gesamtheit der Massnahmen, die der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen. Die Cyberdefence umfasst die Gesamtheit der nachrichtendienstlichen und militärischen Massnahmen, die dem Schutz der für die Landesverteidigung kritischen Systeme, der Abwehr von Cyberangriffen, der Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung der zivilen Behörden dienen.

Für die Cyberkriminalität gibt es keine international anerkannte Definition. Je nach Land fallen unterschiedliche Delikte darunter. In akademischen Kreisen wurden ebenfalls mehrere Klassifizierungen vorgelegt.[5] Dieser Bericht stützt sich auf die Definition der Cyberkriminalität gemäss Strategie NEDIK 2022–2024[6]:

Cyberkriminalität: Gesamtheit aller strafbaren Handlungen und Unterlassungen im Cyber-Raum. Umfasst sowohl «digitalisierte Kriminalität» als auch «Cybercrime».

➔ **Digitalisierte Kriminalität:** Straftaten, die bisher überwiegend in der analogen Welt begangen worden sind. Aufgrund der zunehmenden Digitalisierung werden diese klassischen Delikte vermehrt mit Hilfe von Informationstechnik verübt (teilweise auch als «Cyber-Enabled Crime» bezeichnet). Typische Phänomene der digitalisierten Kriminalität sind beispielsweise die meisten Betrugsarten, die teilweise oder ganz über das Internet begangen werden: Romance Scams[7], CEO Fraud (falsche Überweisungsaufträge)[8], Kleinanzeigenbetrug[9] oder auch Online-Anlagebetrug[10]. Zur digitalisierten Kriminalität gehören ausserdem Straftaten der Online-Pädokriminalität (Teilen pädokrimineller Inhalte, Grooming[11], Live Distance Child Abuse[12]) sowie Rufschädigung. Sie werden nach den jeweiligen Artikeln des Strafgesetzbuches geahndet, die für diese strafbaren Handlungen gelten, unabhängig davon, ob sie in der realen oder in der virtuellen Welt begangen werden.

➔ **Cybercrime:** Hochtechnische Straftaten, die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten, die ebenso hochtechnische Ermittlungsarbeit auf Seiten der Strafverfolgungsbehörden erfordern (teilweise auch als «Advanced Cybercrime» oder «Hightech-

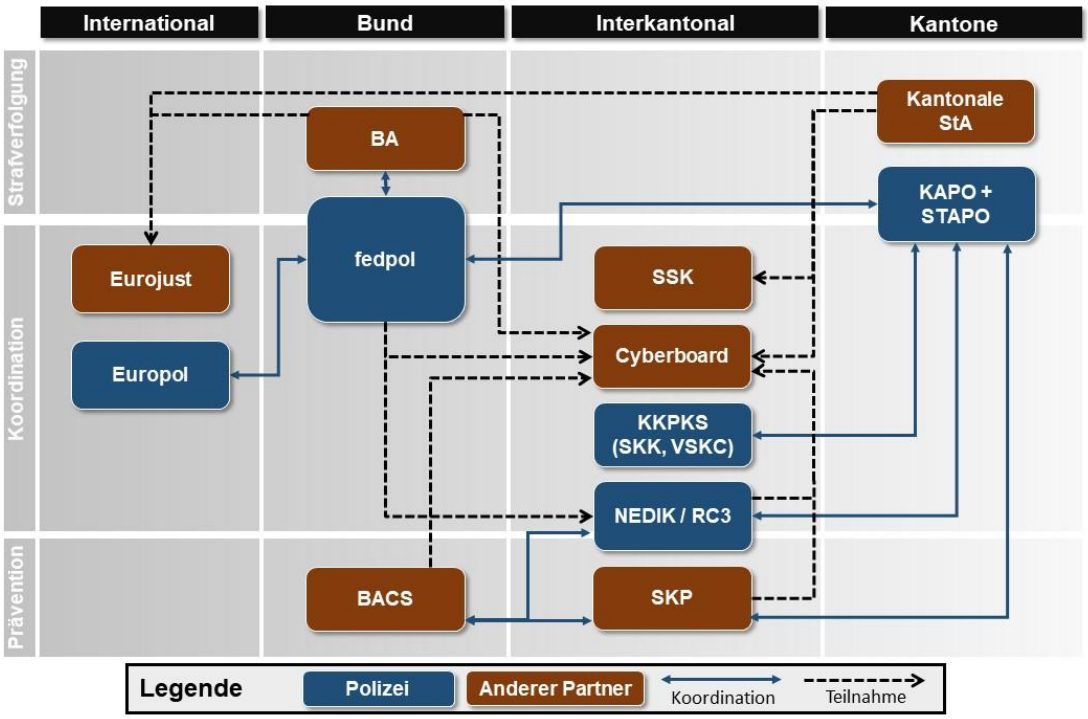
[5] (Wall, 2007)
[6] Die überwiegende Mehrheit der Schweizer Strafverfolgungsbehörden teilt diese Definition. In der Umfrage, welche im Rahmen dieses Berichts durchgeführt wurde, gaben 82 Prozent der Teilnehmenden an, auf diese Definition abzustützen. Einige gaben an, auch die Cyberphänomene aus dem RIPOL zu verwenden. Diese werden von NEDIK in Absprache mit dem Bundesamt für Statistik (BFE) definiert.
[7] Vortäuschen einer Liebes- oder (Freundes-)Beziehung, um dann Geld zu verlangen (häufig wegen eines fiktiven Härtefalls).
[8] Die Täter geben sich als Vertreter eines Unternehmen aus (behaupten, deren CEO, Mitarbeiter oder Anwalt zu sein) und veranlassen einen Geschäftspartner dieses Unternehmens oder eine dort angestellte Person, Geld auf ein ungewöhnliches Konto im Ausland zu überweisen.
[9] Zum Beispiel: Ein betrügerisches Angebot wird auf Kleinanzeige- und Onlineplattformen von der Täterschaft publiziert. Der Käufer bezahlt die Ware, diese wird jedoch nie geliefert.
[10] Jemanden dazu veranlassen, in ein bestimmtes Produkt zu investieren, obwohl dieses nicht existiert oder keinen Wert resp. keine Ertragsaussichten hat. Der Handel (Kauf/Verkauf) dieser Produkte wird dem Opfer vorgetäuscht, findet aber effektiv nicht statt.
[11] Knüpfen von sexuell motivierten Kontakten zu Kindern übers Internet, z. B. in Chatrooms oder über Social Media. Gewisse Täter streben ein Treffen im realen Leben an, um mit dem Opfer sexuelle Handlungen vorzunehmen.
[12] Teilhaben an sexuellen Handlungen mit Kindern via Webcam. Der Konsument/Anstifter meldet z. B. via Chat seine Wünsche, bezahlt den geforderten Betrag und konsumiert danach den sexuellen Missbrauch von Minderjährigen über Webcam.

Crime» bezeichnet). Dazu gehören vor allem sämtliche Formen des unbefugten Eindringens in Datenverarbeitungssysteme – oder Hacking – wie auch Ransomware[13] oder Phishing[14].

2 Cyberkriminalität in der Schweiz

In der Schweiz liegt die Zuständigkeit für die Strafverfolgung der Cyberkriminalität in erster Linie bei den Kantonen; in die Bundeszuständigkeit fallen lediglich gewisse Fälle. Aufgrund des Föderalismus sind dennoch zahlreiche Akteure in die Bekämpfung der Cyberkriminalität involviert. Diese Akteure und ihre Zuständigkeiten werden in Ziffer 2.1 beschrieben. Ziffer 2.2 präsentiert die Lage bezüglich Cyberkriminalität in der Schweiz. Die Einschätzung basiert auf den polizeilichen Kriminalstatistiken, die seit 2019 einen eigenen Teil zu Cyberkriminalität umfassen. Eine ganze Reihe von Faktoren erschwert die Bekämpfung der Cyberkriminalität. Diese Herausforderungen werden in Ziffer 2.3 dargelegt.

2.1 Zuständigkeiten und Akteure



Überblick über die wichtigsten Akteure und ihre Vernetzung

2.1.1 Kantone

2.1.1.1 Kantonspolizeien

Die Strafverfolgung der Cyberkriminalität ist gemäss Artikel 22 ff. der Strafprozessordnung (StPO; SR 312.0) grundsätzlich Aufgabe der Kantone. Diese respektive die Gemeinden verfügen über umfassende Kompetenzen zur Erkennung, Verhinderung beziehungsweise Verfolgung cyberkrimineller

[13] Ransomware ist eine Schadsoftware, die – einmal aktiviert – die Computer- oder Smartphonedaten des Opfers verschlüsselt und eine Geldforderung für die Entschlüsselung stellt. In einer Variante davon wird der Computer oder das Smartphone (manchmal einzig der Browser) infiziert und gesperrt. Sodann erscheint eine vermeintlich behördliche Mitteilung, welche die betroffene Person zu einer Bussenzahlung mittels digitaler Währung bzw. elektronischer Zahlungsmittel auffordert, damit das Informatiksystem wieder entsperrt wird.
[14] Erhältlichmachen von persönlichen und/oder vertraulichen Daten in unbefugter Weise.

Straftaten im sicherheits- wie auch im gerichtspolizeilichen Bereich. Dabei können die Kantonsregierungen Deliktsschwerpunkte setzen, nach denen sich die polizeiliche Tätigkeit richtet. Gestützt auf die kantonalen Polizeigesetze trifft die Polizei Massnahmen zur Verhütung strafbarer Handlungen. Zudem sind die Kantonspolizeien (und gewisse Stadtpolizeien, die über eine Kriminalpolizei verfügen) mit der Führung der Ermittlungen beauftragt, die aufgrund ihrer eigenen Feststellungen oder nach einer Anzeige eingeleitet werden. Diese Feststellungen können auf unterschiedlichen Mitteln basieren, während die Anzeigen von Privatpersonen stammen. Darüber hinaus bearbeiten die Kantonspolizeien auch die Berichte, die sie von fedpol erhalten, namentlich betreffend Pädokriminalität oder Vorermittlungen. Bei Fällen, welche die Kantons- oder die Landesgrenzen überschreiten, werden sie von NEDIK und fedpol unterstützt.

2.1.1.2 Kantonale Staatsanwaltschaften

Die kantonalen Staatsanwaltschaften behandeln die meisten Cyberkriminalitätsfälle, mit Ausnahme jener, die nach StPO in die Zuständigkeit der BA fallen (Art. 22 ff. StPO). In der überwiegenden Mehrheit der Cyberkriminalitätsfälle sind demnach die Staatsanwaltschaften für die Strafuntersuchung zuständig, die entweder zu einer Anklageerhebung oder einem Strafbefehl, einer Einstellungsverfügung oder einer Nichtanhandnahmeverfügung führt.
Um die internationale Koordination zu erleichtern, werden zwei Personen als Verbindungsstaatsanwälte für die Schweiz zu Eurojust beziehungsweise in das European Judicial Cybercrime Network (EJCN) entsendet.[15]

2.1.2 Interkantonale Ebene

2.1.2.1 Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz

Die KKPKS bezweckt die Förderung der Zusammenarbeit sowie des Meinungs- und Erfahrungsaustausches zwischen den schweizerischen Polizeikorps und hat im Rahmen der operativen Umsetzung der vorgegebenen politischen Ziele den Lead in allen wesentlichen Polizeifragen. Die KKPKS verfügt über mehrere Arbeitsgruppen, die sich mit Cyberkriminalität befassen: die Arbeitsgruppe Cyberausbildung, die Schweizerische Kriminalkommission (SKK)[16] und die Vereinigung der Schweizerischen Kriminalpolizeichefs (VSKC).

2.1.2.2 Netzwerk digitale Ermittlungsunterstützung Internetkriminalität

NEDIK wurde 2018 von der KKPKS gegründet. Mit diesem Netzwerk sollen die Spezialistenressourcen gebündelt werden, um die digitale Kriminalität koordiniert und effizient zu bekämpfen und den Austausch von Best Practices sicherzustellen. NEDIK besteht aus einem strategischen Gremium, das Vertreterinnen und Vertreter der Polizeikonkordate und von fedpol vereinigt, sowie einem operativen Gremium, in dem Vertretungen aller Kantone und von fedpol im Zweimonatsrhythmus zusammenkommen, um eine effiziente Ermittlungskoordination zu gewährleisten. Über die operative Koordination hinaus veröffentlicht NEDIK monatliche Lagebulletins zur Cyberkriminalität in der Schweiz und seit 2022 Bulletins zum Phänomen Online-Anlagebetrug.[17] Innerhalb weniger Jahre hat sich NEDIK als der zentrale Akteur in der Koordination der Bekämpfung der Cyberkriminalität in der Schweiz etabliert.

[15] Die Schweiz arbeitet seit 2011 auf der Grundlage eines Abkommens zur Zusammenarbeit in Strafsachen mit der EU-Agentur Eurojust zusammen. Seit 2015 verfügt sie über ein eigenes Verbindungsbüro in Den Haag, welches ein wichtiges Bindeglied zwischen den Strafverfolgungsbehörden der Schweiz und jenen der EU-Mitgliedstaaten und in Eurojust vertretenen Drittstaaten darstellt. Das Verbindungsbüro bietet den Schweizer Strafverfolgungsbehörden wertvolle Unterstützung in rechtlicher und operativer Hinsicht im Rahmen von Rechtshilfeersuchen der Schweiz und aus dem Ausland.
[16] Die SKK setzt sich aus Vertretungen der Kantone (vier aktive Polizeikommandantinnen und Polizeikommandanten und vier Mitglieder der VSKC) sowie einer Vertretung des Bundes (fedpol) zusammen und hat die Bearbeitung von interkantonalen kriminalpolizeilichen Fragen zum Ziel.
[17] Für weitere Informationen zu den Leistungen des NEDIK siehe Ziff. 3.6.

2.1.2.3 Schweizerische Kriminalprävention

Die SKP ist eine interkantonale Fachstelle im Bereich Prävention von Kriminalität und Kriminalitätsfurcht. Sie wird von der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) getragen und von einer ständigen Kommission der KKJPD, der sogenannten Leitungskommission der SKP (welcher fedpol angehört), betrieben. Zu den wichtigsten Aufgaben der SKP gehört die Stärkung der interkantonalen Polizeizusammenarbeit im Bereich Kriminalprävention. Eine weitere wichtige Aufgabe ist die Aufklärung der Bevölkerung über kriminelle Phänomene, Präventionsmöglichkeiten und Hilfsangebote. Die SKP engagiert sich in der Aus- und Weiterbildung von Polizeiangehörigen im Bereich Kriminalprävention und arbeitet hierzu eng mit dem Schweizerischen Polizei-Institut (SPI) zusammen. Über diese Aufgaben trägt die SKP regelmässig zu den Massnahmen der Polizei in Sachen Prävention von Cyberkriminalität bei. Die SKP vertritt die Kantone in Fragen der Kriminalprävention im Sicherheitsverbund Schweiz (SVS). Sie ist Mitglied des Cyber-CASE sowie des erweiterten NEDIK-Ausschusses.

2.1.2.4 Regionales Cyberkompetenzzentrum der Westschweiz

Das 2019 auf Antrag der Konferenz der kantonalen Polizeikommandantinnen und -kommandanten der Westschweiz gegründete Westschweizer Cyberkompetenzzentrum (RC3) ist eine Koordinationsplattform, die Ressourcen und Kompetenzen im Bereich Cyberkriminalität bündelt. Das RC3 wird von den Fachleuten der Kantonspolizei Genf geleitet. Es verfügt über Kompetenzen in Bezug auf den Zugang zu digitalen Daten, die Entwicklungen im Cyberraum, die Nutzung des Internet der Dinge[18] und der Fahrzeuge sowie der Prozesse zur Auswertung und Analyse der gesammelten Informationen. Das RC3 verfügt mit PICSEL (Plateforme d'Information de la Criminalité Sérielle En Ligne) über ein computergestütztes Cyber-Intelligence-Tool, das einen Gesamtüberblick über die Cyberkriminalität in der Westschweiz bietet und die Bildung und Bewirtschaftung von Serien von Phänomen fördert.

2.1.2.5 Schweizerische Staatsanwaltschaftskonferenz

Die SSK[19] hat zum Ziel, die Zusammenarbeit der Strafverfolgungsbehörden der Kantone und des Bundes zu fördern. Sie bezweckt insbesondere den Meinungsaustausch zwischen den Strafverfolgungsbehörden der Kantone untereinander und mit denjenigen des Bundes sowie die Koordination und Durchsetzung gemeinsamer Interessen. Sie fördert eine einheitliche Praxis im Bereich des Straf- und Strafprozessrechtes. Sie nimmt namentlich Stellung zu Gesetzesvorhaben des Bundes, erlässt Resolutionen sowie Empfehlungen und nimmt Einfluss auf die Meinungsbildung in Fragen des Strafrechts und Strafprozessrechts sowie verwandter Gebiete.

2.1.2.6 Cyberboard

Die Bekämpfung der Cyberkriminalität ist eine klassische Verbundsaufgabe der Strafverfolgungsbehörden von Bund und Kantonen. Aus diesem Grund entwickelte die Bundesanwaltschaft (BA) 2018 das Konzept des Cyberboard mit dem Ziel, die Zusammenarbeit zwischen den Strafverfolgungsbehörden von Bund und Kantonen sowie die Koordination bei der gemeinsamen Bearbeitung interkantonaler Fälle zu stärken. Das Cyberboard fungiert als Plattform, die auf der Erhaltung der bestehenden Strukturen und Kompetenzen basiert; es verändert weder Zuständigkeiten, noch schafft es neue Behörden. Es umfasst eine operative Stufe, bestehend aus Staatsanwältinnen und Staatsanwälten, Polizeiangehörigen sowie einer Vertretung des BACS und der SKP[20], und eine strategische Stufe, das Cyber-STRAT.

[18] Als Internet of Things (IoT), oder zu Deutsch «Internet der Dinge», werden Gegenstände und Geräte bezeichnet, welche mit einem Netzwerk wie z. B. dem Internet verbunden sind und über dieses miteinander kommunizieren oder Informationen zur Verfügung stellen. Massnahmen zum Schutz von IOT Geräten (admin.ch)
[19] https://www.ssk-cmp.ch/de
[20] Dabei handelt es sich um das Cyber-CASE, welches die nationale Fallübersicht, den Erfahrungsaustausch unter den Kantonen/Behörden, Diskussionen zu laufenden Fällen usw. sicherstellt.

2.1.2.7 Schweizerisches Polizei-Institut

Das SPI ist eine privatrechtliche Stiftung, die im Interesse der Schweizer Polizei eine nationale, politisch breit abgestützte Ausbildungsstrategie entwickelt und diese didaktisch-methodisch umsetzt. Das SPI koordiniert Inhalte, Methoden und Didaktik und gewährleistet so die Qualität und die Unité de doctrine der Polizeiausbildung. Es garantiert – im Sinne einer ständigen qualitativen Entwicklung – eine einheitliche Grundausbildung, deren Fortsetzung in der Weiterbildung sowie die Einheitlichkeit der eidgenössischen Prüfungen. Als nationales Ausbildungszentrum organisiert das SPI die Kaderausbildung der Polizei auf den Stufen I (Unteroffiziere) und II (höhere Unteroffiziere). Zusammen mit der Hochschule Arc in Neuchâtel und der Hochschule Luzern hat es zudem den CAS (Certificate of Advanced Studies) für die Ausbildung der Offiziere (Stufe III) ins Leben gerufen[21].
Die beiden anderen Ausbildungsrichtungen sind der beruflichen Spezialisierung sowie der Ausbildung von Ausbilderinnen und Ausbildern oder Multiplikatorinnen und Multiplikatoren gewidmet. Im Bereich Cyberausbildung hat das SPI das E-Learning Cybercrime (e-CC) entwickelt, das von allen Polizeiaspirantinnen und -aspiranten in der Schweiz absolviert wird. Darüber hinaus bietet es einen Aufbaukurs an (Cyber II). Das SPI koordiniert seine Tätigkeiten eng mit der entsprechenden Arbeitsgruppe der KKPKS.

2.1.3 Bund

2.1.3.1 Bundesamt für Polizei

Im Bereich der Bekämpfung der Cyberkriminalität übernimmt fedpol nach dem Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten (ZentG; SR 360) die Zentralstellenaufgaben und stellt in diesem Rahmen unter anderem die Schnittstelle zwischen dem Ausland, fedpol und den kantonalen Polizeikorps sicher. fedpol gewährleistet den kriminalpolizeilichen Informationsaustausch mit Interpol und Europol und den Betrieb der an sieben Wochentagen rund um die Uhr erreichbaren Kontaktstelle (SPOC) gemäss der Budapest-Konvention des Europarats. fedpol entsendet einen auf Cyberkriminalität spezialisierten Polizeiattaché ins Verbindungsbüro bei Europol und betreibt die nationale Kontaktstelle für die Zusammenarbeit mit dem National Center for Missing and Exploited Children (NCMEC) der USA. fedpol entlastet die Kantone durch die Triage und die direkte Zuteilung der Fälle an den oder die betroffenen Kantone, durch den Betrieb der nationalen Datei- und Hashwertesammlung (NDHS) sowie durch die operative Koordination nationaler und interkantonaler Fallkomplexe über NEDIK. Bei all diesen Aufgaben fungiert fedpol als nationales Kompetenzzentrum für Cyberkriminalität. Zudem vertritt fedpol die Schweiz in verschiedenen internationalen Fachgruppen von Europol und Interpol und sorgt gemeinsam mit den Spezialistinnen und Spezialisten der grossen kantonalen Polizeikorps innerhalb von NEDIK für die Verbreitung des Expertenwissens und den Austausch von Best Practices. Im Rahmen der Bundeskompetenzen (siehe im Folgenden Ziff. 2.1.3.2) führt fedpol Ermittlungen zu Cyberkriminalität, entweder im Auftrag der BA oder auf eigene Initiative (polizeiliche Ermittlung). Dazu verfügt fedpol über eine Gruppe von Cyberermittlerinnen und Cyberermittler innerhalb seiner Abteilung Wirtschaftskriminalität.
fedpol angegliedert, aber aufgrund von internationalen Vorgaben davon operationell unabhängig, ist die Meldestelle für Geldwäscherei (MROS) als schweizerische Financial Intelligence Unit (FIU). Sie nimmt Verdachtsmeldungen von Finanzintermediären entgegen, analysiert diese und holt bei Bedarf weitere Informationen in der Schweiz und/oder im Ausland ein. Ergibt sich aus der Analyse ein Anfangsverdacht auf eine geldwäschereirechtliche Vortat, auf organisierte Kriminalität oder auf Terrorismusfinanzierung erstattet sie Anzeige an die zuständige Strafverfolgungsbehörde. Eine weitere zentrale Aufgabe der MROS bildet der Austausch zwischen den internationalen Geldwäschereimeldestellen. In dieser

[21] CAS pour la Conduite des engagements de police à l'échelon d'officier - Haute-Ecole Arc (he-arc.ch)

Hinsicht ist die MROS regelmässig mit der betrügerischen Verwendung von Kryptowährungen auf nationaler und internationaler Ebene konfrontiert.[22]

2.1.3.2 Bundesanwaltschaft

Die BA ist zuständig für die Ermittlung und Anklage von Straftaten im Bereich der Bundesgerichtsbarkeit, wie sie in Artikel 23 und 24 der Strafprozessordnung sowie in besonderen Bundesgesetzen aufgeführt werden. Eine fakultative Kompetenz der BA ist somit in grossen Fällen von Cyberkriminalität oder Cyber-Wirtschaftskriminalität gegeben, mit Hinweisen auf Straftaten des zweiten und des elften Titels des StGB, die zu einem wesentlichen Teil im Ausland oder aber in mehreren Kantonen begangen worden sind, ohne dass ein eindeutiger Schwerpunkt in einem Kanton besteht, wobei die aus dem Ausland agierenden Täter sich mit aussergewöhnlichen Anonymisierungstechniken schützten und besonders ausgeklügelte technische Prozesse nutzten. In der Praxis befasst sich die BA insbesondere mit Serien internationaler Fälle von Phishing, E-Banking-Malware[23] und seit Neuerem auch Ransomware. Zu letzterem Phänomen hat die BA 2022 und 2023 mehrere grosse Verfahren eröffnet.

2.1.3.3 Bundesamt für Cybersicherheit

Das BACS ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, die Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Es ist verantwortlich für die Umsetzung der Nationalen Cyberstrategie (NCS).[24] Diese beinhaltet mehrere Massnahmen spezifisch zur Bekämpfung von Cyberkriminalität.[25] Das BACS ist ausserdem ein wichtiger Partner der Strafverfolgungsbehörden, da es über hochmoderne technische Kapazitäten sowie Cybersicherheitsplattformen verfügt. BACS und NEDIK tauschen sich regelmässig zur Lage im Bereich Cyberkriminalität aus. Das BACS verfügt über eine Meldeplattform für Cybervorfälle, auf der die Bevölkerung verschiedene Phänomene der Cyberkriminalität melden kann.[26] Auf dieser Plattform kann nicht Anzeige erstattet werden, die Betroffenen haben aber die Möglichkeit, das BACS zu ermächtigen, Meldungen an die Strafverfolgungsbehörden weiterzuleiten.

2.1.3.4 Bundesamt für Justiz

Der Direktionsbereich Internationale Rechtshilfe des Bundesamts für Justiz (BJ) ist die schweizerische Zentralstelle für internationale Strafrechtszusammenarbeit. Er ist zuständig für Entscheidungen in den Bereichen Auslieferung, akzessorische Rechtshilfe, Übertragung der Strafverfolgung und stellvertretende Strafvollstreckung sowie Überstellung von verurteilten Personen; dies auch im Bereich der Cyberkriminalität.

2.2 Lage

Die Cyberkriminalität entwickelt sich von Jahr zu Jahr weiter, und Cyberangriffe nehmen im Gleichschritt mit der Digitalisierung der Gesellschaft beständig zu. Die zunehmende Vernetztheit – sei es aus beruflichen Gründen, bei der Nutzung von sozialen Netzwerken oder auch beim Online-Shopping – eröffnet Cyberkriminellen Möglichkeiten, die sie zu nutzen wissen. Sie passen ihre Strategien an, um Straftaten zu begehen.[27]

[22] Siehe dazu auch KGGT-Bericht, Ziff. 7.2.1 ff.
[23] (Bundesanwaltschaft, 2022)
[24] (Bundesrat, 2023)
[25] Es sind dies die Massnahmen M12 «Ausbau der Zusammenarbeit der Strafverfolgungsbehörden», M13 «Fallübersicht» und M14 «Ausbildung der Strafverfolgungsbehörden».
[26] BACS Report (admin.ch)
[27] (Khiralla, 2020)

Obige Feststellung gilt auch für die Schweiz. Dennoch sind für die letzten zehn bis zwölf Jahre keine homogenen statistischen Daten verfügbar, um die Entwicklung der Cyberkriminalität zu messen. Der beste Indikator für die Entwicklung der Cyberkriminalität in der Schweiz sind sehr wahrscheinlich die Statistiken des BFS, da sie auf den Anzeigen bei den Strafverfolgungsbehörden basieren. Eine spezifische Kategorie für Cyberkriminalität existiert allerdings erst seit 2019.

2.2.1 Polizeiliche Kriminalstatistiken[28]

Das BFS erhebt jedes Jahr die von den kantonalen Polizeibehörden registrierten Straftaten. Die Statistiken vermitteln aber lediglich ein partielles Bild der Cyberkriminalität, vor allem aus folgenden Gründen:

- Bei der Cyberkriminalität ist die Dunkelziffer – das heisst die Zahl der Delikte, die nicht angezeigt werden – sehr hoch. Eine Schätzung des Dunkelzifferanteils ist naturgemäss sehr schwierig, dennoch wird allgemein davon ausgegangen, dass lediglich 10–20 Prozent der Delikte in Zusammenhang mit Cyberkriminalität angezeigt werden.[29]
- Sie geben keinen Aufschluss über die gerichtlichen Folgen der einzelnen Straftaten. Es existiert keine Statistik über die Anzahl eröffneter Verfahren oder deren Ausgang.
- Vor 2020 wurden in den polizeilichen Kriminalstatistiken lediglich die Zahlen zu den verschiedenen Artikeln des Schweizerischen Strafgesetzbuches veröffentlicht. Obwohl gewisse Straftatbestände des Strafgesetzbuches eine starke digitale Komponente haben, ist der Anteil an Fällen mit einer digitalen Komponente insgesamt sehr schwierig zu beurteilen.

Das Jahr 2020 diente als Referenzgrundlage für die neue Methodik zur Zählung der Straftaten mit digitaler Komponente, welche darin besteht, die Cyberkriminalität anhand der Kombination «Straftat – Tatvorgehen» zu ermitteln. So wird das der Straftat zugrunde liegende Tatvorgehen bestimmt, welches einem Phänomen entspricht, das in die Statistik einfliesst. NEDIK erfasst derzeit 33 verschiedene Tatvorgehen, gegliedert in fünf Bereiche (vgl. nachfolgende Tabelle):

Bereich	**Cyber-Wirtschaftskriminalität**	**Cyber-Sexualdelikte**	**Cyber-Rufschädigung und unlauteres Verhalten**	**Darknet und andere[30]**
Anzahl Tatvorgehen	24	4	3	2
Tatvorgehen (digitalisierte Kriminalität; Cybercrime)	Phishing Hacking (2 Typen) Malware (5 Typen) DDOS Cyberbetrug (12 Typen) Money-/Package-Mules Sextortion (money) Diebstahl von Kryptowährungen	Verbotene Pornografie Grooming Sextortion (sex) Live Streaming	Cybersquatting Cyber-Rufschädigung (geschäftlich) Cyberbullying/Cybermobbing	Illegaler Handel im Darknet Data Leaking

Tab. 1: Tatvorgehen der Cyberkriminalität

[28] Sämtliche in diesem Kapitel präsentierten Zahlen stammen aus den polizeilichen Kriminalstatistiken des BFS.
[29] Crime Survey 2022, Medienmitteilung der KKPKS vom 24. August 2023: «Die Anzeigerate ist dabei sehr tief: Neun von zehn Delikten werden nicht bei der Polizei angezeigt. Ein Grossteil der Cyberdelikte verbleibt daher im Dunkelfeld.»
[30] Da das Darknet nur einen minimalen Anteil an den Fällen von Cyberkriminalität in der Schweiz hat, wurde dieser Bereich für den Bericht mit dem Bereich «Andere» zusammengenommen.

Wie fit sind die Kantone in der Cyber-Strafverfolgung?

Abbildung 1 zeigt die Zahlen von 2019[31] bis 2023 zu sämtlichen vom BFS erhobenen Fällen. Diesen Zahlen zufolge nimmt die Cyberkriminalität seit 2019 regelmässig zu, mit einem Anstieg von rund 111 % in vier Jahren. Den grössten Anteil mit über 80 % der Fälle pro Jahr macht die Cyber-Wirtschaftskriminalität aus. Cyber-Sexualdelikte sind der zweitgrösste Bereich mit durchschnittlich rund 10 % der Fälle pro Jahr; innerhalb dieser Kategorie entfallen rund 90 % der Fälle pro Jahr auf verbotene Pornografie. Es folgen Cyber-Rufschädigungen und unlauteres Verhalten mit durchschnittlich 5 % der Fälle pro Jahr. Die letzten zwei Bereiche schliesslich repräsentieren zusammen knapp 0,1 % der Fälle pro Jahr.

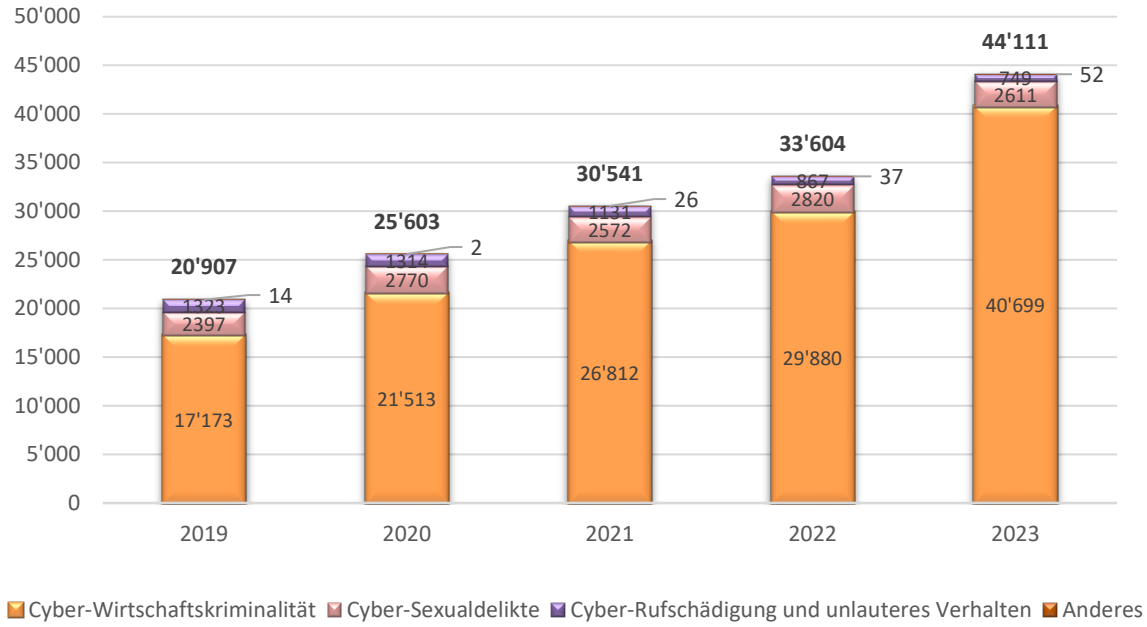


Abb. 1: Anzahl der Fälle pro Jahr nach Cyberkriminalitätsbereich

Die jährliche Entwicklung nach Cyberkriminalitätsbereich ist in Abbildung 2 dargestellt. Die Veränderungen hängen stark mit der Anzeigeerstattung zusammen. Die Cyber-Wirtschaftskriminalität wächst seit 2019 regelmässig; die Zunahme innerhalb von vier Jahren beträgt rund 137 %. Dieser Bereich weist den stärksten Anstieg auf. Die Cyber-Sexualdelikte sind relativ stabil, mit rund 9 % mehr Fällen als 2019 und einem leichten Rückgang im Vergleich zu 2020 und 2022. Cyber-Rufschädigung und unlauteres Verhalten haben über vier Jahre kontinuierlich abgenommen; der Rückgang beträgt rund 43 %. Bei den letzten beiden Bereichen erübrigt sich die Betrachtung der Entwicklung angesichts der zu tiefen jährlichen Fallzahlen.

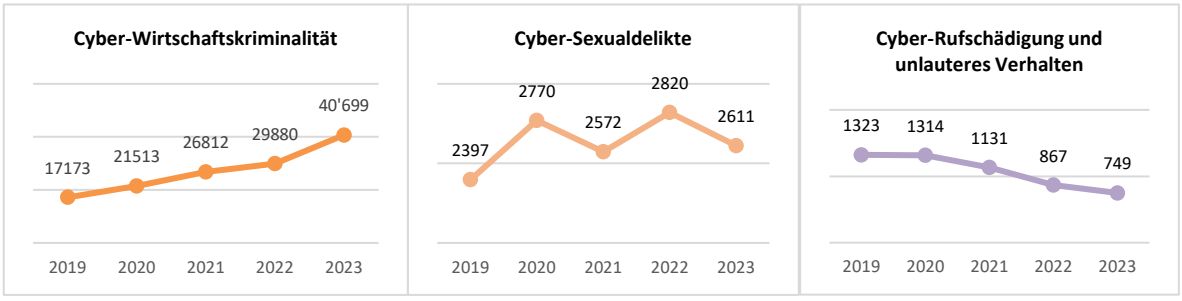


Abb. 2: Entwicklung der Anzahl Fälle pro Jahr nach Cyberkriminalitätsbereich

Abbildung 3 zeigt die Verteilung der Cyber-Wirtschaftskriminalität nach Teilbereich. Der grösste Teilbereich mit 75–80 % der Fälle von Cyber-Wirtschaftskriminalität ist der Cyberbetrug[32]. Bezogen auf

[31] Obwohl die offiziellen Zahlen erst ab dem Jahr 2020 veröffentlicht wurden, standen uns die Zahlen für 2019 zur Verfügung.
[32] Die Kategorie Cyberbetrug aggregiert die Daten der folgenden zwölf Tatvorgehen: CEO/BEC Fraud, betrügerische Internetshops, falsche Immobilienanzeigen, falsche Unterstützungsanfragen, Vorschussbetrug, betrügerischer technischer Support, Romance Scam, Kleinanzeigeplattformen (Ware nicht bezahlt), Kleinanzeigeplattformen (Ware nicht geliefert), Missbrauchen einer fremden Identität / von Online-Zahlungssystemen, um einen Betrug zu begehen, Online-Anlagebetrug, anderer Internetbetrug. Die Definitionen zu diesen Tatvorgehen sind verfügbar unter: Digitale Kriminalität | Bundesamt für Statistik (admin.ch)

die Cyberkriminalität insgesamt macht Cyberbetrug etwa zwei Drittel aller Fälle aus. Bei den anderen Tatvorgehen der Cyber-Wirtschaftskriminalität sind die Anteile 2023 wie folgt: 9,3 % Phishing, 2,7 % Hacking, 1,2 % Malware[33], 7,4 % Mules[34], 4,2 % Sextortion (money)[35] und 0,2 % andere Phänomene.

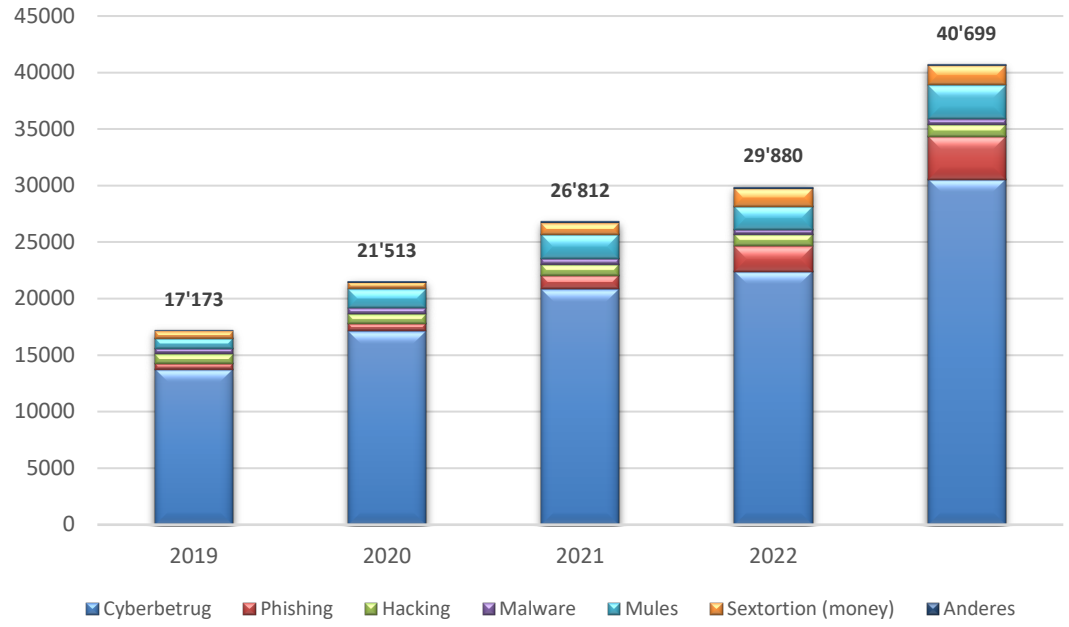
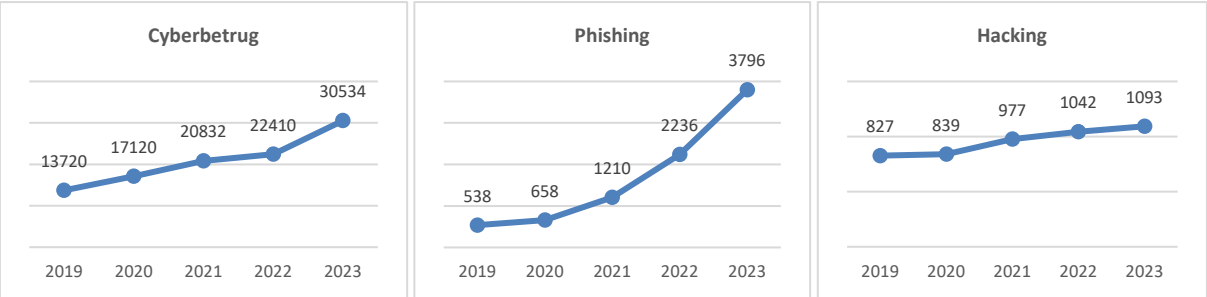


Abb. 3: Jährliche Verteilung der Fälle nach Teilbereich der Cyber-Wirtschaftskriminalität

Abbildung 4 zeigt die Entwicklung der Teilbereiche der Cyber-Wirtschaftskriminalität. Cyberbetrug hat zwischen 2019 und 2023 regelmässig zugenommen; über vier Jahre betrug der Anstieg mehr als 123 %. Auch Phishing hat während des ganzen Zeitraums zugenommen, wobei der Anstieg zwischen 2020 und 2023 stärker ausgeprägt war. Innerhalb von drei Jahren haben die Fälle um fast 605 % zugenommen. Im Vergleich dazu sind beim Hacking die Fälle im betrachteten Zeitraum weniger stark gestiegen, mit einer Zunahme von rund 32,2 %. Bei den Malware-Fällen zeigten sich im Laufe der Jahre leichte Veränderungen sowohl nach oben als auch nach unten, die Zahlen sind aber heute praktisch auf ähnlichem Niveau wie 2019. Dabei ist darauf hinzuweisen, dass diese Zahlen hauptsächlich mit einer allgemeinen Abnahme aller Tatvorgehen ausser Ransomware zusammenhängen. Ransomware machte 2019 noch 46,5% der Malware-Fälle aus, 2022 jedoch über 70 %. 2023 ist ihr Anteil allerdings auf 53 % gesunken. Fälle von Mules und Sextortion (money) schliesslich haben zwischen 2019 und 2023 relativ stark zugenommen, nämlich um 227 % bzw. 162,9 %.



[33] Die Kategorie Malware aggregiert die Daten der folgenden fünf Tatvorgehen: Ransomware, E-Banking-Trojaner, Spyware, Rogueware/Scareware, Botnet. Die Definitionen zu diesen Tatvorgehen sind verfügbar unter: Digitale Kriminalität | Bundesamt für Statistik (admin.ch)
[34] Weiterleiten lassen von Geldern oder Waren krimineller Herkunft durch Dritte (Finanzagenten: Money Mules, Paketagenten: Package Mules).
[35] Erpressung von Geld mittels Nacktaufnahmen oder Videoclips, auf welchen das Opfer sexuelle Handlungen an sich vornimmt (masturbiert), und Androhung der Veröffentlichung des Videos auf Youtube oder des Versands z. B. an Facebook-Freunde des Opfers.

Wie fit sind die Kantone in der Cyber-Strafverfolgung?

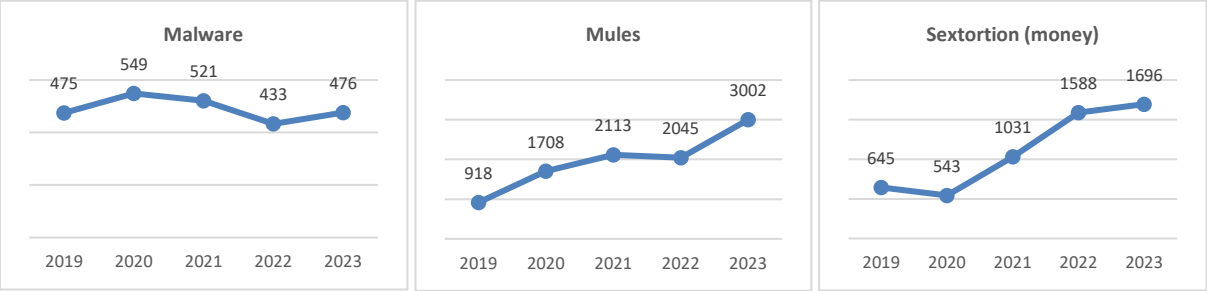


Abb. 4: Entwicklung der Anzahl Fälle pro Jahr nach Teilbereich der Cyber-Wirtschaftskriminalität

2.2.2 Analyse

Im betrachteten Zeitraum hat die Cyberkriminalität zugenommen. Seit 2020 erscheint die Zunahme sehr stark. Der Anstieg der Fallzahlen konzentrierte sich vor allem auf die Kategorie Cyberbetrug, die mittlerweile rund 70 % aller vom BFS erfassten Fälle ausmacht.

Neben einer allgemeinen Zunahme der Cyberkriminalität, die oben präsentierte Statistiken zeigen, stellen gewisse Phänomene der Cyberkriminalität in der Schweiz eine zunehmend grössere Bedrohung dar, obwohl sie nicht zu den häufigsten Tatvorgehen gehören.

Dies gilt beispielsweise für Ransomware, ein Phänomen, das in den letzten Jahren nicht so stark zugenommen hat wie andere, heute aber die schwerwiegendste Cyberbedrohung für die Organisationen in der Schweiz darstellt und von dem mittlerweile sämtliche Wirtschaftszweige weltweit betroffen sind. Auf Seiten der Strafverfolgungsbehörden erfordern diese Fälle eine hochtechnische Ermittlungsarbeit und ausreichend Ressourcen, um solche Ermittlungen tätigen zu können.

In der Kategorie Cyberbetrug hat der Online-Anlagebetrug in den letzten Jahren stark zugelegt. Mit einem Anstieg um rund 261 % zwischen 2020 und 2023 und einem Anteil von 8,4 % aller Cyberbetrugsfälle handelt es sich um eines der Delikte, das die grössten finanziellen Verluste verursacht (2022 über 100 Millionen Schweizer Franken).

Diese allgemeine zunehmende Tendenz in der Cyberkriminalität ist auch auf internationaler Ebene zu beobachten. Die Täterschaft im digitalen Bereich entwickelt sich in alarmierendem Tempo weiter. Die Digitalisierung berührt alle Formen der Kriminalität, und die von Cyberkriminellen verwendeten Methoden werden immer häufiger in anderen Kriminalitätsbereichen übernommen.[36] Zudem haben verschiedene aktuelle technologische Entwicklungen das Potenzial, die Landschaft der Cyberkriminalität zu transformieren. Gewisse dieser Entwicklungen haben bereits einen sichtbaren Einfluss, bei anderen wird dies vermutlich bald der Fall sein wird (zum Beispiel künstliche Intelligenz, Quantentechnologie, Metaverse).[37]

2.3 Aktuelle Herausforderungen

Die Bekämpfung der Cyberkriminalität birgt besondere Herausforderungen, einige davon interner Natur (personelle und technische Ressourcen in den Polizeikorps), andere hängen mit internationalen Tendenzen zusammen, wie unterschiedlichen Regimes der internationalen Rechtshilfe in Strafsachen oder technologischen Entwicklungen, von denen fast immer – zuerst – die Cyberkriminellen profitieren. Im Folgenden werden die wichtigsten Herausforderungen präsentiert. Sie wurden anhand der relevanten Fachliteratur und infolge Diskussionen in der strategischen und der fachlichen Begleitgruppe ausgewählt.

[36] (European Union Agency for Law Enforcement Cooperation, 2021)
[37] (European Union Agency for Law Enforcement Cooperation, 2023)

2.3.1 Mangelnde personelle und technische Mittel

- ❖ Mangelnde personelle Ressourcen sind das Hauptproblem in der Bekämpfung der Cyberkriminalität. Die Feststellung der Fachleute ist eindeutig: Kein Polizeikorps in der Schweiz verfügt über ausreichend Ressourcen für eine wirksame Bekämpfung der Cyberkriminalität.

Auch wenn die meisten Anzeigen bearbeitet werden – in den meisten Fällen werden keine vertieften Ermittlungen durchgeführt (siehe Ziff. 3.2.5). Sowohl infolge der kontinuierlichen Zunahme von Massencyberkriminalität (namentlich beim Cyberbetrug) als auch der relativ stabilen Anzahl hochkomplexer Delikte, die aufzuklären sind (namentlich Ransomware-Angriffe), sind die Ressourcen stark unter Druck. Aufgrund der wachsenden Masse von zu bearbeitenden Daten und der technischen Komplexität von Cybercrime sind auch die ermittlungsunterstützenden Ressourcen unzureichend.
Viele Polizeikorps bekunden Mühe, neues Personal zu finden. Der Verband Schweizerischer Polizei-Beamter (VSPB) hat Ende 2022 seine Besorgnis darüber zum Ausdruck gebracht.[38] Die Stellungnahme ist vor dem Hintergrund zahlreicher Medienberichte zu diesem Thema zu sehen.[39] Um die Rekrutierungsschwierigkeiten und vorzeitigen Personalabgänge zu erklären, werden viele Gründe angeführt: ungenügende Löhne, anspruchsvolle Arbeitsbedingungen (Nachtarbeit, kaum Möglichkeit von Teilzeitarbeit) oder auch Rekrutierungskriterien, die überdacht werden müssen. Im Bereich der Bekämpfung von Cyberkriminalität ist das Problem umso akuter, als das Personal spezifisch ausgebildet werden muss (beispielsweise über die entsprechenden Kurse des Schweizer Polizei-Instituts [SPI]) und das gesuchte Personal (IT-Analytiker, Kriminalanalytikerinnen) einem Profil entspricht, das in anderen Wirtschaftszweigen ebenso sehr gesucht ist.[40]
Nebst dem spezifisch ausgebildeten Personal benötigen die Strafverfolgungsbehörden auch Tools, welche die Täteridentifikation erleichtern. So beispielsweise Tools, die der Nachverfolgung von Geldflüssen in Kryptowährung dienen[41], um an Informationen zu Wallet-Inhaberinnen und -Inhabern zu gelangen – und somit beispielsweise zur Person, die in einem Fall von Online-Anlagebetrug oder einem Ransomware-Angriff die Zahlung erhalten hat. Weiter gehören dazu Tools für die Analyse von Internetnetzwerken oder grossen Mengen beschlagnahmter Daten. Diese Tools werden in der Regel von privaten Unternehmen entwickelt und sind teuer. Darüber hinaus existiert eine Vielzahl an Tools, von denen einige nur bestimmte Funktionen bieten, welche rasch veralten können. Die Strafverfolgungsbehörden müssen daher regelmässig überprüfen, dass sie noch im Besitz der relevanten Tools sind.

2.3.2 Fehlen einer nationalen Datenbank

In der Schweiz hat jede Kantonspolizei ein eigenes System zur Dokumentation ihrer Ermittlungen. Gewisse Bundesdatenbanken (RIPOL[42], IPAS[43], KasewareCH[44]) werden gemeinsam genutzt und ermöglichen den Informationsaustausch zu Personen und Ermittlungen. Dass es diese Datenbanken gibt, liegt daran, dass sie auf einer gesetzlichen Grundlage basieren, welche die Kantone zum Austausch polizeilicher Informationen mit dem Bund und umgekehrt ermächtigt (Bundesgesetz über die polizeilichen Informationssysteme des Bundes, BPI; SR 361).[45] Die Mehrheit der Kantone verfügt hingegen über **keine gesetzlichen Grundlagen, welche den automatischen Austausch von**

[38] Medienmitteilungen: Verband Schweizerischer Polizei-Beamter VSPB
[39] Die Kantonspolizei St. Gallen sucht verzweifelt nach Fachkräften - Blick
Der Polizeiberuf im Aargau büsst an Attraktivität ein (aargauerzeitung.ch)
Face à la pénurie de main d'oeuvre, les polices romandes peinent à susciter des vocations - rts.ch - Régions
[40] In acht Jahren fehlen in der Schweiz fast 40'000 ICT-Fachkräfte | Netzwoche
[41] 22.3017 | Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen | Geschäft | Das Schweizer Parlament
[42] RIPOL ist ein automatisiertes Personen- und Sachfahndungssystem. Es wird gemeinsam durch die zuständigen Behörden des Bundes und der Kantone zur Unterstützung verschiedener gesetzlicher Aufgaben im Bereich der Fahndung geführt.
[43] IPAS ist das informatisierte Personennachweis Aktennachweis- und Verwaltungssystem von fedpol. Im IPAS wird der ganze Interpol-Verkehr aufgenommen sowie Falldaten
– des Erkennungsdienstes (u.a. Personalien zu Fingerabdrücken und DNA-Profilen);
– der Verwaltungspolizei im Zuständigkeitsbereich von fedpol.
[44] KasewareCH ist das von fedpol, den Kantonspolizeien, dem BAZG, der BA und dem BJ verwendete Ermittlungssystem.
[45] Das BPI regelt namentlich den polizeilichen Informationssystem-Verbund (Art. 9–14), das automatisierte Polizeifahndungssystem (RIPOL; Art. 15), den nationalen Teil des Schengener Informationssystems (N-SIS; Art. 16), den Nationalen Polizeiindex (Art. 17) und das Geschäfts- und Aktenverwaltungssystem von fedpol (Art. 18).

polizeilichen Informationen mit anderen Kantonen und dem Bund erlauben.[46] In der Konsequenz bedeutet dies, dass beispielsweise in einem Fall einer Phishing-Mail-Welle unter Umständen mehrere Kantone parallel zum gleichen Täter ermitteln, ohne sich untereinander zu koordinieren. Um dieses Problem zu beheben, arbeitet das EJPD an der Umsetzung der Motion 18.3592 Eichenberger.[47] Die Westschweizer Kantone haben ein eigenes Instrument aufgebaut, um diese Lücke zu schliessen: die Plateforme d'Information sur la Criminalité Sérielle en Ligne (PICSEL)[48]. Mehrere Kantone haben sich der Plattform seit ihrer Schaffung angeschlossen, dennoch wird sie insgesamt in einer Minderheit der Kantonspolizeien verwendet.
Das Fehlen einer gemeinsamen interkantonalen oder nationalen Datenbank erschwert die Koordination der Bekämpfung der Cyberkriminalität. Dank der Gründung von **NEDIK konnten Redundanzen reduziert werden,** da der operative Austausch zu laufenden Ermittlungen begünstigt wird.[49] Auf Stufe der Staatsanwaltschaften **strebt das Cyberboard ebenfalls eine Verbesserung der strategischen und operativen Koordination** in der Bekämpfung der Cyberkriminalität an.[50] Dieses **Ziel ist ohne nationale Datenbank schwer zu erreichen,** welche einen Gesamtüberblick über die laufenden Fälle bieten würde. Auch die internationale Koordination leidet unter diesem Mangel, ist es doch schwierig, sich an grossangelegten internationalen Operationen zu beteiligen, solange man lediglich einen partiellen Überblick über die in der Schweiz laufenden Ermittlungen hat.

> Die Westschweizer Kantone haben ein eigenes Instrument aufgebaut, um die Lücke zu schliessen: die Plateforme d'Information sur la Criminalité Sérielle en Ligne (PICSEL). Obwohl sich der Plattform seit ihrer Schaffung mehrere Kantone angeschlossen haben, wird sie insgesamt nur in einer Minderheit der Kantonspolizeien verwendet. Um dieses Problem zu beheben, arbeitet das EJPD an der Umsetzung der Motion 18.3592 Eichenberger.

2.3.3 Zu seltene Strafanzeigen

In 90 Prozent der Fälle erstatten die Opfer von Cyberkriminellen keine Strafanzeige. Diese Zurückhaltung kann unterschiedliche Gründe haben: ein mit der Tatsache, Opfer von Betrug geworden zu sein, verbundenes Schamgefühl, ein geringer entwendeter Betrag, komplizierte Verfahren zur Erstattung einer Anzeige oder auch Resignation angesichts der geringen Hoffnung, dass die Täterschaft verhaftet oder das Geld zurückerlangt werden kann. Die sehr tiefe Anzeigerate erschwert der Polizei die Arbeit beträchtlich. Es ist äusserst schwierig, einen besonders aktiven Täter zu identifizieren und dafür die notwendigen Ressourcen aufzuwenden, wenn lediglich 10 Prozent der Delikte angezeigt werden. Die tiefe Anzeigerate bedeutet auch, dass zahlreiche Täter ganz einfach **nicht verfolgt werden und eine gewisse Straflosigkeit geniessen.**[51]

> Die Umsetzung des Online-Anzeigeportals «Suisse ePolice» wird das Problem der Anzeigeerstattung reduzieren. Über dieses Portal können drei Massenphänomene zentral angezeigt werden. Bislang sind zwölf Polizeikorps am Dispositiv beteiligt, langfristig sollen alle Kantone angeschlossen werden. Das Problem der tiefen Anzeigerate darf nicht isoliert von den personellen Ressourcen betrachtet werden: Eine Steigerung der Anzeigerate muss mit der Bereitstellung zusätzlicher Ressourcen für Ermittlungen einhergehen.

[46] 18.3592 | Nationaler polizeilicher Datenaustausch | Geschäft | Das Schweizer Parlament
[47] Die Motion beauftragt den Bundesrat, «eine zentrale nationale Polizeidatenbank oder eine Vernetzungsplattform für die bestehenden kantonalen Polizeidatenbanken zu schaffen, mittels welcher die Polizeikorps der Kantone und die Polizeiorgane des Bundes direkt auf die polizeilichen Daten über Personen und deren Vorgänge in der gesamten Schweiz zugreifen können. Sofern die hierfür notwendige Rechtsgrundlage fehlt, ist eine solche im Bundesrecht zu schaffen.» Der Bundesrat hat die Annahme der Motion beantragt und die Umsetzungsarbeiten sind in Gang.
[48] Communiqué de presse - Les polices romandes se dotent d'un Centre de Compétence Cyber | ge.ch
[49] Verstärkter Einsatz der Kantone gegen Cyber- und Pädokriminalität - KKJPD - CCDJP - CDDGP - DE
[50] (Bundesanwaltschaft, 2021)
[51] Das grosse Tabu der Cyberkriminalität: Erfolgreiche Erpresser (watson.ch)

2.3.4 Noch unzureichende Prävention

Nach begangener Straftat die Täterschaft zu fassen, ist in der Regel sehr komplex. Ermittlungen sind aufwändig und dauern lange. Selbst wenn es den Ermittlerinnen und Ermittlern gelingt, die Täterschaft zu identifizieren, ist die Wahrscheinlichkeit tief, dass die Vermögenswerte wiedererlangt und die Täter verurteilt werden (vor allem, wenn sie in Ländern Zuflucht suchen, mit denen die justizielle Zusammenarbeit kompliziert ist). Prävention ist daher zentral. In den meisten Fällen wird eine Straftat erst möglich, wenn das Opfer einen Fehler macht – zum Beispiel ein zu einfaches Passwort benutzt, die Herkunft von E-Mails nicht kontrolliert, eine Anwendung nicht updatet oder sensible Daten an Unbekannte weitergibt. Es ist daher wichtig, die Bevölkerung für einfache, aber wirksame, nicht sehr aufwändige Methoden zu sensibilisieren, mit denen verhindert werden kann, Opfer solcher Straftaten zu werden. Die Kriminellen passen ihre Betrugsmethoden unablässig den technologischen und geopolitischen Entwicklungen an. Die Prävention darf diesbezüglich nicht nachstehen. Auch muss geprüft werden, inwiefern die Internet Service Provider ihre Präventionsanstrengungen steigern können, um namentlich zu verhindern, dass ihre Plattformen zu kriminellen Zwecken missbraucht werden. Diesbezüglich kommt dem Austausch zwischen Strafverfolgungsbehörden und diesen Plattformen eine wichtige Rolle zu, da er die Implementation von technischen Präventionsmassnahmen ermöglicht.

2.3.5 Schwierigkeiten beim Zugang zu elektronischen Beweismitteln

Heute benötigen Ermittlerinnen und Ermittler in den allermeisten Ermittlungen Zugang zu elektronischen Daten, etwa zum Inhalt eines E-Mail-Postfachs oder zu Konversationen in Chat-Anwendungen. Gerade im Zusammenhang mit Cyberkriminalität ist zentral, rasch über diese Daten zu verfügen. Die Täter sind häufig erfahren und versuchen, ihre Spuren schnellstmöglich zu verwischen. Das Problem ist, dass diese Daten nur sehr selten in der Schweiz gespeichert sind. Das Übereinkommen über Cyberkriminalität (Budapest-Konvention) geht dieses Thema in einigen Elementen bereits an, beschränkt sich aber auf die Zusammenarbeit mit Vertragsstaaten und gestattet den direkten und somit schnelleren Zugriff auf Beweisdaten lediglich auf freiwilliger Basis. Um ausserhalb dieser Möglichkeiten an die Daten zu gelangen, wird daher häufig der Weg der traditionellen Rechtshilfe in Strafsachen beschritten. Diese ist jedoch häufig zu langsam, als dass die Strafverfolgungsbehörden ihre Arbeit effizient erledigen könnten.[52] In vielen Fällen wird schlicht keine Rechtshilfe geleistet. In gewissen Ländern sind Internet Service Provider nicht verpflichtet, den Internetverkehr ihrer Kundschaft zu speichern, sodass sie selbst bei Erhalt eines begründeten Ersuchens keine Daten liefern können. Und selbst wenn sie im Besitz der Daten wären, hat die Täterschaft angesichts des langsamen Prozesses häufig Gelegenheit, ihre Spuren zu verwischen. Gewisse Initiativen, wie die Budapest-Konvention, sehen Instrumente vor (Preservation Request), mit denen die Grenzen der internationalen Rechtshilfe in Strafsachen teilweise umgangen werden können. Allerdings fehlt eine weltweite Harmonisierung, und diese Instrumente sind nicht voll und ganz zufriedenstellend.[53] Am 13. Juni 2023 hat die EU das Gesetzespaket zur e-Evidence verabschiedet. Ziel des Gesetzespakets ist es, einen kohärenten EU-Rahmen für den Umgang mit elektronischen Beweismitteln zu schaffen und deren Erhebung zu beschleunigen.[54] Das Schweizer Recht basiert derzeit ausschliesslich auf der Rechtshilfe, die relativ langsam und nicht auf elektronische Beweismittel zugeschnitten ist.[55] Die beachtlichen Schwierigkeiten beim Zugang zu elektronischen Daten bedeuten daher eine grosse Herausforderung für die Strafverfolgungsbehörden. Es ist wichtig, dass die Schweiz die internationalen Entwicklungen, insbesondere auf Ebene der EU, verfolgt und allfällige Massnahmen prüft.

[52] (Bundesamt für Justiz, 2021), S. 4.
[53] (European Union Agency for Law Enforcement Cooperation, 2022)
[54] (Bundesamt für Justiz, 2023), S. 3.
[55] (Bundesamt für Justiz, 2023), S. 23.

2.3.6 Verwendung neuer Technologien mit bösartigen Absichten

- ❖ Viele neue Technologien werden rasch von Cyberkriminellen aufgegriffen und mit schädlichen Absichten eingesetzt, sei dies zum Zweck der Anonymisierung oder auch für neue kriminelle Aktivitäten.

Die Digitalisierung der Gesellschaft bringt mit sich, dass mehr und mehr kritische Daten in elektronischer Form gespeichert werden. Kriminelle haben sich dies mit der Entwicklung und Verbreitung von Ransomware rasch zunutze gemacht. Ransomware macht nur einen minimalen Anteil der Cyberstraftaten aus, verursacht aber enorme Schäden[56], die schwer zu quantifizieren sind.[57] In vielen Cyberbetrugsfällen werden Kryptowährungen verwendet, sei es als Zahlungsmittel für das Lösegeld, als Vehikel für die Geldwäsche illegaler Profite oder auch als Betrugsmechanismus an sich.[58] Obwohl Kryptowährungen – entgegen der landläufigen Meinung – in der Regel rückverfolgbar sind, braucht es dazu qualifiziertes Personal und teure Software.[59] Andere Technologien sind noch zu neu, als dass Cyberkriminelle sie massenhaft nutzen. Die künstliche Intelligenz hat jedoch das Potenzial, künftig für unzählige kriminelle Zwecke eingesetzt zu werden: von überzeugenden Phishing-Mails über adaptive Malware bis zur Verbesserung der Konversationen für pädokriminelle Zwecke oder Romance Scams.[60] Künstliche Intelligenz hat auch zur Entstehung von «Deepfakes» – äusserst realistischen, aber gefälschten Videos – geführt, die zu pädokriminellen Zwecken, zur Verbreitung von Fake News oder zu Betrugszwecken verwendet werden können.[61] Gewisse in der realen Welt begangene kriminelle Aktivitäten können ebenso in der Virtual Reality (Metaverse) begangen werden (Rekrutierung, Pädokriminalität).[62]

Auch wird es für Kriminelle immer einfacher, ihre Spuren zu verbergen. Zahlreiche Anwendungen, die einfach heruntergeladen werden können und grossmehrheitlich zu legalen Zwecken verwendet werden, umfassen eine Nachrichtenverschlüsselung. Gewisse Anwendungen bieten darüber hinaus zusätzliche Dienste, um die Anonymität ihrer Kundschaft zu garantieren, sodass diese Unternehmen, selbst wenn sie von der Polizei – über den Dienst ÜPF – um Informationen angefragt werden, kaum welche liefern.[63] Die Verwendung solcher Techniken mit Technologien wie Virtual Private Networks (VPN, mit denen die IP-Adresse verschleiert werden kann) oder The Onion Router (TOR, der ebenfalls Anonymität garantiert) erschwert den Strafverfolgungsbehörden die Identifikation der Cyberkriminellen erheblich. Über andere Techniken der Anonymisierung, oder vielmehr des Identitätsmissbrauchs, können Cyberkriminelle verschiedene identifizierende Informationen nachahmen, etwa eine Telefonnummer (Spoofing, Smishing) oder auch eine E-Mail-Adresse oder Internetdomain. Solche Techniken werden in sehr vielen Betrugsfällen eingesetzt, häufig zusammen mit der Voice-over-IP-Technik (Telefonanrufe übers Internet). Sie ermöglichen gleichzeitig, das Opfer in die Irre zu führen und die Spuren der Täter zu verschleiern.[64]

2.4 Schlussfolgerungen

Die Bekämpfung der Cyberkriminalität ist komplex. In der Schweiz sind zahlreiche Akteure involviert – insbesondere die 26 Kantonspolizeien und die 26 kantonalen Staatsanwaltschaften sowie die Bundesanwaltschaft und fedpol. Diese Vielzahl an Akteuren erschwert die Koordination. Eine gewisse Abhilfe schaffen spezifisch hierfür ins Leben gerufene Koordinationsgremien. Durch die konstante

[56] Ransomware: the number one cyber threat for enterprises... - NCSC.GOV.UK
[57] In sehr vielen Fällen verzichten die Opfer – in der Regel Unternehmen, aber auch öffentliche Verwaltungen – auf eine Anzeige und/oder zahlen das Lösegeld. Über die Lösegeldzahlung hinaus sind auch die Reputationsschäden und die Verluste in Zusammenhang mit der Beeinträchtigung oder dem vollständigen Ausfall der Infrastruktur zu berücksichtigen.
[58] (European Union Agency for Law Enforcement Cooperation, 2021)
[59] Siehe dazu ausführlicher KGGT-Bericht, Ziff. 7.4.1.
[60] (European Union Agency for Law Enforcement Cooperation, 2023)
[61] (European Union Agency for Law Enforcement Cooperation, 2022)
[62] (European Union Agency for Law Enforcement Cooperation, 2022)
[63] Internet_organised_crime_threat_assessment_iocta_2021.pdf (europa.eu), S. 9.
[64] FBI Warns Against Vishing Scams Over VoIP (securityintelligence.com)

Zunahme der Cyberkriminalität sind die Strafverfolgungsbehörden mit zahlreichen weiteren Herausforderungen konfrontiert: ungenügenden Personalressourcen, einem manchmal inadäquaten nationalen und internationalen Rechtsrahmen, agilen Kriminellen, die bei jeder technologischen Innovation die sich bietende Gelegenheit nutzen, oder auch einer sehr tiefen Anzeigerate. Diese Fragen wurden in der Konsultation der kantonalen Strafverfolgungsbehörden aufgegriffen, deren Ergebnisse in Kapitel 3 präsentiert werden.

3 Ergebnisse der Konsultation

Im Gegensatz zu anderen Bereichen, wie der Cybersicherheit, gibt es keinen internationalen Standard, der definiert, worin eine wirksame Bekämpfung der Cyberkriminalität besteht. Anstatt also zu versuchen, zu ermitteln, wie fit die Kantone diesbezüglich sind, bezweckt der Bericht vielmehr, die Forderung des Postulanten zu erfüllen und eine Bestandesaufnahme im Bereich der Bekämpfung der Cyberkriminalität in der Schweiz vorzulegen. Der Postulant verlangt namentlich, dass geprüft wird, ob die gesetzlichen Grundlagen und die Organisation angepasst wurden und ob Ressourcen gebündelt werden müssen. Die Bestandsaufnahme wurde mithilfe einer Umfrage realisiert, die Fragen rund um die gesetzlichen Grundlagen, die Organisation (Rekrutierung, Aufbau von spezifischen Einheiten zur Bekämpfung von Cyberkriminalität) und die Ressourcenbündelung beinhaltete. Um eine vollständige Gesamtsicht zu erhalten, wurde die Umfrage mit Fragen zu Ausbildung, technischen Mitteln, Best Practices und Massnahmen, die zur Verbesserung der Bekämpfung der Cyberkriminalität ergriffen werden sollten, ergänzt.

Fast alle Kantonspolizeien und Staatsanwaltschaften sowie eine Mehrheit der Gerichte haben sich an der Umfrage beteiligt. Um gewisse Ergebnisse einzuordnen, wurden die Antworten in den Begleitgruppen diskutiert. Zum ersten Mal wurde eine so umfassende Umfrage zur Cyberkriminalität bei den Schweizer Strafverfolgungsbehörden durchgeführt. Dank dem ausgezeichneten Rücklauf kann die vom Postulat geforderte Bestandesaufnahme erstellt werden.

3.1 Gesetzliche Grundlagen

- Lediglich eine Minderheit der Kantone verfügt über die gesetzlichen Grundlagen für einen automatischen interkantonalen Austausch von polizeilichen Informationen. Eine Mehrheit der Kantone verfügt über die gesetzlichen Grundlagen für präventive verdeckte Massnahmen im Internet.

Lediglich eine Minderheit der Kantonspolizeien (11) gab an, über die gesetzlichen Grundlagen für einen vollständigen automatischen interkantonalen Austausch von polizeilichen Informationen zu verfügen. Vierzehn Kantonspolizeien gaben an, über gesetzliche Grundlagen zu verfügen, welche einen partiellen Austausch erlauben (das heisst in der Regel einen Austausch im Einzelfall). Drei Kantone sind dabei, ihre kantonalen Gesetze anzupassen, um den automatischen Datenaustausch zu erlauben.

Die überwiegende Mehrheit der Kantonspolizeien (23) verfügt über die gesetzlichen Grundlagen für präventive verdeckte Massnahmen im Internet, einschliesslich Peer-to-Peer-Monitoring oder Verwendung von Legenden (Pseudonymen) im Internet. Zwei Kantonspolizeien gaben zudem an, dass eine Anpassung der gesetzlichen Grundlagen im Gang sei. Auch wenn die Mehrheit der Kantone über gesetzliche Grundlagen verfügt, bedeutet dies allerdings nicht zwingend, dass sie auch über die technischen oder personellen Mittel zur Durchführung solcher Massnahmen verfügen.

3.2 Organisation

Die zahlreichen Polizeikorps in der Schweiz verfügen je über eine eigene Organisation. Unterschiedliche demografische und wirtschaftliche Faktoren sorgen dafür, dass die Anzahl (Cyber-)Delikte von einem Kanton zum anderen sehr stark variiert.[65] Daher ist es sehr schwierig, die Zahlen – wie beispielsweise die Grösse der Kriminalpolizei oder von spezifisch der Bekämpfung von Cyberkriminalität gewidmeten Einheiten – zu vergleichen. Es ist nicht einfach – nicht einmal für die einzelne Polizei – zu beziffern, wie viele Ressourcen für die Bekämpfung der Cyberkriminalität eingesetzt werden (siehe im Folgenden Kasten zum Begriff «Cyberermittler/in»). Denn die Bearbeitung einer Anzeige in Zusammenhang mit Cyberkriminalität durchläuft zahlreiche Etappen, die nicht alle von Cyberermittlerinnen und Cyberermittlern durchgeführt werden. Die Entgegennahme der Anzeige, die forensische Analyse und die verdeckten Massnahmen werden von anderen Spezialistinnen und Spezialisten ausgeführt. Umgekehrt kommt es vor, dass Cyberspezialistinnen und -spezialisten ihre Kolleginnen und Kollegen – angesichts der Digitalisierung der Gesellschaft – in Verfahren aller Art unterstützen, die nicht zwingend mit Cyberkriminalität zusammenhängen. Gewisse Polizeikorps bearbeiten so wenig Fälle, dass sie keine Vollzeitstelle für diese Art von Ermittlungen brauchen. Mehrere Kantone haben ausserdem eine Vereinbarung mit einem anderen Kanton geschlossen, um von diesem IT-forensische Leistungen beziehen zu können. Diese Kantone verfügen folglich nicht über eigene IT-forensische Ressourcen.

Aufgrund all dieser Faktoren wurden die in diesem Unterkapitel präsentierten Zahlen in der Regel schweizweit konsolidiert. Um möglichst feine Daten zu haben, wird empfohlen, dass jeder Kanton für sich eine Bestandesaufnahme zu den eigenen Mitteln erstellt, die er zur Bekämpfung der Cyberkriminalität einsetzt.

3.2.1 Struktur

Im Bereich der Bekämpfung von Cyberkriminalität existieren verschiedene Organisationsformen. Zahlreiche Polizeien haben sich für die Schaffung einer eigenen Einheit mit Cyberermittlerinnen und Cyberermittlern entschieden. Diese Einheit befasst sich nur mit Cyberkriminalität. Es gibt Einheiten, die sich ausschliesslich mit Cybercrime befassen, andere auch mit digitalisierter Kriminalität. In den meisten Polizeien ermitteln Ermittlerinnen und Ermittler, die nicht diesen Einheiten angehören, ebenfalls zu Cyberkriminalität (vor allem digitalisierter Kriminalität). Darüber hinaus werden alle diese Ermittlerinnen und Ermittler von Kriminalanalytikerinnen und IT-Forensik-Spezialisten unterstützt, welche in der Regel Leistungen für das ganze kriminalpolizeiliche Korps erbringen. Im Übrigen haben einige Polizeien ein Netzwerk von Cyberkontaktstellen in den dezentralisierten Einheiten aufgebaut.

[65] In der Schweiz werden im Durchschnitt 3,6 Delikte / 1000 Einwohnerinnen und Einwohner gezählt. Es gibt aber grosse Unterschiede je nach Kanton. Neun Kantone melden mehr als 4 Delikte / 1000 Einwohnerinnen und Einwohner (höchster Wert = 6,11/1000) und sechs Kantone melden weniger als 3 Delikte / 1000 Einwohnerinnen und Einwohner (tiefster Wert = 0,96/1000).

3.2.2 Spezifische Cybereinheit

Generell beabsichtigt die überwiegende Mehrheit der Kantonspolizeien (22/26), eine eigene Ermittlungseinheit ausschliesslich für die Bekämpfung der Cyberkriminalität zu schaffen, oder hat dies bereits getan. Deren Grösse unterscheidet sich erheblich von Kanton zu Kanton. Gemäss den Rückmeldungen der Kantone sind demnach über die ganze Schweiz verteilt 190 Vollzeitäquivalente für solche Einheiten vorgesehen.

Die Definition, was eine Cyberermittlerin oder ein Cyberermittler ist, variiert je nach Polizeikorps beachtlich. In einigen Korps übernehmen diese Personen mehrheitlich Ermittlungen in Zusammenhang mit Cybercrime, in anderen ist es eher die digitalisierte Kriminalität, und in einigen Korps bilden die Cyberermittlerinnen und Cyberermittler einen Pool, der die Kolleginnen und Kollegen bei allen Ermittlungen mit einer digitalen Komponente unterstützt. Es ist daher sehr schwierig, präzise zu quantifizieren, wie viele Cyberermittlerinnen und Cyberermittler in den einzelnen Korps vorhanden sind. Ausserdem gibt es Korps, die so wenige Cyberkriminalitätsfälle haben, dass die Schaffung einer Vollzeitstelle nicht zwingend gerechtfertigt ist.

3.2.3 Schaffung von Stellen

- Eine Mehrheit der Kantonspolizeien verfügt über eine spezifische Einheit zur Bekämpfung der Cyberkriminalität. Diese haben ihre Personalbestände zur Bekämpfung der Cyberkriminalität aufgestockt und planen, in den nächsten zehn Jahren weiteres zusätzliches Personal einzustellen.

Laut den Rückmeldungen der Kantone wurden in den letzten zehn Jahren in 23 Kantonspolizeien über 167 Stellen für Cyberermittlerinnen und Cyberermittler sowie IT-Forensik-Spezialistinnen und -Spezialisten geschaffen. Für Cyberermittlerinnen und Cyberermittler wurden schweizweit in den letzten zehn Jahren rund 85 Stellen geschaffen. Diese zusätzlichen Stellen sind auf 23 Kantone verteilt. Mehr als 82 zusätzliche Stellen sind insgesamt in 23 verschiedenen Kantonspolizeien für IT-Forensik-Spezialistinnen und -Spezialisten geschaffen worden.

Die Cyberermittlerinnen und Cyberermittler werden von anderen Fachleuten unterstützt, beispielsweise Expertinnen und Experten für IT-Forensik. Zu deren zahlreichen Aufgaben gehören die Sicherung von IT-Beweismitteln (Festplatten, Telefonen, vernetzten Geräten), die Analyse von deren Inhalt, Netzwerkanalysen oder auch die Analyse von Geldflüssen in Kryptowährung. Aufgrund der Digitalisierung der Gesellschaft werden sie in fast alle Ermittlungen eingebunden, nicht nur in Ermittlungen zu Cyberkriminalität. Darüber hinaus sind weitere Einheiten an solchen Ermittlungen beteiligt (zum Beispiel in Zusammenhang mit verdeckten Massnahmen wie Online-Infiltrationen oder Observationen oder auch der operativen oder taktischen Kriminalanalyse).

Gemäss den Rückmeldungen der Kantone werden in den nächsten zehn Jahren in 21 Kantonen 142 zusätzliche Ermittler- und Forensikerstellen geschaffen. Zum einen werden in 21 verschiedenen Kantonspolizeien über 87 neue Cyberermittlerstellen geschaffen. Zum anderen werden 15 Kantone auch ihre Bestände an IT-Forensik-Spezialistinnen und -Spezialisten aufstocken, dies mit insgesamt 55 zusätzlichen Stellen.

Auf regionaler Ebene variiert die Erhöhung in absoluten Zahlen zwischen den Polizeikonkordaten beachtlich. Das Polizeikonkordat Nordwestschweiz (PKNW)[66] verzeichnet die stärkste Bestandesaufstockung (+113 Ermittler und IT-Forensik-Spezialisten). Die Conférence latine des

[66] Das PKNW vereinigt die Kantonspolizeien Aargau, Basel-Landschaft, Basel-Stadt, Bern und Solothurn.

commandants des polices cantonales (CLCPC)[67] wird ihre zusätzlichen Bestände zur Bekämpfung der Cyberkriminalität in den nächsten zehn Jahren fast verdreifachen (+55,5 VZÄ gegenüber +30 in den letzten zehn Jahren). Allgemein wurden in den letzten zehn Jahren auf Konkordatsebene Anstrengungen unternommen, die auch in den kommenden zehn Jahren weitergeführt werden.
Stellt man die Anzahl neu geschaffener Ermittlerstellen der Zahl der 2022 registrierten Cyberdelikte gegenüber, so ist das Verhältnis unter den verschiedenen Konkordaten relativ stabil: Es variiert zwischen 133 Delikten pro neue Ermittlerstelle (PKNW) und 201 Delikten pro neue Ermittlerstelle (CLCPC). Vergleicht man die Anzahl Cyberdelikte pro Konkordat mit der Gesamtzahl neu geschaffener Stellen (sowohl Ermittler als auch IT-Forensik-Spezialisten), so sind die Resultate noch stabiler. Sie liegen zwischen 85 Delikten pro neue Ermittlerstelle (PKNW) und 95,9 Delikten pro neue Ermittlerstelle (Ostpol[68]).

Und auf Bundesebene? Die Ressourcen von fedpol zur Bekämpfung der Cyberkriminalität sind in den vergangenen zehn Jahren nicht erhöht worden. Seit 2020 führt fedpol pro Jahr rund zehn Verfahren in Zusammenhang mit Cyberkriminalität. Dabei werden Cyberermittlerinnen und Cyberermittler aus dem personellen Gesamtbestand der Abteilung Wirtschaftskriminalität diesen Ermittlungen zugeteilt, dies also zulasten anderer Aufträge der BA. Infolge der Annahme des Postulats 23.4349 am 28. Februar 2024 durch den Nationalrat werden die Ressourcen von fedpol, einschliesslich jener zur Bekämpfung von Cyberkriminalität, einer Überprüfung unterzogen.

3.2.4 Personal (StA)

- Die meisten kantonalen Staatsanwaltschaften verfügen über Staatsanwältinnen und Staatsanwälte, die teilweise oder ausschliesslich für die Bekämpfung von Cyberkriminalität zuständig sind. Eine Minderheit dieser Personen arbeitet in einer eigens dieser Thematik gewidmeten Einheit. Die Schaffung neuer Stellen variiert von Kanton zu Kanton stark. Die bisherige (+22) und die geplante (+18) Aufstockung von Stellen ist relativ hoch, konzentriert sich aber auf eine begrenzte Anzahl von Kantonen.

Die Mehrheit der kantonalen Staatsanwaltschaften verfügt über teilweise (14) oder ausschliesslich (6) auf die Behandlung von Cyberkriminalitätsfällen spezialisierte Staatsanwältinnen und Staatsanwälte. Sechs Staatsanwaltschaften haben keine auf diesen Bereich spezialisierte Staatsanwältinnen und Staatsanwälte.

Gemäss den Rückmeldungen der Kantone behandeln rund 40 Staatsanwältinnen und Staatsanwälte ausschliesslich (15) oder teilweise (25) Cyberkriminalitätsfälle. Diese werden von rund 30 Mitarbeitenden unterstützt. Sechs kantonale Staatsanwaltschaften verfügen über eine spezifische Einheit, die ausschliesslich für die Bekämpfung von Cyberkriminalität zuständig ist. Die Hälfte (20) der teilweise oder ausschliesslich auf die Bekämpfung der Cyberkriminalität spezialisierten Staatsanwältinnen und Staatsanwälte sowie die grosse Mehrheit des sie unterstützenden Personals (25) arbeiten in solchen Einheiten. Auf Ebene der kantonalen Staatsanwaltschaften befassen sich also rund 60 Personen ausschliesslich oder teilweise mit der Bekämpfung der Cyberkriminalität.

[67] Die CLCPC vereinigt die Kantonspolizeien Freiburg, Genf, Jura, Neuenburg, Waadt und Wallis.
[68] Das Ostschweizer Polizeikonkordat (Ostpol) vereinigt die Kantonspolizeien von Appenzell Ausserrhoden, Appenzell Innerrhoden, Glarus, Graubünden, Schaffhausen, St. Gallen und Thurgau, die Stadtpolizeien Chur und St. Gallen sowie die Landespolizei des Fürstentums Liechtenstein.

In den letzten zehn Jahren wurden in neun kantonalen Staatsanwaltschaften 22 zusätzliche Stellen zur Bekämpfung der Cyberkriminalität geschaffen. In den zehn kommenden Jahren sollen in sechs kantonalen Staatsanwaltschaften 18 zusätzliche Stellen geschaffen werden.

Und auf Bundesebene? Die Bundesanwaltschaft verfügt über einen Fachbereich für die Bekämpfung von Cyberkriminalität. Dieser besteht aus zwei Staatsanwälten, drei Assistenz-Staatsanwälten sowie einem Cyberreferenten. Diese sechs Personen wurden zwischen 2016 und 2023 angestellt.

3.2.5 Bearbeitung der Anzeigen

Neun Kantonspolizeien haben angegeben, nicht in der Lage zu sein, alle Anzeigen zu bearbeiten. Durchschnittlich können diese Polizeien 70 Prozent der eingegangenen Anzeigen behandeln. Zur Priorisierung der zu bearbeitenden Fälle werden verschiedene Kriterien herangezogen: der verursachte Schaden (materiell, finanziell, Reputation), die Art der betroffenen Infrastruktur (zum Beispiel kritische Infrastruktur), der Delikttyp (zum Beispiel ist bei einem Delikt einer Deliktserie die Chance grösser, dass es untersucht wird, sofern die Serie erkannt wird), die Erfolgschancen von Ermittlungen (die sich aus den Verbindungen ins Ausland, dem Vorhandensein forensischer Spuren, der raschen Anzeige des Delikts ergeben können) oder die Ermittlungsmassnahmen (zum Beispiel Sperrung von Vermögenswerten). Aufgrund dieser verschiedenen Kriterien werden gewisse Delikte, wie Ransomware-Angriffe (hoher Schaden) oder Online-Anlagebetrug (hoher Schaden und Deliktserien),

Die Praxis bei der Bearbeitung der Anzeigen ist sehr unterschiedlich. So haben gewisse Fachleute angegeben, dass eine Anzeige als bearbeitet gelten kann, wenn sie in der Polizeidatenbank erfasst worden ist. Sehr viele Kantone haben angegeben, 100 Prozent der Anzeigen zu bearbeiten, was folglich nicht heisst, dass für jede dieser Anzeigen tatsächlich Ermittlungen erfolgen.

prioritär behandelt.

Als Gründe, warum nicht alle Anzeigen bearbeitet werden können, geben alle neun Kantonspolizeien den Mangel an Ermittlerinnen und Ermittlern an, zwei Drittel erwähnen den Mangel an weiteren personellen Mitteln (Analytikerinnen, IT-Forensik-Spezialisten), etwa die Hälfte führt ausserdem fehlende technische Mittel oder qualitativ ungenügende Anzeigen an.

3.2.6 Personalrekrutierung

- Die meisten Kantonspolizeien sind mit Rekrutierungsschwierigkeiten konfrontiert, ob für IT-Fachleute oder Cyberermittlerinnen und Cyberermittler. Diese Schwierigkeiten sind auf zahlreiche Gründe zurückzuführen, und die meisten Polizeien setzen Massnahmen um, um diesen zu begegnen, namentlich über die Weiterbildung.

18 Kantonspolizeien haben angegeben, bei der Rekrutierung von qualifiziertem Personal mit Schwierigkeiten zu kämpfen. Besonders akut sind diese Schwierigkeiten bei den IT-Forensik-Spezialistinnen und -Spezialisten, relativ hoch aber auch bei den Cyberanalystinnen und den Ermittlern. Verschiedene Faktoren erklären diese Schwierigkeiten.
Zunächst einmal stagnieren in einigen Kantonen die Bewerbungen von Polizeiaspirantinnen und -aspiranten oder gehen gar zurück.[69] Kann Personal rekrutiert werden, muss es auch gelingen, dieses zu halten. Ausgebildetes Personal stellt für den ausbildenden Kanton eine beachtliche Investition dar – welche nicht amortisiert wird, wenn Personen zu einem anderen Polizeikorps wechseln oder den

[69] Face à la pénurie de main d'oeuvre, les polices romandes peinent à susciter des vocations - rts.ch - Régions

Polizeiberuf ganz aufgeben. Für das ausgebildete Personal kann es auch desillusionierend sein, wenn die Verfahren im Bereich Cyberkriminalität, häufig gegen Unbekannt, nur selten zu einer Verurteilung führen.

Um den Rekrutierungsproblemen zu begegnen, stehen den Kantonspolizeien verschiedene Lösungsansätze zur Verfügung. Zunächst gilt es, bestehendes, aber nicht spezialisiertes Personal zu nutzen. Dieses kann mehr oder weniger intensiv zu Cyberkriminalität ausgebildet werden. Ermittlerinnen und Ermittler können im Kurs Cyber II des SPI die unerlässlichen Grundkenntnisse für Ermittlungen gegen Cyberkriminalität erlernen. In der Schweiz wie auch im Ausland gibt es ausserdem weitere Ausbildungen für eine tiefergreifende Ausbildung von Ermittlern, Kriminalanalytikerinnen oder auch IT-Forensik-Spezialisten. Es gilt jedoch nicht nur Spezialistinnen und Spezialisten auszubilden. Sämtliche Polizeiangehörigen sind mit den Grundkenntnissen zur Bekämpfung von Cyberkriminalität auszustatten. Damit sind sie in der Lage, die jeweils geeignetsten Massnahmen zu treffen (zum Beispiel bei der Entgegennahme einer Anzeige die richtigen Fragen zu stellen) und so die Spezialistinnen und Spezialisten zu entlasten.

In Sachen Personalbindung müssen die Kantone manchmal kreativ sein. Die Kantonspolizeien gewisser Kantone können in Sachen Lohn nicht mit anderen Kantonen oder Privatunternehmen konkurrenzieren. Besonders akut stellt sich dieses Problem bei den IT-Forensik-Spezialistinnen und -Spezialisten, deren Kompetenzen auch in der Privatwirtschaft sehr gesucht sind. Daher müssen andere Faktoren in den Vordergrund gestellt werden, zum Beispiel den öffentlichen Auftrag, attraktive Weiterbildungsmöglichkeiten oder Arbeitsbedingungen, die den Erwartungen entsprechen.

Trotz dieser Massnahmen muss jedoch auch neues Personal rekrutiert werden, um die Abgänge zu kompensieren und der Zunahme der Cyberkriminalität etwas entgegenzusetzen. Wie in Ziffer 3.2.3 aufgezeigt, sind in den letzten zehn Jahren Stellen geschaffen worden, und auch in den kommenden zehn Jahren werden zahlreiche Stellen zu besetzen sein. Dazu müssen entsprechende Rekrutierungskampagnen umgesetzt werden. Die Rekrutierung von jungen Personen kann durch das Anbieten von Praktika oder Aufnahme von Personen in einer berufsbegleitenden Ausbildung begünstigt werden. Damit erhalten sie Einblick in die Polizeiwelt und können, wenn eine passende Stelle offen ist, später definitiv in diese aufgenommen werden. Eine weitere Möglichkeit ist, Spezialistinnen und Spezialisten mit seltenen technischen Kompetenzen zu rekrutieren, die nicht über den Fachausweis als Polizistin oder Polizist verfügen. In diesem Fall ist entscheidend, ihnen die nötige Ausbildung zu bieten, damit sie in den Polizeiberuf einsteigen können. Schliesslich kann auch sein, dass für gewisse sehr spezifische Kompetenzen das gesuchte Profil auf dem Arbeitsmarkt schlicht nicht verfügbar ist oder dass die Ausbildung bestehenden Personals nicht realistisch ist. In diesem Fall sind die bestehenden Möglichkeiten der Zusammenarbeit auf regionaler und nationaler Ebene zu prüfen – zum Beispiel über die Amtshilfe. In gewissen, eng abgegrenzten Fällen ist auch der Beizug von privaten Leistungserbringern eine gute Option. Zum Beispiel könnten punktuell Aufträge an Unternehmen für Cybersicherheit vergeben werden, die über sehr hohe technische Kompetenzen verfügen.

3.3 Technische Mittel

- Die meisten Kantonspolizeien verfügen über die notwendigen technischen Mittel für eine wirksame Bekämpfung der Cyberkriminalität. Allerdings muss häufig evaluiert werden, ob die verwendete Software noch adäquat ist. Auch ist sicherzustellen, dass zahlenmässig ausreichend sachkundiges Personal vorhanden ist.

Für die kriminalpolizeilichen Einheiten, die mit der Bekämpfung der Cyberkriminalität beauftragt sind, sind die technischen Mittel ein unabdingbares Hilfsmittel. Eine Mehrheit der Kantonspolizeien verfügt über Software für die Analyse von Geldflüssen in Kryptowährungen (15), Netzwerkanalysen (16) und

die Erkennung von serieller Online-Kriminalität (15). Eine Minderheit der Kantonspolizeien verfügt über Mittel, welche die Sperrung von Vermögenswerten erleichtern (11) oder mit denen eine Internetüberwachung vorgenommen werden kann – zum Beispiel von sozialen Netzwerken oder des Darkweb (9). Einige Kantonspolizeien geben an, keine solchen Tools zu besitzen, aber über Vereinbarungen mit anderen Polizeikorps indirekt Zugang dazu zu haben.

Dennoch lässt sich auch mit diesen Tools die Täterschaft nicht einfach mit einem Klick finden. Ihre Verwendung erleichtert den Ermittlerinnen und Ermittlern zwar die Arbeit, erfordert aber auch Spezialkenntnisse und generiert Arbeit. Ebenso sind für die Nutzung solcher Tools im Terrain, zum Beispiel während einer Hausdurchsuchung, spezialisierte Ressourcen nötig.[70]

Produkte im Bereich Kryptowährungen ermöglichen namentlich, Geldflüsse zu verfolgen (aber nicht zu stoppen), und können Ermittlerinnen und Ermittlern helfen, die Täterschaft zu identifizieren. Allerdings funktionieren diese Produkte mit Lizenzmodellen, die erstens teuer sind und zweitens nicht alle Kryptowährungen abdecken. Bei der Bekämpfung von Pädokriminalität oder auch Betäubungsmittelhandel sind Monitoring-Tools für die Überwachung des Darknet oder etwa von Peer-to-Peer-Austauschplattformen eine wertvolle Hilfe.

In den kommenden Jahren dürfte sich die Situation weiter verbessern: Einige Kantonspolizeien, die derzeit noch nicht über bestimmte technische Produkte verfügen, werden diese beschaffen. Eine grosse Mehrheit der Kantonspolizeien wird dann über die technischen Mittel verfügen, welche die Nachverfolgung von Geldflüssen in Kryptowährungen, die Identifikation von serieller Online-Kriminalität oder eine Internetüberwachung erlauben. Allerdings sind viele Kantone (10) der Auffassung, dass es zurzeit an einem wirksamen und benutzerfreundlichen Mittel für die Beschaffung von Informationen in offenen Quellen (OSINT) fehlt, sei es im Clear- oder im Darkweb. Ein solches Mittel wäre in der überwiegenden Mehrheit der Ermittlungen ein Mehrwert. Zu bedenken ist allerdings, dass Investitionen in neue technische Mittel ihre Wirksamkeit nur entfalten können, wenn gleichzeitig in personelle Ressourcen investiert wird.

3.4 Ausbildung

- ❖ In der Schweiz gibt es heute zahlreiche Ausbildungen, die ganz oder teilweise der Bekämpfung der Cyberkriminalität gewidmet sind. Diverse Akteure bieten Ausbildungen an (SPI, NEDIK, Kantonspolizeien, Universitäten und Hochschulen, Privatsektor). Gewisse Themen werden jedoch nicht oder kaum abgedeckt.

Eine grosse Mehrheit der Kantonspolizeien hat interne Ausbildungen rund um die Bekämpfung von Cyberkriminalität entwickelt. Diese gehen von allgemeinen Themen (Einführung in die Cyberkriminalität) bis zu sehr spezifischen Themen wie Kryptowährungen, OSINT, Darknet oder Metaverse. Auch NEDIK bietet Fachausbildungen an, die von den Teilnehmenden sehr geschätzt werden. Einige würden es begrüssen, wenn die Leistungen von NEDIK im Ausbildungsbereich ausgebaut würden.

Das SPI hat ein E-Learning entwickelt, das von allen Polizeiaspirantinnen und Polizeiaspiranten im Rahmen der Polizeischule absolviert wird (18 796 Mal[71] wurde der Abschlusstest bestanden). Einige Teilnehmende sind der Meinung, dass alle Polizistinnen und Polizisten das E-Learning nochmals absolvieren sollten, besonders wenn es inhaltlich aktualisiert wurde. Auch wird gewünscht, dass die Grundausbildung zum Thema Cyberkriminalität ab der Polizeischule stärker vertieft und vereinheitlicht wird. Das SPI hat ausserdem einen Fachkurs für Ermittlerinnen und Ermittler entwickelt, den Kurs

[70] Siehe hierzu auch KGGT-Bericht, Ziff. 7.4.1.
[71] März 2023

Cyber II, der sich an interessierte Angehörige der Kriminalpolizei richtet. Seit es ihn gibt, haben den Kurs laut Auskunft des SPI 841[72] Teilnehmende abgeschlossen.

Die grosse Mehrheit der Umfrageteilnehmenden hält die Ausbildungen des SPI im Cyberbereich für ausreichend.[73] Gleichzeitig wird aber gewünscht, dass das SPI seine Ausbildungen hauptsächlich in den folgenden Bereichen vertieft: OSINT, verdeckte Fahndung im Internet, Kryptowährungen, Prävention, Malware-Analyse, verschlüsselte Kommunikationsmittel, Analyse von Massendaten, Cyberphänomene. Mehrere Teilnehmende weisen darauf hin, dass der Kurs Cyber II für einen Inspektor der Kriminalpolizei ausreichend ist, nicht aber für einen auf Cyberkriminalität spezialisierten Ermittler.

Hierfür bieten verschiedene Universitäten «Certificate of Advanced Studies» (CAS) oder «Master of Advanced Studies» (MAS) an, die als inoffizielle Weiterführung der Ausbildung des SPI fungieren. Die Schweizer Ausbildungen sind auf der Plattform cyberpie.ch erfasst.[74] Angesichts der rasanten Entwicklungen in der Cyberkriminalität wird angeregt, dass das SPI mit den Hochschulen und Universitäten zusammenspannt, um ein Weiterbildungsprogramm anzubieten, welches auf dem Kurs Cyber II aufbaut. Auch wird vorgeschlagen, einen MAS ausschliesslich für Strafverfolgungsbehörden zu schaffen, der mehrere bestehende CAS zusammenfassen würde. Dieser MAS entspräche dem höchsten Spezialisierungsniveau.

Zahlreiche Teilnehmende geben an, an Universitäten im Ausland Ausbildungen zu besuchen. Dabei handelt es sich in vielen Fällen um MAS. Angesichts des Fehlens von MAS in der Schweiz erscheint dies logisch, ausserdem sind gewisse ausländische Universitäten (namentlich Dublin) in diesem Bereich Vorreiter. Über diese Ausbildungen hinaus gibt es auch punktuelle Webinare internationaler Organisationen (Interpol, Europol, CEPOL). Zudem bieten gewisse Unternehmen ihren Kunden spezifische Schulungen zur Nutzung ihrer Software.

Bei den Staatsanwaltschaften hat lediglich eine Minderheit interne Ausbildungen entwickelt. Allerdings scheinen die Staatsanwaltschaften stärker auf regionale Strukturen abzustützen (Kurse der Staatsanwaltsakademie[75] oder der Ecole romande de la magistrature pénale[76]). Die Staatsanwaltschaften weisen darauf hin, dass es in der Schweiz nicht genügend an sie gerichtete Ausbildungen gibt. Sie würden die Schaffung eines Kurses vom Typ Cyber II für Staatsanwältinnen und Staatsanwälte begrüssen. Einige geben ferner an, Kurse zu besuchen, die sich an Polizeiangehörige richten.

3.5 Prävention

- Sämtliche Polizeien setzen Präventionsmassnahmen um. Dennoch sind es schlichtweg zu wenige, um der Zunahme der Cyberkriminalität die Stirn zu bieten. Die Präventionsmassnahmen müssen in allen Themenbereichen verstärkt werden und die ganze Bevölkerung ansprechen. Die Kantonspolizeien sind sich dieser Situation bewusst, und die Mehrheit von ihnen wird ihre Präventionsanstrengungen zur Bekämpfung der Cyberkriminalität in den kommenden Jahren verstärken.

Sämtliche Kantonspolizeien haben in den letzten fünf Jahren Präventionsmassnahmen zum Thema Cyberkriminalität umgesetzt. Ebenso haben sämtliche Kantonspolizeien an von der Schweizerischen

[72] März 2023
[73] 27 Stellen gaben an, eher einverstanden, einverstanden oder völlig einverstanden zu sein. 9 Stellen waren eher nicht einverstanden, nicht einverstanden oder überhaupt nicht einverstanden.
[74] Diese Plattform ist das Ergebnis eines Projektes der Arbeitsgruppe Cyberausbildung der KKPKS. Bis anhin sind 22 Ausbildungen aufgeführt.
[75] Home (staatsanwaltsakademie.ch)
[76] École romande de la magistrature pénale (ERMP) - Haute-Ecole Arc (he-arc.ch)

Kriminalprävention organisierten Massnahmen mitgewirkt. Eine Minderheit von Kantonen hat sich an Aktionen beteiligt, die von anderen öffentlichen oder privaten Akteuren organisiert wurden.

Die Mehrheit der Befragten (43/69) ist allerdings der Ansicht, dass die heutigen Präventionsmassnahmen nicht ausreichen.[77] Eine Mehrheit ist der Meinung, dass die Massnahmen in fast allen Themenbereichen verstärkt werden müssen; zugleich ist nur eine sehr kleine Minderheit der Auffassung, dass die falschen Themen angegangen werden. Vor allem in den Bereichen Online-Anlagebetrug, Betrug auf Kleinanzeigenplattformen und Money Mules sollen die Anstrengungen verstärkt werden.[78]

Auch wird betont, dass die Präventionsmassnahmen quantitativ nicht ausreichen, zu wenig koordiniert sind und nicht die richtigen Zielgruppen erreichen. Diesbezüglich spricht sich die grosse Mehrheit der befragten Behörden dafür aus, dass die Prävention bei der gesamten Bevölkerung intensiviert wird, mit einem besonderen Fokus auf die über 65-Jährigen. Eine antwortende Person merkt an: Wer noch nie Opfer von Cyberkriminalität geworden sei, fühle sich nicht betroffen. Dies ist zum Beispiel bei vielen KMU der Fall, die sich zwar der Risiken bewusst sind, aber keine Massnahmen zu deren Eindämmung ergreifen. Cyberkriminalität nimmt stark zu – daher müssen auch die Präventionsanstrengungen zunehmen und ausserdem sehr rasch auf neue Tatvorgehen angepasst werden.

Anzumerken ist allerdings, dass die tatsächliche Wirkung von Präventionskampagnen immer schwierig einzuschätzen ist. Auch wenn die Präventionsmassnahmen verstärkt werden, wird es alles andere als einfach sein, Indikatoren zu haben, die deren Einfluss auf die polizeilichen Kriminalstatistiken belegen.

3.6 Ressourcenbündelung

- ❖ Fast die Gesamtheit der Befragten hält eine Ressourcenbündelung zur Bekämpfung der Cyberkriminalität für wünschenswert. Jedoch besteht kein Konsens darüber, wie diese umgesetzt werden soll. Generell sehr geschätzt wird die Arbeit von Stellen, die für die ganze Schweiz Leistungen erbringen, wie NEDIK, Cyber-CASE, BACS oder auch fedpol.

Fast sämtliche Befragten sind sich darin einig, dass eine Ressourcenbündelung zur Bekämpfung der Cyberkriminalität wünschenswert wäre.[79] Die Mehrheit vertritt die Auffassung, dass die Ressourcen in fast allen Bereichen gebündelt werden sollten, mit Ausnahme der Doktrin. Bevorzugt zu berücksichtigen sind die Bereiche technische Mittel, Ausbildung und Prävention. Was die Ausbildung und die Prävention anbelangt, bestehen bereits nationale Strukturen (SPI, SKP), die das Bedürfnis nach einer Ressourcenbündelung erfüllen. Die Bündelung von technischen Mitteln erfolgt über andere Stellen (NEDIK, fedpol, PTI).

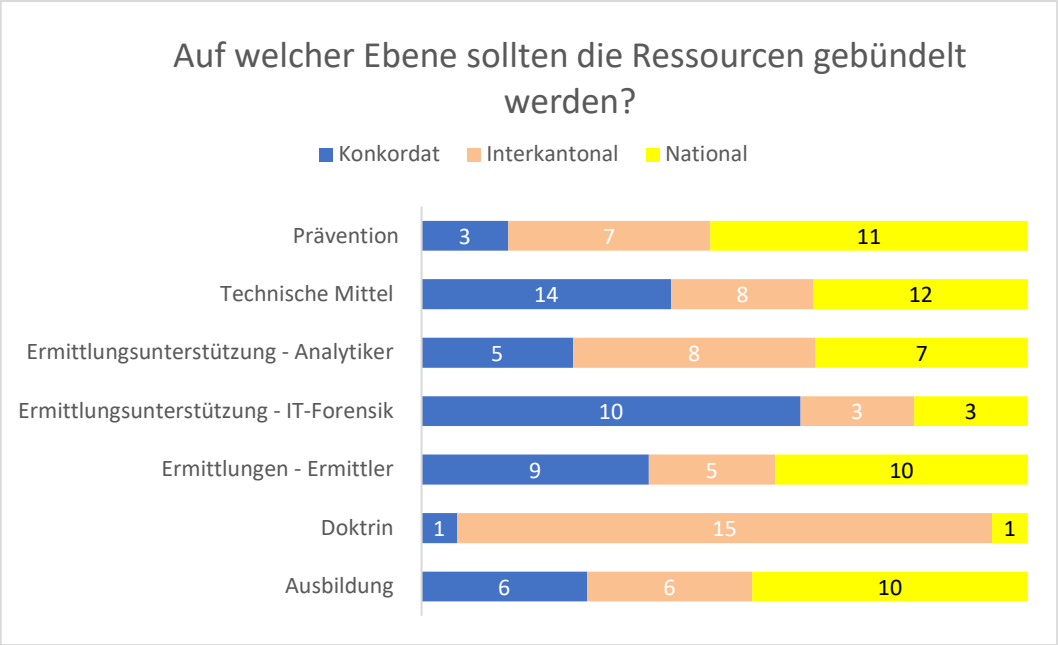
Laut den Teilnehmenden sollten auch die personellen Mittel in den Bereichen Ermittlungen, IT-Forensik und Kriminalanalyse gebündelt werden. Im Ermittlungsbereich wäre eine Bündelung aber nicht ganz einfach, weil in jedem Einzelfall Gerichtsbarkeitsfragen zu klären wären. Mehrere Teilnehmende erwähnten die Möglichkeit einer partiellen oder vollständigen Übertragung der Strafverfolgungskompetenzen im Bereich der Cyberkriminalität an den Bund.

[77] Die zu bewertende Aussage lautete: «Die heutigen Präventionsmassnahmen im Bereich Cyberkriminalität sind ausreichend.» Sie wurde den Kantonspolizeien, den Staatsanwaltschaften sowie den Gerichten vorgelegt. Im Detail sind 43 Teilnehmende mit dieser Aussage nicht einverstanden (5 überhaupt nicht einverstanden; 15 nicht einverstanden; 22 eher nicht einverstanden) und 26 Teilnehmende einverstanden (1 völlig einverstanden, 5 einverstanden, 22 eher einverstanden).

[78] Auf die Aussage «Es braucht mehr Präventionsmassnahmen in den folgenden Bereichen» lauteten die Antworten: Online-Anlagebetrug (72 %), Gefälschte Inserate (63 %), Money-Mules (58 %), Romance-Scam (55 %), IT-Hygiene (55 %), andere Arten von Cyberbetrug (50 %), Kinderpornografie im Internet (45 %), Hassrede im Netz (42 %).

[79] Auf die Aussage «Es ist erstrebenswert, zur Bekämpfung der Cyberkriminalität die Ressourcen zu bündeln» lauteten die Antworten: völlig einverstanden 50 %, einverstanden 27 %, eher einverstanden 19 %, eher nicht einverstanden 2,5 %, nicht einverstanden 1,5 %.

Auch wenn über die Notwendigkeit einer Ressourcenbündelung Konsens besteht, sind die Positionen bezüglich der Frage, auf welcher Stufe diese erfolgen soll, viel weniger klar. Bei der IT-Forensik spricht sich die Mehrheit der Befragten für eine Bündelung auf Konkordatsebene aus. Bei der Prävention hingegen sollte die Ressourcenbündelung nach Ansicht einer Mehrheit der Befragten auf nationaler Ebene stattfinden, während bei der Doktrin wiederum die Ressourcen gemäss einer grossen Mehrheit der Befragten auf interkantonaler Ebene gebündelt werden sollten.



Acht Kantonspolizeien gaben an, personelle Ressourcen im Bereich der Bekämpfung der Cyberkriminalität zu bündeln. Hingegen hat keine Kantonspolizei angegeben, künftig eine Bündelung zusätzlicher Ressourcen zu planen. Die Ressourcenbündelung scheint insbesondere im Rahmen des Zuger IT-Forensik-Kompetenzzentrums zu erfolgen, das für die Kantone Zug, Schwyz, Nidwalden, Obwalden sowie Uri Leistungen erbringt.[80] Ebenso bietet das Kompetenzzentrum Forensik des Kantons St. Gallen[81] seine Leistungen allen Kantonen des Ostpol-Konkordats an.[82] Gewisse Mittel werden auch im RC3 Romandie (mit Sitz in Genf) gebündelt, wo mit einem vom Konkordat RBT finanzierten VZÄ das operative Dispositiv PICSEL betreut wird. Auch das RC3 erbringt Leistungen für alle Westschweizer Kantone, namentlich bei der Einführung von Spezialsoftware, der forensischen Analyse der Bord-IT von Fahrzeugen sowie im Bereich der Bekämpfung von Pädokriminalität. Ausserhalb dieser drei Strukturen erfolgt die Ressourcenbündelung in Zusammenhang mit Cyberkriminalität hauptsächlich in interkantonalen Strukturen wie NEDIK, der SKP[83] und dem SPI[84] (siehe im Folgenden). Obwohl der Kanton Zürich keinem Konkordat angehört, fördert er die regionale Zusammenarbeit und unterstützt die anderen Kantone auf Anfrage.

Bei den technischen Mitteln wird eine Ressourcenbündelung begrüsst, weil sich damit Lizenzkosten für gewisse IT-Produkte reduzieren lassen. Eine grosse Mehrheit der Kantonspolizeien bündelt daher bereits technische Mittel auf Konkordats- oder interkantonaler Ebene oder plant, dies zu tun. So wurde auf Initiative von NEDIK für die ganze Schweiz ein Einheitspreis – der tiefer ist als die vorherigen Tarife – für eine Software zur Analyse von Kryptowährungen definiert. Die Bündelung kann auch bis zur Verwendung gemeinsamer Software wie PICSEL gehen, die mittlerweile von neun Kantonen eingesetzt

[80] IT-Forensik Kompetenzzentrum (zg.ch)
[81] Forensik | sg.ch
[82] Ausser St. Gallen: Appenzell Ausserrhoden, Appenzell Innerrhoden, Glarus, Graubünden, Schaffhausen, Thurgau sowie das Fürstentum Liechtenstein.
[83] Die SKP wird über Kantons- und Bundesbeiträge finanziert.
[84] Das SPI erhält Subventionen von den Kantonen und vom Bund.

wird. Die Zurverfügungstellung von intern entwickelten Tools ist eine weitere Form der Ressourcenbündelung. Hier geht die Luzerner Kantonspolizei mit gutem Beispiel voran, die bereits mehrere Softwareprogramme zur Verfügung gestellt hat.

3.6.1 NEDIK

Über NEDIK werden rund 5,5 VZÄ[85] finanziert, die Aufgaben für die ganze Schweiz erbringen. Die Kantonspolizei Zürich stellt die nationale Koordination auf strategischer und operativer Stufe sicher (2 VZÄ), die Kantonspolizei Bern die nationale Koordination für das Monitoring von Peer-to-Peer-Netzwerken im Rahmen der Bekämpfung von Online-Pädokriminalität (2 VZÄ).[86] Die Kantonspolizei St. Gallen stellt das Wissensmanagement (0,5 VZÄ) und die Kantonspolizei Genf die Steuerung von PICSEL auf nationaler Ebene sicher (1 VZÄ). Ausserdem stehen zusätzliche Gelder für verschiedene Leistungen zur Verfügung, wie Softwarebeschaffungen, Projektmanagement oder die Organisation von Ausbildungen.

Die meisten Befragten erachten die Leistungen von NEDIK als zufriedenstellend.[87] Für eine grosse Mehrheit von ihnen bietet NEDIK einen Mehrwert in den Bereichen der Vernetzung und des Wissenstransfers. Eine Mehrheit sieht bei der operativen Koordination einen Mehrwert von NEDIK, eine Minderheit ausserdem bei der strategischen Koordination sowie der Ausbildung und eine kleine Minderheit in den Bereichen Unité de doctrine und Kriminalanalyse.

Verbesserungspotenzial ist vor allem bei der operativen Koordination auszumachen. Dies ist der einzige Bereich, in dem NEDIK nach Ansicht einer Mehrheit der Umfrageteilnehmenden verbessert werden könnte. Konkret würden sich die Teilnehmenden wünschen, dass NEDIK Ermittlungen koordiniert, namentlich für das Phänomen Ransomware.[88] Ebenso wäre erwünscht, dass NEDIK dabei unterstützt, Serien vor Gericht zu bringen, indem es sich über das Cyber-CASE (siehe unten) mit den Staatsanwaltschaften koordiniert. Im Bereich der strategischen Koordination würde eine Koordination mit den Staatsanwaltschaften ebenfalls begrüsst; einige der Befragten wünschen sich eine gemeinsame (Cyber-)Kriminalpolitik von NEDIK und Cyberboard. Schliesslich äusserten mehrere Umfrageteilnehmende den Wunsch, dass NEDIK im Namen der Kantone die Preise für die Anschaffung von gewissen Lizenzen oder Spezialgeräten verhandelt – was zum Teil bereits der Fall ist.

Verschiedene Faktoren schränken diese Verbesserungspotenziale jedoch ein. So merkt ein Teilnehmer an, dass NEDIK in Ermangelung eigentlicher regionaler Cyberkompetenzzentren nicht als «Netzwerk der Netzwerke» fungieren kann und somit nicht seinen maximalen Mehrwert erreichen kann. Die NEDIK zugeteilten Mittel sollten ausserdem neu evaluiert werden; ein Teilnehmer betont, dass für die Leitung von NEDIK eine Vollzeitstelle vorgesehen werden sollte.

3.6.2 Cyber-CASE

Das Cyber-CASE ist in erster Linie ein Instrument für die Staatsanwaltschaften, jedoch nehmen auch rund zehn Kantonspolizeien an den Sitzungen teil. Eine grosse Mehrheit der Teilnehmenden erachtet die Leistungen des Cyber-CASE als zufriedenstellend.[89] Besonders anerkannt ist dessen Rolle beim Wissenstransfer und bei der Vernetzung. Zahlreiche Teilnehmende betonen den Mehrwert, den es für sie hat, mit ihresgleichen zusammenzukommen, Fälle zu diskutieren oder auch Präsentationen zu verschiedenen Aspekten der Cyberkriminalität zu erhalten.

[85] Die finanziellen Mittel werden von KKJPD und KKPKS gewährt. Die KKPKS fungiert als Auftraggeber von NEDIK.
[86] Für weitere Informationen zu diesem Thema siehe den Bericht des Bundesrates in Erfüllung der Postulate Feri-Regazzi.
[87] Auf die Aussage «Die Dienstleistungen von NEDIK sind zufriedenstellend» lauteten die Antworten wie folgt (N = 26): völlig einverstanden 11 %, einverstanden 27 %, eher einverstanden 27 %, eher nicht einverstanden 23 %, nicht einverstanden 8 %, überhaupt nicht einverstanden 2 %.
[88] NEDIK kann keine Ermittlungen führen, nur die Koordination gewährleisten, indem es den Informationsaustausch sicherstellt.
[89] Auf die Aussage «Die Dienstleistungen des Cyber-CASE sind zufriedenstellend» lauteten die Antworten wie folgt (N = 37): völlig einverstanden 5,5 %, einverstanden 48,5 %, eher einverstanden 35,5 %, eher nicht einverstanden 3 %, nicht einverstanden 5,5 %, überhaupt nicht einverstanden 3 %.

Lediglich eine Minderheit der Teilnehmenden ist der Auffassung, dass das Cyber-CASE im Bereich der operativen Koordination einen Mehrwert bringt (Festlegung des Gerichtsstands, Falldiskussionen). Eine Mehrheit wünscht denn auch, dass das Cyber-CASE seine Tätigkeit in diesem Bereich verstärkt. Namentlich wird gewünscht, dass es in der frühzeitigen Erkennung von Serien mit derselben Täterschaft aktiver wird, um deren Übernahme durch eine einzige Behörde zu erleichtern und somit Doppelspurigkeiten bei den Ermittlungen zu vermeiden. Es wird darauf hingewiesen, dass das Cyber-CASE über eine Liste der laufenden Fälle verfügt, die von den Kantonen aber zu selten aktualisiert wird. Eine Stärkung des Cyber-CASE auf operativer Stufe gelingt nur, wenn die kantonalen Staatsanwaltschaften und die Polizeien Fallserien melden (beispielsweise über NEDIK).

Einige Teilnehmende möchten zudem, dass das Cyber-CASE seine strategische Tätigkeit verstärkt, namentlich durch eine Sensibilisierung von Politikerinnen und Politikern oder durch Anregen von Gesetzesänderungen, welche die Bekämpfung der Cyberkriminalität erleichtern würde.

3.6.3 BACS

Eine wichtige Rolle kommt auch der Zusammenarbeit mit dem BACS zu. Diese betrifft im Wesentlichen zwei Bereiche: die Prävention und das technische Know-how. Bei Ersterer wird vor allem die Prävention, die sich an KMU und die Bevölkerung richten, hervorgehoben. Die Teilnehmenden weisen auch darauf hin, dass die Aufgabenteilung zwischen dem BACS und den Polizeien in Sachen Prävention verbessert werden sollte.

Die Meldeplattform des BACS und die wöchentlichen Informationsbulletins, die daraus hervorgehen, haben auch für die Strafverfolgungsbehörden einen Mehrwert. Einige Teilnehmende würden es begrüssen, wenn das BACS über die gesetzlichen Grundlagen verfügen würde, die ihm die Zusammenarbeit mit den Strafverfolgungsbehörden erleichtern würden. Eine Meldepflicht des BACS an die Strafverfolgungsbehörden im Falle eines Angriffs auf kritische Infrastrukturen ist ein Beispiel, das genannt wird. Auf technischer Ebene werden die Kompetenzen des BACS geschätzt, die sich namentlich auf die Informationsplattform zu Malware (PolMISP) sowie auf die punktuelle Unterstützung im Rahmen von Ermittlungen (zum Beispiel bei der forensischen Analyse von Malware) konzentrieren.

3.6.4 fedpol

Die meisten Befragten beurteilen die Leistungen von fedpol in der internationalen Koordination als zufriedenstellend.[90] Einige sind der Meinung, dass fedpol mehr Dienstleistungen in Zusammenhang mit seiner Rolle als Zentralstelle anbieten müsste, namentlich in Verbindung mit dem Ausland. Auch wird gewünscht, dass der Informationsaustausch mit dem Ausland verbessert wird, beispielsweise über den Erhalt von Analyseprodukten anderer Länder oder internationaler Organisationen.

Die grosse Mehrheit der Befragten ist auch der Meinung, dass die Schweiz ihre Präsenz bei den internationalen Organisationen verstärken sollte, um die Bekämpfung der Cyberkriminalität zu verbessern. Diese Leistung könnte beispielsweise durch die Entsendung von Polizeiattachés in die Herkunftsregionen der Täter gestärkt werden.

3.6.5 Analyseprodukte

Die Vielzahl der herausgegebenen Analyseprodukte widerspiegelt die Komplexität der Cyberkriminalität und des Föderalismus. NEDIK veröffentlicht zwei Produkte: ein monatliches Bulletin, welches die

[90] Auf die Aussage «Die Leistungen von fedpol im Bereich der internationalen Koordination (Zentralstelle Cyber, Verbindungsbüro bei Europol, Polizeiattachés) sind zufriedenstellend» fielen die Antworten wie folgt aus (N = 28): völlig einverstanden: 10,5 %, einverstanden 35,5 %, eher einverstanden 20,5 %, eher nicht einverstanden 27,5 %, keine Antwort 7 %.

aktuellen Tendenzen beleuchtet und gewisse Fälle kommentiert, sowie ein monatliches Bulletin spezifisch zum Online-Anlagebetrug (PICSEL OAB). Letzteres beruht auf der nationalen Nutzung von in PICSEL erfassten Daten im Rahmen eines Pilotprojekts.[91]
Sämtliche in PICSEL erfassten Daten sind ausserdem Gegenstand eines monatlichen Bulletins, das die Statistiken und besondere Fälle präsentiert. Dieses Bulletin reflektiert natürlich lediglich die Daten der neun an PICSEL beteiligten Kantone. Das BACS publiziert ein wöchentliches Bulletin, das die über seine Meldeplattform eingegangenen Informationen präsentiert und analysiert. Ausserdem wird auf interessante Fälle hingewiesen. Schliesslich publiziert fedpol pro Jahr mehrere Berichte zu aktuellen Themen (Kryptowährungen, Metaverse, künstliche Intelligenz). Alle erwähnten Produkte sind auf einer Plattform von NEDIK verfügbar. Auch die Berichte von Europol werden dort abgelegt. Eine grosse Mehrheit der Teilnehmenden ist der Ansicht, dass diese Produkte für ihre Arbeit einen Mehrwert bedeuten. Als hauptsächliche Verbesserungsmöglichkeit wird die Reduktion der Anzahl Produkte angeführt. Die Teilnehmenden betonen ausserdem, dass mehr operative Informationen geteilt werden sollten, nach dem Beispiel der PICSEL-Bulletins, und dies auch regelmässiger. Die Mehrheit der Teilnehmenden wünscht sich, dass ein solches Produkt auf interkantonaler Ebene herausgegeben wird.

4 Analyse der Stärken und Schwächen des heutigen Systems

In der Umfrage wurden die Teilnehmenden gebeten, sich zu den Stärken und Schwächen der Organisation der Schweiz im Bereich der Bekämpfung von Cyberkriminalität zu äussern. Ihre Rückmeldungen sind in diesem Kapitel zusammengefasst.

4.1 Stärken

- Die Teilnehmenden betonen, dass die Schweiz sich bei der Bekämpfung der Cyberkriminalität auf zahlreiche Erfolgsfaktoren abstützen kann: Genannt werden unter anderem gut ausgebildete Fachleute, ein formelles und informelles Netzwerk von Expertinnen und Experten, die sich persönlich kennen, die Solidarität unter den Kantonen oder auch die im internationalen Vergleich beachtlichen finanziellen Mittel.

Eine der grössten Stärken ist der Faktor Mensch. Das Personal ist hochengagiert und das generelle Ausbildungsniveau – einschliesslich im Bereich von Strafverfahren – sowie die Sprachkenntnisse sind unverkennbare Vorteile. Die Ausbildung im Bereich Cyberkriminalität wird immer besser, und es gibt immer mehr Ausbildungsmöglichkeiten, um sich zu spezialisieren. Auch ist das Spezialisierungsniveau sehr hoch, gewisse Einheiten verfügen über ausgewiesene Spezialistinnen und Spezialisten im Ermittlungs- wie auch im IT-Bereich. Das informelle Netzwerk, das diese Fachleute bilden, erleichtert den Wissens- und Erfahrungsaustausch enorm. Angesichts der geografischen Nähe kennen sich die Fachleute persönlich, was die direkte, unbürokratische Zusammenarbeit über Kantonsgrenzen hinaus vereinfacht.

Diese Zusammenarbeit ist eine logische Folge des Föderalismus im Polizeibereich. Jener ist in einem so transnationalen Bereich wie der Cyberkriminalität zwar ein Hindernis, bietet aber auch Vorteile. Die vielfältigen Herangehensweisen der Kantone sind bereichernd, ermöglichen den Ideenaustausch und ebnen neuen Ermittlungsansätzen den Weg. Föderalismus heisst nicht «jeder für sich». So erwähnen einige Kantone, dass die «grossen» Kantone die «kleinen» bereitwillig unterstützen. Der Kanton Zürich

[91] PICSEL und PICSEL OAB sind nicht zu verwechseln. Mit PICSEL werden alle Phänomene der Cyberkriminalität analysiert, allerdings ist lediglich eine Minderheit der Kantone am Dispositiv beteiligt. PICSEL OAB hingegen ist ein Pilotprojekt rund um die Analyse eines einzigen solchen Phänomens (Online-Anlagebetrug). An diesem Dispositiv ist eine Mehrheit der Kantone beteiligt. PICSEL OAB basiert auf der Infrastruktur und der Doktrin von PICSEL.

wird hier als Beispiel angeführt, namentlich aufgrund seiner Bereitschaft, in anderen Kantonen initiierte Verfahren zu übernehmen. Diese Unterstützung ist natürlich von der Verfügbarkeit von Ressourcen abhängig, was zunehmend weniger gegeben ist. Der Föderalismus sorgt zudem für die wertvolle Nähe zum Terrain, jede Kantonspolizei – oder Stadtpolizei – ist stark lokal verankert. Dies erlaubt auch ein rasches Reagieren auf eine Anzeige. Eine Folge des Föderalismus ist ausserdem eine hohe Anpassungsfähigkeit, die sich sowohl im Operativen als auch bei der Schaffung von interkantonalen Koordinationsstrukturen zeigt.

Solche Strukturen kompensieren die Grenzen des Föderalismus. So verfolgen NEDIK oder das Cyber-CASE dasselbe Ziel: durch die Förderung der Zusammenarbeit über die kantonalen Grenzen hinaus die Bekämpfung der Cyberkriminalität erleichtern. Diese Zusammenarbeit nimmt unterschiedlichste Formen an: von operativen Sitzungen, über den Informationstransfer zu neuen Phänomenen und eine «Unité de doctrine» bis zum Wissensmanagement. Andere regionale Kompetenzzentren (RC3, Forensik-Kompetenzzentren von Zug und St. Gallen) ermöglichen zudem, Ressourcen zu bündeln und Kriminalitätsphänomene aus regionaler Perspektive anzugehen.

Das hohe Wirtschaftsniveau der Schweiz ist ein weiterer Vorteil. Einerseits können die Strafverfolgungsbehörden mit (im internationalen Vergleich) adäquaten finanziellen Mitteln ausgestattet werden, was ein hohes Ausbildungsniveau und die Beschaffung von modernsten technischen Mitteln ermöglicht. Andererseits können die Strafverfolgungsbehörden sich auf ein dichtes Netz von Hochschulen und Universitäten sowie weiteren Partnern (zum Beispiel SWITCH) abstützen. Dies begünstigt die Zusammenarbeit mit akademischen Akteuren. Das PICSEL-Tool ist das Ergebnis einer solchen Zusammenarbeit.

Auch international ist die Schweiz gut vernetzt, namentlich aufgrund ihrer Präsenz bei Europol und Interpol sowie enger bilateraler Beziehungen mit Ländern, die in der Bekämpfung der Cyberkriminalität eine Schlüsselrolle spielen. Auch die Beteiligung der Schweiz am Budapester Übereinkommen über Cyberkriminalität ist ein Vorteil, da die Schweizer Strafverfolgungsbehörden von dessen Instrumenten profitieren (Informations-, Datensicherungs- und Datenübermittlungsersuchen). Die Schweiz verfügt ausserdem über gesetzliche Grundlagen, welche die Service Provider verpflichten, Daten während sechs Monaten aufzubewahren, was in vielen Ländern nicht der Fall ist (wo die Dauer kürzer ist oder keine solche Pflicht besteht).

4.2 Best Practices

Die taktische Kriminalanalyse, namentlich über das PICSEL-Dispositiv, bringt den beteiligten Kantonen einen wichtigen Mehrwert. Das Pilotprojekt PICSEL OAB wird ebenfalls als Beispiel angeführt, welches es ermöglicht hat, einen schweizweiten Lageüberblick zu einem spezifischen Phänomen zu gewinnen, Serien zu erkennen, Ermittlungen zu koordinieren und die verursachten Schäden zu quantifizieren. Erwähnt wird ausserdem die Fallübersicht von NEDIK im Bereich Ransomware, dank der rasch in Erfahrung gebracht werden kann, in welchem Kanton zu welchen Angriffen bereits ein Verfahren läuft, und Verfahren gegebenenfalls zusammengeführt werden können.

Die nationale Zusammenarbeit ist unabdingbar. In diesem Wissen unterstützen grosse Kantone manchmal die anderen Kantone. Die Zusammenarbeit ist ausserdem institutionalisiert. Als Beispiele werden die operativen Sitzungen von NEDIK oder auch der OSINT-Community angeführt. Die Zusammenarbeit mit dem BACS bringt einen Mehrwert, der noch weiter vertieft werden könnte. Positiv ist auch die Zusammenarbeit mit privaten Dienstleistern (Banken, Online-Verkaufsplattformen) gegen Cyberbetrug. Ausserdem wird der Beitrag von fedpol zur internationalen Kooperation hervorgehoben, namentlich über die Präsenz in der JCAT oder die Leistungen der Zentralstelle Cyber beispielweise bei Provideranfragen.

Im Ausbildungsbereich wird das Drei-Ebenen-System gelobt. Polizistinnen und Polizisten müssen mit Grundkenntnissen zu den Phänomenen geschult werden, damit sie beim Aufnehmen einer Anzeige wissen, welche relevanten Informationen sie einholen müssen. Ermittlerinnen und Ermittler müssen die geeigneten Ermittlungstaktiken kennen, um Täter zu identifizieren, insbesondere wenn es um digitalisierte Kriminalität geht (Kurs Cyber II). Auf Cyberkriminalität spezialisierte Ermittlerinnen und Ermittler müssen darüber hinaus über technische Fähigkeiten verfügen, die sie dazu befähigen, in komplexen Cyberkriminalitätsfällen die besten Massnahmen zu treffen (CAS/MAS). Die Ausbildung der Strafverfolgungsbehörden muss regelmässig angepasst werden, um die rasanten technologischen Entwicklungen zu berücksichtigen. Durch den Austausch – korpsintern, unter Spezialistinnen und Spezialisten sowie mit den Staatsanwaltschaften – kann der Transfer von Best Practices sichergestellt werden.

Im Präventionsbereich wird die Zusammenarbeit der SKP mit den Kantonen positiv gewertet. Die gezielten Präventionsanstrengungen, namentlich bei Jugendlichen und älteren Menschen, sind lohnenswert. Für diese letzte Gruppe eignet sich vor allem eine einfache, auf realen Vorkommnissen basierende Kommunikation zu den besten Sendezeiten, zum Beispiel vor der Tagesschau. Was die Zielgruppe der Jungen angeht, muss die Kommunikation schwerpunktmässig auf den sozialen Netzwerken stattfinden. Die Waadtländer Kantonspolizei geht hier mit gutem Beispiel voran: mit ihrem Projekt «E-Cop», einem Polizisten, der regelmässig auf Tiktok postet.[92]

Für die erfolgreiche Bekämpfung von Cyberkriminalität ist Reaktivität entscheidend. Namentlich gilt es, Daten im In- und Ausland rasch zu sichern. In manchen Fällen können die gesicherten Daten anschliessend einfach über das Übereinkommen über Cyberkriminalität eingeholt werden. Die Nachverfolgung der Finanzflüsse ist – wie in anderen Kriminalitätsbereichen – äussert wichtig. Tätern kann ein vernichtender Schlag versetzt werden, wenn ihnen die IT-Infrastruktur genommen wird, über die sie agieren. Dazu ist die internationale Kooperation unabdingbar, beispielsweise über gemeinsame Ermittlungsteams (JIT).

4.3 Schwächen

- ❖ Trotz allem bestehen auch zahlreiche Schwächen. Insbesondere verwiesen die Umfrageteilnehmenden auf die weit unzureichenden personellen Mittel, nicht ausreichend angepasste gesetzliche Grundlagen (automatischer Austausch von polizeilichen Informationen, internationale Rechtshilfe in Strafsachen), eine föderalismusbedingte Zersplitterung der Ressourcen oder auch eine noch unzureichende Prävention.

Zahlreiche Teilnehmende haben darauf hingewiesen, dass die personellen Ressourcen derzeit absolut nicht ausreichen. Dies gilt sowohl für die Polizei als auch die Staatsanwaltschaften. Demgemäss sind schlicht und einfach zu wenige Ressourcen vorhanden, um zu allen eingehenden Anzeigen vertiefte Ermittlungen zu tätigen. Alle Kantone sind dadurch beeinträchtigt, ganz besonders aber die kleinen, die nicht genügend Ressourcen haben, um einen Teil davon spezifisch für die Bekämpfung der Cyberkriminalität einzusetzen. Der Mangel an personellen Mitteln beeinflusst auch die Präventionsanstrengungen. Ausserdem wird darauf hingewiesen, dass die Zunahme der Anzeigen den Ressourcenmangel noch verschärft. Es ist nicht mehr möglich, diesen Mangel lediglich durch Prozessoptimierungen auszugleichen. Auch ist eine einfache Umteilung bestehender Ressourcen nicht erwünscht, da sich dies auf die anderen Polizeiaufgaben auswirken würde. Erwünscht ist vielmehr die Schaffung neuer Stellen.

[92] François, le policier vaudois d'internet qui doit parler aux jeunes - rts.ch - Vaud

Bei den gesetzlichen Grundlagen monieren zahlreiche Teilnehmende hauptsächlich die Langsamkeit und die Komplexität der internationalen Rechtshilfe in Strafsachen.[93] Die Langsamkeit ist insofern besonders problematisch, als sie es den Tätern erlaubt, ihre Spuren zu verwischen.
Auf Ebene der Schweiz ist ausserdem das Fehlen von gesetzlichen Grundlagen für den automatischen Austausch von polizeilichen Informationen sehr problematisch.[94] Daher wird gewünscht, dass beachtliche Anstrengungen unternommen werden, um die Blockaden in Zusammenhang mit den kantonalen Gesetzesgrundlagen rasch aus dem Weg zu schaffen. Hinzu kommen Gerichtsstandregeln, die im Zusammenhang mit der Cyberkriminalität als überholt betrachtet werden. Fragmentierte Strafverfolgungskompetenzen verschärfen die Problematik zusätzlich. Angeführt werden ausserdem weitere Aspekte wie die Schwerfälligkeit und die Kosten gewisser Verfahren zur Überwachung des Fernmeldeverkehrs (in Echtzeit oder rückwirkend).

Wie bei den Gesetzesgrundlagen bereits erwähnt, wird der Föderalismus auch als eine Schwäche der Schweiz wahrgenommen. Er erschwert die Koordination und die Ressourcenbündelung. Er führt zu einer Zersplitterung der Ressourcen, insbesondere in kleinen Kantonen. Diese verfügen nicht über die erforderlichen Ressourcen für eine wirksame Bekämpfung der Cyberkriminalität, haben gleichzeitig aber auch nicht genügend Fälle, um eine spezifische Einheit hierfür zu schaffen. Dies führt dazu, dass sie komplexere Cybercrime-Fälle in der Regel nicht effektiv bearbeiten können. Ohne ein regionales Kompetenzzentrum müssen sie sich auf die Solidarität der grossen Kantone verlassen.

Die Zersplitterung wirkt sich auch auf die technischen Tools aus: Entwicklungen oder Beschaffungen werden in einzelnen Kantonen realisiert anstatt gebündelt. Manchmal herrscht ein «Jeder für sich»-Denken beziehungsweise Zurückhaltung vor, wenn es darum geht, Fälle zu übernehmen, die mehrere Kantone betreffen. Bei Fällen mit starken internationalen Verästelungen wird gewünscht, dass der Bund den Lead übernimmt. Ohne ein nationales Ermittlungssystem oder ein nationales System für die taktische Kriminalanalyse ist das Risiko gross, dass dieselben Tätergruppen Gegenstand mehrerer, nicht koordinierter Verfahren sind. Mehrere Teilnehmende weisen darauf hin, dass die Vielzahl der zu einem Teil in die Bekämpfung der Cyberkriminalität involvierten Stellen (BACS, NEDIK, Cyber-CASE, Staatsanwaltschaften, Kantonspolizeien, fedpol, NDB Cyber) die Situation komplex macht. Auf internationaler Ebene ist zudem der Status der Schweiz als Europol-assoziierter Staat ein Faktor, der die Kooperation einschränkt.

Was die Ermittlungen anbelangt, wird hervorgehoben, dass Verfahren und Täter im Ausland selten vor Gericht enden. Das erzeugt mitunter den Eindruck, dass die Repressionsarbeit ins Leere läuft, wenn selbst dann, wenn die Täterschaft identifiziert wurde, ihre Auslieferung fast unmöglich ist, weil sie sich in kaum oder nicht kooperativen Jurisdiktionen befinden. Nebst diese Grenzen betonen die Teilnehmenden auch die Herausforderung durch die wachsende Masse an gesicherten Daten, die es zu analysieren gilt. Manchmal, etwa bei der Fahndung im Darknet, stellt sich auch gerade das umgekehrte Problem: forensische Spuren zu finden und einem Täter zuzuordnen.

Generell wird ein Mangel an Prävention beklagt. Einige Befragte weisen auf das Fehlen einer Hotline für Privatpersonen hin. Empfohlen werden innovativere Präventionskampagnen, zum Beispiel Phishing-Kampagnen zu Sensibilisierungszwecken. Ausserdem wird eine stärkere Einbindung privater Akteure – deren Dienste häufig missbraucht werden – gewünscht. Erwartet wird ausserdem auch ein vermehrter Rückgriff auf technische Prävention.

[93] Ein Teilnehmer fasst die Problematik lakonisch wie folgt zusammen: «Rechtshilfeersuchen dauern sehr lange und müssten auf internationaler Ebene vereinfacht werden. Die Täterschaft erreicht Millionen von Leuten innerhalb von wenigen Sekunden. Die Strafverfolgungsbehörden erreichen sich nicht einmal innerhalb von Monaten. Täterschaft ist meistens im Ausland und für Schweizer Behörden nicht greifbar. Antworten sollten innerhalb nützlicher Frist eingehen.»
[94] Ein Spezialist schildert die Problematik so: «Ich erhalte mehr Informationen von anderen Staaten des Schengen-Raums als von den Kantonspolizeien der Nachbarskantone.»

5 Handlungsbedarf

Gestützt auf die in Kapitel 2.3 identifizierten Herausforderungen sowie die Umfrageergebnisse wurden fünf Bereiche identifiziert, in denen Handlungsbedarf besteht. Diese Bereiche entsprechen Problemstellungen, die bereits bei der Erarbeitung der NCS hervorgehoben wurden, in welche die kantonalen Strafverfolgungsbehörden eng eingebunden waren.

Über den automatischen interkantonalen Austausch von polizeilichen Informationen die taktische Kriminalanalyse zu Cyberkriminalität ermöglichen

Ohne einen automatischen interkantonalen Austausch von polizeilichen Informationen ist es für die einzelnen Polizeien sehr kompliziert in Erfahrung zu bringen, welches Korps gegen welche Täter ermittelt. Oder anders gesagt: Die Polizei weiss nicht, was die Polizei weiss. Dies verursacht einen grossen, unnötigen Mehraufwand (Überprüfung im Einzelfall), beinhaltet das Risiko von doppelt geführten Ermittlungen und verhindert die Entwicklung einer nationalen taktischen Kriminalanalyse. Lediglich eine Minderheit von Kantonen verfügt über gesetzliche Grundlagen, die den automatischen interkantonalen Austausch von polizeilichen Informationen erlauben.

- **Laufende Massnahme:** Die Umsetzung der Motion 18.3592 wird durch die Kantone und den Bund mit der Nationalen polizeilichen Abfrageplattform (POLAP) vorangetrieben. Mit der POLAP wird der Austausch von Informationen unter den Polizeien in der Schweiz und international massiv vereinfacht. Allerdings fehlen seitens der Kantone grossmehrheitlich die gesetzlichen Grundlagen für den Austausch von polizeilichen Informationen ausserhalb von Verfahren gemäss Schweizerischer Strafprozessordnung (StPO). Diese Lücke soll durch die neue «Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme» geschlossen werden. Dieses unmittelbar rechtsetzende Konkordat befindet sich derzeit in der von der KKJPD durchgeführten Vernehmlassung bei den Kantonen und beim Bund. Der Bund unterstützt den von der KKJPD und KKPKS eingeschlagenen Weg des Konkordats. Sollte das Konkordat scheitern, so müsste für eine vollständige Umsetzung der Motion die Bundesverfassung angepasst und der nationale polizeiliche Datenaustausch durch den Bund geregelt werden. Eine dahingehende Motion der SiK ist derzeit im Parlament in Bearbeitung (Motion 23.4311 «Schaffung einer Verfassungsgrundlage für eine Bundesregelung des nationalen polizeilichen Datenaustauschs»).

Dank der taktischen Kriminalanalyse können Verbindungen zwischen Tätern hergestellt, Tendenzen erkannt und präventive Massnahmen ergriffen werden. Dies bedeutet einen grossen Mehrwert für die Bekämpfung der Cyberkriminalität, erst recht in einem föderalistischen Land. Am PICSEL-Dispositiv ist lediglich eine Minderheit von Kantonen beteiligt.

- **Laufende Massnahmen:** Kurzfristig müssen sämtliche Kantone, die über eine gesetzliche Grundlage verfügen, eine Beteiligung an PICSEL prüfen. Parallel dazu muss das PTI-Projekt «PICSEL CH» erfolgreich zu Ende geführt werden. Das Projekt verfolgt das Ziel, PICSEL oder eine ähnliche Lösung schweizweit einzuführen. Seine Umsetzung hängt auch von der Anpassung der gesetzlichen Grundlagen ab, welche den automatischen Austausch von polizeilichen Informationen unter den Kantonen ermöglichen. Die Behebung dieses Problems ist auch das Ziel der Massnahme M13 der NCS.[95]

[95] Auszug aus M13: «Es sind aber noch nicht alle Kantone daran beteiligt. Grund dafür ist eine fehlende gemeinsame und einheitliche Rechtsgrundlage, die es PICSEL erlauben würde, in der gesamten Schweiz Anwendung zu finden. Es muss geklärt werden, wie eine Rechtsgrundlage für eine Plattform für den Informationsaustausch geschaffen werden kann.»

Die Rechtsgrundlagen anpassen, um die Bekämpfung der Cyberkriminalität zu erleichtern

Ob es darum geht, Beweismittel zu erhalten oder die Täterschaft vor Gericht zu bringen: Viel zu oft stossen die Strafverfolgungsbehörden an die Grenzen der internationalen Rechtshilfe in Strafsachen. Die heutige Situation ist nicht befriedigend und führt zu schwerwiegender Ineffizienz (Verlangsamung der Ermittlungen, Straflosigkeit für die Täter). Die Schweiz muss ihre Anstrengungen intensivieren, um sich den bestehenden Mechanismen anzuschliessen, die darauf abzielen, die relevanten Rechtsgrundlagen an die technologischen Entwicklungen anzupassen. Hauptsächlich handelt es sich dabei um das zweite Zusatzprotokoll zur Budapest-Konvention, das Gesetzespaket e-Evidence der EU oder auch den CLOUD Act der USA. Das BJ hat 2021 sowie 2023 die Diskussionsgrundlagen vorgelegt.[96] Diese Arbeiten werden derzeit konkretisiert, damit ein Grundsatzentscheid getroffen werden kann. Ergänzend dazu wäre auch der Abschluss bilateraler Polizeiabkommen mit Ländern zu prüfen, in denen die besonders aktiven Täter ansässig sind. Eine solche Massnahme setzt die Entwicklung einer nationalen taktischen Kriminalanalyse im Bereich Cyberkriminalität voraus. Auf dieser Grundlage könnte bestimmt werden, welche Länder Priorität haben.

- **Laufende Massnahmen:** Die Herausforderungen der internationalen Rechtshilfe in Strafsachen sind in drei Massnahmen der NCS thematisiert:
  M12 «Koordination bei der Zusammenarbeit mit nationalen und internationalen Akteuren, vor allem im Bereich der Beweissicherung sowie der Rechtshilfen»;
  M16 «Aktive Beteiligung der Schweiz an der Weiterentwicklung und der Umsetzung des Übereinkommens über die Cyberkriminalität (‹Budapest-Konvention›) des Europarats»;
  M17 «Es werden bilaterale Abkommen zur gegenseitigen Unterstützung bei der Bekämpfung von Cyberkriminalität angestrebt».

Über die internationale Rechtshilfe in Strafsachen hinaus müssten zahlreiche weitere Rechtsgrundlagen daraufhin überprüft werden, ob sie für die Bekämpfung der Cyberkriminalität noch adäquat sind.[97] Zum Beispiel sind die Gerichtsstandregeln zu klären – gerade zu Beginn der Ermittlungen geht bis zur Bestimmung des Gerichtsstands häufig wertvolle Zeit verloren. Weiter sind innovative Mechanismen wie Sicherheitspflichten im Bereich Cybersicherheit oder die Möglichkeit von Online-Durchsuchungen zu sondieren, die Regulierung von Krypto-Assets zu prüfen, die öffentlich-private Zusammenarbeit zu Zwecken der technischen Prävention zu erleichtern.

Die Koordination bei der Bekämpfung von Cyberkriminalität stärken

Generell sind nicht neue Koordinationsgremien zu schaffen, sondern die bestehenden zu stärken. Die operative Koordination der Bekämpfung der Cyberkriminalität wird von NEDIK gewährleistet. Um dem Wachstum der Cyberkriminalität Rechnung zu tragen, muss eruiert werden, mit welchen Massnahmen NEDIK gestärkt werden könnte. Namentlich ist zu prüfen, ob die NEDIK-Vereinbarung und der Leistungskatalog den Bedürfnissen entsprechen. Auch ist zu prüfen, ob die vorhandenen personellen Ressourcen ausreichen.

Die Stärkung der Zusammenarbeit auf nationaler und regionaler Ebene, beispielsweise über die Polizeikonkordate, müsste ebenfalls beleuchtet werden. Denkbar wäre, regionale Cyberkompetenzzentren zu realisieren oder vorzusehen, dass sich einige Kantone in gewissen Bereichen spezialisieren, um zugunsten der anderen Konkordatskantone Leistungen zu erbringen und so Doppelspurigkeiten zu vermeiden. Geprüft werden sollte weiter, inwieweit gemeinsame Ermittlungsteams aufgebaut werden könnten. Um die Praktiken auf nationaler Ebene zu vereinheitlichen, ist zu prüfen, inwiefern eine Strategie zur Bekämpfung der Cyberkriminalität erstellt werden könnte. Auf Ebene Bund ginge es darum, zu prüfen, inwiefern Leistungen der internationalen Koordination gestärkt werden können, etwa im Bereich des internationalen Austauschs von polizeilichen

[96] (Bundesamt für Justiz, 2023)
[97] Dieser Punkt wird im Übrigen auch in der NCS angeführt: **M12** «Dazu gehört auch zu prüfen, welche Anpassungen der rechtlichen Grundlagen dafür nötig sind. […] Die örtlichen Zuständigkeitsregeln der Strafprozessordnung erschweren die Strafverfolgung der Cyberkriminalität.»

Informationen oder der Verbreitung von Analyseberichten. Das Schweizer Verbindungsbüro bei Europol und Eurojust wäre beispielsweise zu stärken.

Im Bereich der Prävention ist vor allem die Organisation innovativer Kampagnen auf nationaler Ebene zu intensivieren und die Ausrichtung der Präventionsprodukte auf die jeweiligen Zielgruppen anzupassen.[98] Auch sollten sich die kantonalen Strafverfolgungsbehörden stärker bei nationalen Präventionskampagnen engagieren, diese unterstützen und sich daran beteiligen. Zu diesem Zweck müsste auch die Verbindung zwischen NEDIK und der SKP gestärkt werden. Ferner muss geprüft werden, inwieweit der Betrieb einer nationalen Plattform ausschliesslich zur Prävention von Cyberkriminalität zweckmässig ist (zum Beispiel cybercrimepolice.ch). Auch muss evaluiert werden, mit welchen Mitteln private Partner stärker in Präventionsmassnahmen eingebunden werden könnten. Schliesslich muss auch die Anwendung von Massnahmen der technischen Prävention systematischer erfolgen. Die Sensibilisierung der Bevölkerung gegenüber Cyberrisiken ist in der NCS vorgesehen.[99]

- **Laufende Massnahme:** Eine Stärkung der Zusammenarbeit ist auch das Ziel der Massnahme M12 der NCS: «Stärkung der bestehenden Zusammenarbeit: durch die Standardisierung von Prozessen sowie Schnittstellen und Förderung des Erfahrungsaustausches. […] Bündelung von Fachkompetenzen (z. B. zu IT-Forensik) und von sicherheitsrelevanten Beschaffungen.»

Die Mittel an die Zunahme der Cyberkriminalität anpassen

Obwohl die Umfrage zeigt, dass die Kantone mehrheitlich Anstrengungen unternehmen, um Personal spezifisch für die Bekämpfung der Cyberkriminalität einzusetzen oder zu rekrutieren, sind sehr viele Befragte der Ansicht, dass die eingesetzten Ressourcen massiv unzureichend sind. In erster Linie sollte also das Personal in Staatsanwaltschaften und Polizeien aufgestockt werden, um den konstanten Fallanstieg und die zunehmende Komplexität der Fälle bewältigen zu können.
Zudem verwenden viele Polizeikorps dieselben technischen Mittel, beschaffen diese aber unabhängig voneinander. Daraus ergibt sich eine gewisse Ineffizienz: hohe Lizenzpreise, separate Ausbildungen. Die Anstrengungen für eine zentrale oder gebündelte Beschaffung von technischen Mitteln sollten daher verstärkt werden. Die Beschaffung neuer technischer Mittel muss weiterhin gemeinsam gedacht werden. Auch müssen Partnerschaften gestärkt werden, um solche technischen Mittel bei anderen Ländern oder Kompetenzzentren zu erhalten. Bemühungen in diese Richtung laufen bereits: über NEDIK (Analyse von Kryptowährungen) und fedpol/PTI (IT-Forensik-Tools). Die NCS greift diesen Punkt ebenfalls auf.[100]

- **Massnahmenvorschlag:** Die personellen und technischen Mittel, die für die Bekämpfung der Cyberkriminalität eingesetzt werden, liegen in der alleinigen Kompetenz der einzelnen Kantone. Obwohl mit der Umfrage quantitative Daten erhoben wurden, wird den Kantonen empfohlen, einzeln eine Selbstevaluation vorzunehmen. Deren Ziel wäre zu bestimmen, ob die gegenwärtigen Mittel ausreichen, um die Cyberkriminalität wirksam zu bekämpfen.
- Das Postulat 23.4349 «Ressourcenüberprüfung beim Fedpol» der Finanzkommission des Nationalrates[101] verlangt eine Überprüfung, ob die fedpol zur Verfügung stehenden Ressourcen, auch im Bereich Cyberkriminalität, genügen. Der Nationalrat hat das Postulat am 28. Februar 2024 angenommen.

[98] Viele Kampagnen entsprechen diesem Bedürfnis bereits: SUPER, Kampagne Card Security Phishing, Pharming and Co.
[99] **M2** «Der Sensibilisierungs- und Präventionsbedarf in den unterschiedlichen Bereichen wird kontinuierlich geprüft. Als Grundlage dafür dienen aktuelle Vorfälle, die Entwicklung der Bedrohungslage sowie die Einschätzungen der Behörden, Unternehmen und Wirtschaftsverbände zum Sensibilisierungsbedarf in ihren Bereichen. […] Die in der Sensibilisierung tätigen Akteure sind bekannt und der Austausch unter ihnen wird gezielt gefördert. […] Die Aufwände und Wirkungen der Sensibilisierungsmassnahmen werden erhoben, um ihren Erfolg zu ermitteln und sie optimieren zu können.»
[100] M12 «Bündelung von Fachkompetenzen (z. B. zu IT-Forensik) und von sicherheitsrelevanten Beschaffungen.»
[101] 23.4349 | Ressourcenüberprüfung beim Fedpol | Geschäft | Das Schweizer Parlament

Wichtig ist auch die Ausbildung der Strafverfolgungsbehörden, ob Polizisten, Staatsanwältinnen oder Richter. In einem so dynamischen Bereich wie der Cyberkriminalität ist sicherzustellen, dass die Ausbildungen aktuell sind. Idealerweise wird eine Zertifizierungsmöglichkeit auf der Stufe eines schweizerischen «Master of Advanced Studies» (MAS) geschaffen, der die bestehenden Ausbildungen zusammenführt. Zudem muss sichergestellt werden, dass Staatsanwältinnen und Staatsanwälte sowie Richterinnen und Richter ebenfalls Zugang zu spezifischen Ausbildungen haben.

- **Laufende Massnahme:** Die Massnahme M14 «Ausbildung der Strafverfolgungsbehörden» der NCS deckt diese Thematik ab.

6 Fazit und Ausblick

Die Cyberkriminalität nimmt konstant zu, sowohl was die Anzahl der Delikte als auch die Schwere der verursachten Schäden anbelangt. Die überwiegende Mehrheit der Kantone hat Anpassungen vorgenommen, um dieser Zunahme der Cyberkriminalität zu begegnen. So wurden in den Kantonspolizeien spezifische Einheiten zur Bekämpfung von Cyberkriminalität aufgebaut und neue Ermittler-, IT-Forensiker- und Analytikerstellen geschaffen. Auch in den nächsten zehn Jahren dürften weitere Stellen geschaffen werden. Dabei gibt es von Kanton zu Kanton grosse Unterschiede. Die meisten kantonalen Staatsanwaltschaften sowie die BA verfügen über Staatsanwältinnen und Staatsanwälte, die auf die Bekämpfung von Cyberkriminalität spezialisiert sind.

Zahlreiche Umfrageteilnehmende sind jedoch der Auffassung, dass die aktuell in der Bekämpfung der Cyberkriminalität eingesetzten Personalbestände absolut nicht ausreichend sind und keine vertiefte Bearbeitung der eingegangenen Anzeigen erlauben. Sie betonen diesbezüglich, dass zusätzliches Personal benötigt wird, nicht eine Umteilung bestehender Ressourcen. Der Bundesrat empfiehlt den Kantonen daher, individuell eine Selbstevaluation vorzunehmen, um zu überprüfen, ob die eingesetzten Mittel der Lage im Bereich Cyberkriminalität entsprechen.

Die Zusammenarbeit zwischen Kantonen – die in der Bekämpfung der Cyberkriminalität besonders angezeigt ist – wird über interkantonale Stellen sichergestellt, wie sie mit NEDIK oder dem Cyber-CASE eingerichtet wurden. Auch andere bestehende Stellen wie die SKP oder das SPI berücksichtigen die Problematik in ihren Aktivitäten. Die Leistungen dieser verschiedenen Gremien werden von den Spezialistinnen und Spezialisten sehr geschätzt. Darüber hinaus bestehen zahlreiche weitere Formen der Zusammenarbeit, wie das Cyberkompetenzzentrum in der Westschweiz oder die Forensik-Kompetenzzentren des Kantons Zug und des Polizeikonkordats Ostpol. Diese institutionalisierten Formen der Zusammenarbeit werden durch informelle Kooperationen im Einzelfall ergänzt, wenn beispielsweise besser dotierte Kantone in anderen Kantonen initiierte Verfahren übernehmen oder sie mit anderen Leistungen unterstützen.

Auch unter Bezugnahme auf die Vorschläge des Postulats 22.3017 der Sicherheitspolitischen Kommission des Nationalrats stellt der Bundesrat fest, dass die Entwicklung von Kapazitäten durch die Kantone wie auch die Institutionalisierung der interkantonalen Koordination in der Bekämpfung der Cyberkriminalität gegen eine vollständige Übernahme der Strafverfolgungskompetenzen durch den Bund spricht. Nur eine Minderheit der Umfrageteilnehmenden hat diese Massnahme vorgebracht. Deren Umsetzung würde einerseits die kantonale Souveränität im Sicherheitsbereich und andererseits die organisatorischen Anstrengungen und die Investitionen, welche die Kantone zur Bekämpfung dieser Form der Kriminalität unternommen haben, infrage stellen. Sie widerspräche zudem den Bestimmungen der Strafprozessordnung in diesem Bereich. Auch hätte diese Massnahme einen massiven Personalbedarf beim Bund zur Folge. Aus ebendiesen Gründen ist die Schaffung eines Kompetenzzentrums für die Analyse von Kryptowährungen beim Bund für die Kantone nicht zielführend.

Wie fit sind die Kantone in der Cyber-Strafverfolgung?

Die kantonalen Strafverfolgungsbehörden sind heute in ihren Strafverfahren regelmässig mit Kryptowährungen konfrontiert. Sie haben bereits begonnen, sich entsprechend auszurüsten und ihr Personal auszubilden. Dank NEDIK wurde ein schweizweit einheitlicher Preis für ein Kryptoanalysetool definiert. Nach Ansicht des Bundes ist diesem Beispiel zu folgen.

Zwei grosse Hindernisse stehen einer Verbesserung der Bekämpfung der Cyberkriminalität im Weg: zum einen das Fehlen von gesetzlichen Grundlagen, welche den automatischen Austausch von polizeilichen Informationen zwischen den Kantonen sowie mit dem Bund ermöglichen. Zum anderen ist das Regime der internationalen Rechtshilfe in Strafsachen relativ langsam und nicht auf elektronische Beweismittel zugeschnitten.

Ohne den automatischen Austausch von polizeilichen Informationen ist es sehr kompliziert, Verbindungen zwischen Verfahren herzustellen, die in verschiedenen Kantonen zu den gleichen Tätern im Gang sind. Dies führt zu einer Ressourcenverschwendung und schwächt die Erfolgschancen der Ermittlungen. Auch verhindert es die Weiterentwicklung der taktischen Kriminalanalyse zu Cyberkriminalität auf nationaler Ebene. Diese ist jedoch entscheidend, wenn es darum geht, technische Präventionsmassnahmen, Massnahmen zur Sensibilisierung der Bevölkerung oder auch kohärente Strategien zur Bekämpfung der Cyberkriminalität zu entwickeln. Ohne diesen automatischen Austausch ist es zudem kompliziert, Verfahren, welche dieselben Täter betreffen, zu konsolidieren, sei es auf kantonaler oder auf Bundesebene. Mit der Umsetzung der Motion 18.3592 Eichenberger wird diese Lücke bald geschlossen. Parallel dazu führt PTI Schweiz ein Projekt durch, um schweizweit eine ähnliche Lösung wie PICSEL einzuführen.

Die internationale Rechtshilfe kann für Ermittlungen eine Herausforderung darstellen. Gerade ausserhalb des Rahmens der Budapest-Konvention des Europarates können ihre Grenzen (Langsamkeit, ausgedehnte Rechtsbehelfe, administrative Komplexität und das Problem, dass die internationale Rechtshilfe nicht auf elektronische Beweismittel zugeschnitten ist) Cyberkriminellen zum Vorteil gereichen und ihre Chancen erhöhen, der Justiz zu entwischen. Selbst wenn Ermittlungen erfolgreich sind, zeigt sich, dass zahlreiche Täter in Ländern Unterschlupf finden, mit denen die Rechtshilfe sehr kompliziert ist oder nicht funktioniert. Neben der Budapest-Konvention über Cyberkriminalität des Europarates und ihrem zweiten Zusatzprotokoll, deren Ziel die Verbesserung der Bekämpfung von Cyberkriminalität ist, haben gewisse Länder, wie die EU oder die USA, verschiedene Rechtsakte und Rechtsgrundlagen erlassen, um dem technologischen Fortschritt in der Rechtshilfe Rechnung zu tragen.[102] Die Bundesverwaltung verfolgt die internationalen Entwicklungen in diesem Bereich aufmerksam[103] und hat die Diskussionsgrundlagen vorgelegt, zum Beispiel betreffend das e-Evidence-Projekt der EU.[104] Diese Arbeiten werden derzeit konkretisiert, damit ein Grundsatzentscheid getroffen werden kann.

Gemäss den Rückmeldungen der konsultierten kantonalen Behörden sind auch in anderen Bereichen Verbesserungen angezeigt. Die bestehenden Zusammenarbeitsmechanismen (NEDIK, Cyber-CASE) müssen gestärkt und die Präventionsanstrengungen erhöht und so angepasst werden, dass sie die ganze Bevölkerung und die Gesamtheit der Unternehmen im Land erreichen. Bei der Beschaffung von technischen Mitteln sind Verhandlungen zugunsten aller Polizeikorps Einzelbeschaffungen vorzuziehen. Der gesetzliche Rahmen, beispielsweise was die Festlegung des Gerichtsstands oder Pflichten für private Anbieter angeht (Prävention über die Nutzerinnen und Nutzer, Anzeige von Missbräuchen, technische Missbrauchsprävention), muss analysiert werden und wenn nötig sind Änderungsanträge vorzulegen. Die internationale Kooperation muss intensiviert werden.

[102] (Bundesamt für Justiz, 2023), S. 3. Die USA verabschiedeten im November 2018 den Clarifying Lawful Overseas Use of Data Act (CLOUD Act), der im Rahmen von Strafverfahren zu einem erleichterten Zugriff auch auf im Ausland gelagerte Daten führen soll. Die EU hat das Gesetzespaket zur e-Evidence verabschiedet, um einen kohärenten EU-Rahmen für den Umgang mit elektronischen Beweismitteln zu schaffen und deren Erhebung zu beschleunigen.
[103] US CLOUD Act, E-Evidence der EU, zweites Zusatzprotokoll zur Budapest-Konvention, UN-Konvention gegen Cyberkriminalität.
[104] (Bundesamt für Justiz, 2023)

Die meisten der in diesem Bericht präsentierten Empfehlungen sind auch in der NCS zu finden. Bei deren Ausarbeitung waren die Strafverfolgungsbehörden bereits eng eingebunden. Daher ist der Bundesrat der Auffassung, dass mit den von der NCS – beziehungsweise deren Steuerungsausschuss – vorgesehenen Umsetzungsmechanismen die Verbesserung der Voraussetzungen für die Bekämpfung der Cyberkriminalität sichergestellt werden kann.

Glossar

BA	Bundesanwaltschaft
BACS	Bundesamt für Cybersicherheit
BAZG	Bundesamt für Zoll und Grenzsicherheit
BFS	Bundesamt für Statistik
BJ	Bundesamt für Justiz
CAS	Certificate of Advanced Studies
CCC	Convention on Cybercrime (Übereinkommen über Cyberkriminalität)
EC3	European Cybercrime Centre
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EU	Europäische Union
FBI	Federal Bureau of Investigation
fedpol	Bundesamt für Polizei
FIU	Financial Intelligence Unit
FMG	Fernmeldegesetz
IKT	Informations- und Kommunikationstechnologien
IOT	Internet of Things
JCAT	Joint Cybercrime Action Taskforce
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
KKPKS	Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz
MAS	Master of Advanced Studies
MROS	Money Reporting Office Switzerland
NCMEC	National Center for Missing and Exploited Children
NCS	Nationale Cyberstrategie
NEDIK	Netzwerk digitale Ermittlungsunterstützung Internetkriminalität
PICSEL	Plateforme d'Information sur la Criminalité Sérielle en Ligne
PTI	Polizeitechnik und -informatik Schweiz
RC3	Regionales Cyberkompetenzzentrum
SIK-N	Sicherheitspolitische Kommission des Nationalrates
SKK	Schweizerische Kriminalkommission
SKP	Schweizerische Kriminalprävention
SOCTA	Serious and Organised Crime Threat Assessment
SPI	Schweizerisches Polizei-Institut
SSK	Schweizerische Staatsanwaltschaftskonferenz
StGB	Schweizerisches Strafgesetzbuch
StPO	Schweizerische Strafprozessordnung
SVR	Schweizerische Vereinigung der Richterinnen und Richter
SVS	Sicherheitsverbund Schweiz
TOR	The Onion Router
VPN	Virtual Private Network
VSKC	Vereinigung der Schweizerischen Kriminalpolizeichefs
VSPB	Verband Schweizerischer Polizei-Beamter
ZentG	Bundesgesetz über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten

Bibliografie

Bundesamt für Justiz. (2021). *Bericht zum US CLOUD Act.*

Bundesamt für Justiz. (2023). *Bericht zur e-Evidence-Vorlage der EU.*

Bundesanwaltschaft. (2021). *Tätigkeitsbericht 2020.*

Bundesanwaltschaft. (2022). *Tätigkeitsbericht 2021.*

Bundesrat. (2023). *Nationale Cyberstrategie (NCS).*

Eidgenössische Finanzmarktaufsicht (FINMA). (2022). *Kryptobasierte Vermögenswerte.*

European Union Agency for Law Enforcement Cooperation. (2021). *EUROPOL SPOTLIGHT - CRYPTOCURRENCIES: TRACING THE EVOLUTION OF CRIMINAL FINANCE.*

European Union Agency for Law Enforcement Cooperation. (2021). *Internet Organised Crime Threat Assessment.*

European Union Agency for Law Enforcement Cooperation. (2022). *4 TH ANNUAL SIRIUS EU DIGITAL EVIDENCE SITUATION REPORT.*

European Union Agency for Law Enforcement Cooperation. (2022). *FACING REALITY? LAW ENFORCEMENT AND THE CHALLENGE OF DEEPFAKES.* Luxembourg: Publications Office of the European Union.

European Union Agency for Law Enforcement Cooperation. (2022). *POLICING IN THE METAVERSE: WHAT LAW ENFORCEMENT NEEDS TO KNOW.* Luxembourg: Publications Office of the European Union.

European Union Agency for Law Enforcement Cooperation. (2023). *ChatGPT - The impact of Large Language Models.* Luxembourg: Publications Office of the European Union.

European Union Agency for Law Enforcement Cooperation. (2023). *Internet Organised Crime Threat Assessment.*

Khiralla, F. (2020). Statistics of cybercrime from 2016 to the first half of 2020. *Int. J. Comput. Sci. Netw., 9(5*, 252-261.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Cambridge, Polity.

Anhänge

1 Umfragemethodik

Die Umfrage wurde durch fedpol und den SVS erstellt. Sie wurde mit verschiedenen Partnern aus den Kantonspolizeien (NEDIK via ZH, GE) sowie den Staatsanwaltschaften (BA, SSK) und der SKP konsolidiert. Die Umfrage enthielt allgemeine und spezifische Fragen (das heisst solche, welche nur die Polizei oder nur die Staatsanwaltschaften betrafen). Die Umfrage wurde anschliessend im Februar 2023 über die KKPKS, die SSK und die kantonalen Kanzleien an die Polizeikorps, die Staatsanwaltschaften beziehungsweise die Gerichte verteilt. Die Antwortfrist betrug zwei Monate.

Insgesamt sind über das Tool 74 vollständig ausgefüllte Umfragen eingegangen (davon zwei doppelt), und eine vollständig ausgefüllte Umfrage wurde via Mail retourniert.

- Fast alle Kantonspolizeien (mit einer Ausnahme) sowie eine Stadtpolizei haben die Umfrage ausgefüllt.
- Fast alle Staatsanwaltschaften (mit einer Ausnahme) sowie die Bundesanwaltschaft haben die Umfrage ausgefüllt.
- Eine Mehrheit der Gerichte (18 über das Tool + 1 via Mail) hat die Umfrage ausgefüllt.
- Weitere Organisationen, wie die Schweizerische Kriminalprävention, haben die Umfrage ebenfalls ausgefüllt.