Bundeskriminalamt

BKA AUTUMN CONFERENCE HERBSTTAGUNG

Wie halten wir Schritt? Ein „Standpunkt“

Langfassung

Holger Münch
Präsident des Bundeskriminalamtes

Wie halten wir Schritt? – Polizeiliche Strategien für die Zukunft
BKA-Herbsttagung, 16. – 17. November 2022

WIE HALTEN WIR SCHRITT? EIN „STANDPUNKT“

Sehr geehrte Damen und Herren,

Frau Ministerin Faeser und Herr Dr. Shaw haben die dringende Notwendigkeit, mit den großen Herausforderungen in der Organisierten Kriminalität Schritt zu halten, aufgezeigt – und entsprechende Antworten vorgestellt.

Dazu auch von mir später mehr.

Liebe Gäste,

viele von Ihnen sind sicher, so wie ich, mit der Bahn oder dem Flugzeug angereist – haben vorab online eingecheckt und sich bei der Ticket-Kontrolle mit Ihrem digitalen Ticket ausgewiesen.

Aus Wiesbaden und Umgebung sind vermutlich einige mit dem Auto gekommen – und wer den Weg nicht kennt, hat sich von Google Maps zum RMCC leiten lassen.

Andere wollten vielleicht mit dem Bus fahren – bis eine Push-Nachricht des RMV über dessen Ausfall informierte. Also haben Sie sich spontan per App einen E-Roller gemietet.

Ein paar sind auch zu Fuß gekommen – und haben ihre Schrittzähler-App gleich mitlaufen lassen.

Wieder andere haben sich all diese Schritte gespart und bequem digital zugeschaltet – aus Meckenheim, Berlin oder Den Haag.

Warum sage ich das? Weil das unsere Lebenswirklichkeit ist.

Aber – nicht nur unsere: auch die der kriminellen Täter.

Mit der Digitalisierung verändert sich Kriminalität – strukturell und mit hoher Geschwindigkeit.

In klassisch analogen Phänomenbereichen wie Gewaltkriminalität, Diebstahl und insbesondere Wohnungseinbruchdiebstahl beobachten wir eine spürbar sinkende Anzahl der Straftaten in den vergangenen 10 Jahren: um rund 16, 38 und sogar 62 Prozent.

Sehr starke Anstiege verzeichnen wir hingegen insbesondere im Bereich der Darstellungen sexualisierter Gewalt zum Nachteil von Kindern und Jugendlichen sowie im Phänomenbereich Cybercrime.

Insgesamt ist die Anzahl der Straftaten unter Nutzung des „Internet als Tatmittel“ in den vergangenen zehn Jahren um 67 Prozent gestiegen.

Damit geht auch eine Verschiebung der Kriminalität aus einem analogen Hellfeld in ein digitales Dunkelfeld einher: Die Anzeigequote ist bei Eigentumsdelikten hoch, im Bereich Cybercrime extrem niedrig.

Die vor einer Woche veröffentlichten Ergebnisse der gemeinsamen Studie des BKA und der Polizeien der Länder „Sicherheit und Kriminalität in Deutschland“(SKiD) untermauern diese strukturelle Veränderung.

Die meisten Opfererfahrungen werden im Bereich der Cybercrime gemacht.

Mit der Digitalisierung der Kriminalität steigt auch die Menge an sichergestellten Daten. Und nicht allein die Menge, auch die Komplexität der digitalen Spuren, z.B. durch Verschlüsselung, nimmt rasant zu und erhöht die Bearbeitungsaufwände.

Gleichzeitig sind die Zeitfenster zur Entdeckung und Bearbeitung oftmals begrenzt, weil digitale Spuren häufig flüchtige Daten und somit nur vorübergehend verfügbar und nutzbar sind.

Meine Damen und Herren,

diese Entwicklung wird weitere Jahrzehnte andauern und zu noch mehr Flexibilität, Komplexität und Schnelllebigkeit führen.

Herzlich Willkommen im Jetzt – so langsam wie heute wird es nie wieder!

Bei dieser Herbsttagung stellen wir uns deshalb der Frage, wie wir mit dieser Entwicklung Schritt halten, und welche Strategien wir in einem modernen, leistungsfähigen polizeilichen Verbund verfolgen müssen.

Im letzten Jahr habe ich die Antwort hierauf aus Sicht des Bundeskriminalamtes vorgestellt. Diese lautet: Der kriminellen digitalen Vernetzung müssen wir eine polizeiliche digitale Vernetzung – dem Crime-as-a-Service ein Crimefighting-as-a-Service entgegenstellen.

Dafür braucht es einen systemischen Ansatz: die Entwicklung des BKA hin zu einer Zentralstelle der Zukunft, bestehend aus vier ineinandergreifenden Dimensionen:

Erstens: Die Polizei arbeitet im Rahmen der Plattformstrategie an und auf einer gemeinsamen digitalen Plattform mit einem Datenhaus und für alle verfügbaren Anwendungen. Das BKA entwickelt sich zu einem zentralen IT-Dienstleister der Polizei in Deutschland weiter. Fähigkeiten werden einmal entwickelt und allen Teilnehmern zur Verfügung gestellt.

Zweitens: Crimefighting-as-a-Service: Das BKA ist hierbei zentraler Service- und Solution-Provider für den polizeilichen Verbund. Es stellt finanziell und technisch anspruchsvolle Lösungen für die Kriminalitätsbekämpfung zur Verfügung.

Drittens, die digitale Eingangsstelle: Das BKA ist bereits digitale Eingangsstelle für polizeiliche Informationen aus dem Ausland – und künftig zunehmend auch für definierte Bereiche im Inland.

Viertens, Lastenausgleich: Das BKA entlastet die Länderpolizeien durch die vermehrte Übernahme von Ermittlungsverfahren und unterstützt bedarfsgerecht im polizeilichen Verbund.

Dieser Ansatz ist, davon bin ich überzeugt, nach wie vor richtig. Wir werden ihn deshalb gemeinsam mit den Polizeien der Bundesländer weiter konkretisieren und ausbauen.

Zugleich müssen wir unsere rechtlichen Rahmenbedingungen sowie unsere kriminalpolizeilichen Instrumente und Prozesse kontinuierlich überprüfen.

Werfen wir dafür einen Blick auf den Phänomenbereich Politisch motivierte Kriminalität: Die Auswirkungen der Digitalisierung hierauf stand bereits im Fokus der Herbsttagung 2019 .

Wo standen wir damals und was ist seither geschehen?

2019 mussten wir feststellen, dass Ausgrenzung, Hass und Gewalt in unserer Gesellschaft vehement nach außen getragen werden: mit dem Ziel, ein Klima der Angst zu schüren, das Vertrauen in den Staat zu unterminieren und eine eigene gesellschaftspolitische Agenda durchzusetzen.

Das Internet und soziale Medien dienten dabei als Resonanzraum für radikales Gedankengut, extremistische Ideologien und Verschwörungstheorien.

Dieses aggressive Klima gipfelte damals in dem grausamen Mord an Dr. Walter Lübcke und dem Attentat von Halle.

Und es spiegelte sich in der hohen Zahl der politisch motivierten Straftaten, derer zum Nachteil von Amts- und Mandatsträgern sowie der Straftaten im Bereich Hasskriminalität, einschließlich Antisemitismus.

Wir waren uns einig, dass die wehrhafte Demokratie ihr Instrumentarium schärfen, die roten Linien zwischen Meinungsfreiheit und Strafbarkeit klarer benennen und mit rechtsstaatlichen Mitteln auch konsequenter durchsetzen muss.

Folglich wurden unterschiedliche Maßnahmen ergriffen:

Im Bereich der Rechtsetzung erstens, das geänderte Netzwerkdurchsetzungsgesetz: Damit sind soziale Netzwerke mit mindestens zwei Millionen registrierten Nutzern in Deutschland verpflichtet, Inhalte, die ihnen in einer Beschwerde gemeldet worden sind und die sie als rechtswidrig einordnen, dem BKA zu übermitteln.

Zweitens, die Änderung des Paragraphen 126a Strafgesetzbuch: Damit wurde die Verbreitung sogenannter Feindeslisten unter Strafe gestellt.

Drittens, die Novellierung des Paragraphen 188 StGB. Dieser ermöglicht die Strafverfolgung von ehrverletzenden Angriffen bis hin zu Beleidigung von Amts- und Mandatsträgern auch auf der kommunalen Ebene.

Im BKA haben wir unsere Auswerte- und Ermittlungskapazitäten ausgebaut:

2019 habe ich hier das sogenannte 3 Ebenen-Modell– vorgestellt. Dazu gehören der personenbezogene Ansatz, die Netzwerkerkennung und die Bekämpfung von Hass und Hetze im Internet.

Das Kernstück der 3. Ebene war und ist die Einrichtung einer Zentralen Meldestelle für strafbare Inhalte im Internet, kurz ZMI, zur Entgegennahme der durch das NetzDG verpflichtenden Meldungen, im BKA.

Derzeit, Sie wissen es, sind Klageverfahren der Telemediendienstanbieter (TMDA) Google, Meta, Twitter und TikTok gegen die Bundesrepublik Deutschland wegen einzelner Verpflichtungen nach dem NetzDG anhängig.

Die aufgebauten Strukturen nutzen wir dennoch: Am 01.02.2022 ist die ZMI mit freiwilligen Kooperationspartnern in den Wirkbetrieb gestartet.

Die ZMI prüft die strafrechtliche Relevanz der von den Kooperationspartnern angelieferten Meldungen, stellt, wenn möglich, den mutmaßlichen Verfasser fest und übermittelt den Sachverhalt an die örtlich zuständigen Strafverfolgungsbehörden in den Bundesländern.

Halten wir also Schritt?

2022 müssen wir feststellen: Die Befunde von 2019 sind unverändert gültig - und die Lage ist nicht besser, sondern schlechter geworden.

Die Zahlen im Bereich der PMK erreichten 2021 mit über 55.000 Delikten einen neuen Höchststand.

Dies ist nicht nur ein Anstieg um rund 23 % gegenüber dem Vorjahr: Im Zehn-Jahres-Vergleich hat sich diese Zahl sogar nahezu verdoppelt.

Besorgniserregend ist auch die stetig steigende Anzahl von Straftaten im Bereich Hasskriminalität und Antisemitismus sowie der politisch motivierten Straftaten zum Nachteil von Amts- und Mandatsträgern: Diese Angriffe gegen das Rückgrat unserer Demokratie sind seit 2018 um mehr als 276% gestiegen.

Hass und Hetze bis hin zu Drohungen, Gewaltaufrufen und Übergriffen verbreiten sich rasend schnell – im analogen wie digitalen Raum.

Radikalisierungs- und Mobilisierungsprozesse haben sich beschleunigt und intensiviert.

Diese Entwicklung wird bestätigt durch das subjektive Empfinden und Erleben der Menschen vor Ort, in den Kommunen: Eine Kommunalstudie des BKA ergab, dass 46 Prozent der befragten Amtsträgerinnen und Amtsträger zwischen April und Oktober 2021 verbale Anfeindungen, Hasspostings im Internet und tätliche Übergriffe erlebt haben.

Mit erheblichen Folgen für die Betroffenen: 81 Prozent berichten über Folgen wie depressive Verstimmung, Angst, Konzentrationsschwierigkeiten und Rufschädigung. Mehr als jeder zehnte Betroffene hat schon einmal erwogen, sein Amt aufgrund von Anfeindungen niederzulegen.

Das Rekordhoch der PMK-Fallzahlen, aber auch das subjektive Erleben weisen auf eine Zuspitzung politischer und gesellschaftlicher Spannungen hin.

Und sie offenbaren die zumindest in einigen Bevölkerungsteilen bestehenden Radikalisierungstendenzen: Hass und Hetze sind zu einer konkreten Gefahr für unsere Demokratie und unseren gesellschaftlichen Zusammenhalt geworden.

Angesichts dieser bedrohlichen Entwicklung und der zugleich seit 2019 ergriffenen Maßnahmen müssen wir uns fragen:

Wie kann das sein? Und was müssen wir tun, um mit extremistischen Hetzern und Gewalttätern Schritt zu halten?

Ich meine: Eine wesentliche Voraussetzung dafür sind die entsprechenden rechtlichen Rahmenbedingungen bzw. die Anwendung bestehenden Rechts:

Lassen Sie es mich so deutlich sagen: In Deutschland bestimmen die Kooperationsbereitschaft der TMDA Facebook, Twitter & Co und die Geschäftsmodelle der Provider über den Erfolg, die Geschwindigkeit und den Aufwand der Strafverfolgung im Netz. Wieso behaupte ich das?

Das BKA erhält strafrechtlich relevante Hinweise auf Darstellungen von Kindesmissbrauch im Internet insbesondere über die US-amerikanische Organisation NCMEC („National Center for Missing and Exploited Children“).

Mit den Hinweisen wird in der Regel auch die zur Tatzeit dem jeweiligen Nutzer zugewiesene IP-Adresse übermittelt. Eigentlich eine optimale Ausgangssituation.

Wir werden umgehend tätig und verlangen bei dem Telekommunikationsanbieter (TK-Anbieter) die Auskunft, welchem Anschluss die IP-Adresse zum Zeitpunkt der Tat zugewiesen war.

Dennoch sind wir in vielen Fällen nicht erfolgreich, weil die IP-Adresse dort nicht mehr gespeichert ist. Denn: In Deutschland speichern die TK-Anbieter die IP-Adressen, wenn überhaupt, nur für wenige Tage.

Wir erreichen in diesem bereits stark optimierten NCMEC-Prozess und unter Einsatz aller Ermittlungsmaßnahmen eine Erfolgsquote von 75%, könnten aber über 90% erreichen, wenn die IP-Adressen bei den TK-Anbietern lang genug gespeichert würden.

Sind IP-Adressen nicht mehr verfügbar, erfolgen weitere aufwändige Maßnahmen wie beispielsweise verdeckte Ermittlungen, um den Täter doch noch identifizieren zu können.

Es gibt außerdem Fälle, in denen die IP-Adresse den einzigen Ermittlungsansatz darstellt.

Ist diese dann nicht zuordenbar, sind keine weiteren Maßnahmen zur Täteridentifizierung und Aufklärung der Straftat möglich.

Zweites Beispiel: In unserer ZMI erhalten wir, wie bereits erläutert, strafrechtlich relevante Hinweise auf Hasskriminalität im Netz.

Hier müssen wir zunächst die letzte Einwahl-IP-Adresse durch eine Bestands- und Nutzungsdatenanfrage bei den TMDA bzw. sozialen Netzwerken feststellen.

Nur selten erhalten wir hierauf eine schnelle und umfassende Antwort. Üblicherweise liegt uns eine Antwort nach etwa einer Woche vor – dann ist die mitgeteilte IP-Adresse nicht mehr zuordenbar und eine Anschlussinhaberfeststellung bei den TK-Anbietern nicht mehr möglich.

Wenn die von den TMDA beauskunfteten Bestandsdaten eines Nutzers keine Echtdaten enthalten oder inaktuell sind, ermitteln wir auch hier mit anderen Methoden, wie Open Source Intelligence.

Der Ermittlungsaufwand steigt dadurch stark an, es dauert länger und die Erfolgsquote sinkt auf 50%.

Arbeiten Anbieter gar nicht mit uns zusammen, wie beispielsweise Telegram, steigt der Aufwand noch stärker und die Erfolgsquote sinkt weiter.

Die Lösung wäre nun einfach, denn: Der Europäische Gerichtshof hat am 20. September 2022 die anlasslose Speicherpflicht für IP-Adressen ausdrücklich zugelassen – mit dem Wissen, dass das Datum zur Täteridentifizierung grundsätzlich bedeutsam und der Eingriff in die Freiheitsrechte deshalb gerechtfertigt ist: insbesondere, weil eben keine Persönlichkeitsprofile gebildet werden können.

Meine Damen und Herren,

wir wollen die Freiheitsrechte von Opfern sexualisierter Gewalt, von Cybercrime oder von Hass und Hetze im Netz konsequenter schützen können. Dafür brauchen wir zielgerichtete, erfolgsversprechende Maßnahmen zur Täteridentifizierung.

Andere, weniger effektive aber aufwändigere und zum Teil eingriffsintensivere Ermittlungsmaßnahmen binden erhebliche Ressourcen, die dann für die Bekämpfung anderer Taten fehlen.

Das können und dürfen wir uns nicht leisten. Und es ist vermeidbar.

Was wir ausdrücklich nicht wollen, ist in die Rechte Unbeteiligter eingreifen. Und diese, Sie und ich, werden durch die Speicherung von IP-Adressen in etwa so belastet wie durch ein Kraftfahrzeugkennzeichen im Straßenverkehr, das die Halterfeststellung erlaubt.

Ausreichende Speicherverpflichtungen sind allerdings nur eine Voraussetzung, um Schritt halten zu können.

Natürlich müssen wir auch unsere polizeilichen Instrumente und Prozesse der digitalen Zusammenarbeit verbessern und flexibilisieren:

Eindrücklich wurde uns das in der Sendung ZDF Magazin Royale am 27. Mai 2022 vor Augen geführt:

Jan Böhmermann präsentierte dort das Ergebnis eines Experiments zur polizeilichen Bearbeitung von Strafanzeigen im Bereich Hass im Internet.

Sein Redaktionsteam zeigte zeitgleich am 3. August 2021 sieben strafrechtlich relevante Hasskommentare bei insgesamt 16 Polizeidienststellen in allen Bundesländern an.

Angezeigt wurden auf Twitter, Telegram und Facebook veröffentlichte Morddrohungen, antisemitische, verfassungsfeindliche und rechtsextremistische Inhalte.

9 Monate nach Anzeigenerstattung informierte sich das Redaktionsteam bei den Dienststellen über den Sachstand ihrer Anzeigen.

Das Ergebnis: ernüchternd – denn der Umgang der Polizei mit den Anzeigen und den Ermittlungen war sehr unterschiedlich.

Bei vier Hasspostings konnte jeweils der Urheber ermittelt werden. Gegen zwei der Urheber wurde Anklage erhoben – ein Täter wurde verurteilt.

Greifen wir den Fall des verurteilten Täters exemplarisch heraus:

Mehrere Dienststellen haben diesen identifiziert. Welches Bundesland mit den Ermittlungen „am schnellsten“ war, lässt sich nicht klar nachvollziehen.

Drei Dienststellen haben der Redaktion die Verurteilung des Täters entsprechend beauskunftet.

Drei andere Dienststellen meldeten hingegen zurück, dass die Ermittlungen eingestellt wurden, da kein Tatverdächtiger gefunden wurde.

Drei Dienststellen teilten mit, dass die Ermittlungen noch andauern.

Während der Täter also bereits verurteilt war, waren einige Polizeidienststellen noch dabei zu ermitteln.

Eine Dienststelle hat keine Auskunft erteilt, in einer anderen war die Anzeige nicht mehr auffindbar.

Bei fünf Dienststellen ist der Status der Anzeige unklar.

Im Ergebnis haben in diesem und anderen Fällen 16 Dienststellen die gleiche Anzeige gar nicht oder parallel, jede für sich bearbeitet und sind zu unterschiedlichen Resultaten gelangt.

Insgesamt waren 18 Staatsanwaltschaften beteiligt.

Welche Erkenntnis und welche Konsequenz ziehen wir daraus?

Das Experiment zeigt, wie dringlich eine digital vernetzte, ressourcenschonende Zusammenarbeit im polizeilichen Verbund ist.

Die gute Nachricht ist: Das BKA bietet dafür bereits eine Lösung an. Wie diese aussieht, möchte ich Ihnen gleich zeigen.

Rufen wir uns zunächst in Erinnerung, wie die Polizei Verbindungen in der analogen Welt feststellt.

Analoge Spuren und Hinweise wie Fingerabdrücke, DNA oder sonstige biometrische Daten werden erhoben oder sichergestellt und im polizeilichen Informationsverbund erfasst, um diese Daten auch anderen Verbundteilnehmern zugänglich zu machen.

Bei entsprechender Abfrage ergeben sich dann Treffer, die weitere Ermittlungsansätze liefern können.

Die Digitalisierung bringt nun eine Entwicklung mit sich, die für die Polizei von großem Wert ist: Eindeutigkeit.

E-Mail-Adressen, IP-Adressen, User-Accounts: Diese Elemente der digitalen Welt haben eine Gemeinsamkeit – es gibt sie nur einmal – und sie werden überwiegend auch immer nur von einer Person genutzt. Sie sind „digitale Spuren“, sogenannte Cyber-Entitäten.

Heute beschäftigt sich die Polizei in nahezu jedem Ermittlungsverfahren mit genau diesen Cyber-Entitäten: die biometrischen Daten der neuen Welt.

In der analogen Welt würde die Polizei diese nun – meistens zeitversetzt – im Informationsverbund erfassen, damit andere Kollegen danach suchen und auf vorhandene Erkenntnisse treffen.

Eine Alternative wäre, so früh wie möglich danach zu fragen, ob jemand anders diese digitalen Spuren bereits "gesichert" hat. Fragen werden bisher mit Wissen -den erfassten Daten der Polizei - abgeglichen:

Was aber, wenn wir Fragen mit Fragen abgleichen würden?

Dann wären wir als Zentralstelle in der Lage, Kolleginnen und Kollegen mit gleichen Informationsbedürfnissen und überlappender Spurenlage miteinander zu verknüpfen.

Alle relevanten Erkenntnisse können zusammengeführt und unnötige Aufwände vermieden werden - nach dem Prinzip: Ressourcen schonen, Informationslage verdichten!

Dies wird in modernen Prozessbeschreibungen als Deconfliction bezeichnet. Und, all das machen wir bereits - in der Abteilung Cybercrime des BKA.

Wie genau das funktioniert, wird mein Kollege Mirko Manske nun erläutern:

[Einschub Einspieler]

Meine Damen und Herren,

Die Cybertoolbox ist Ausdruck eines modernen Zentralstellenverständnisses des BKA: Das Erkennen und Zusammenführen von Ermittlungen und Erkenntnissen in Bund und Ländern geschieht automatisiert und ohne menschlichen Ressourcenbedarf.

Die Erfolgschancen, den Täter zu identifizieren steigen und Doppelarbeit wird vermieden, indem quasi die „Schwarm-Intelligenz" der Polizei aktiviert wird. Deconfliction ist dabei nur eine von vielen Funktionen der Cybertoolbox.

Was folgt daraus?

Ich habe es erläutert: Kriminalität wird digitaler. Wir werden deshalb aufmerksam verfolgen, für welche weiteren Phänomenbereiche die Cybertoolbox außerdem nützlich sein kann. Hierzu stehen wir in engem Austausch mit den Polizeien der Bundesländer.

Um eine digitale Zusammenarbeit auch technisch ressourcenschonend zu ermöglichen, müssen wir außerdem die Anbindung der Cybertoolbox an bestehende polizeiliche Informationssysteme mitdenken.

Auch das tun wir bereits. So bereiten wir über ein Tool, das im Programm P 20 entwickelt wird, den Anschluss der polizeilichen Vorgangsbearbeitungssysteme an die Cybertoolbox vor. Das Roll-out ist für Ende des ersten Quartals 2023 geplant.

Halten wir also fest: Für eine erfolgreiche Kriminalitätsbekämpfung im digitalen Zeitalter brauchen wir eine eindeutige Identifizierbarkeit der Täter anhand von IP-Adressen, schnelle und vollständige Auskünfte der TMDA sowie neue innovative Tools wie Deconfliction.

Denn: Die Polizei kann sich eine ressourcenintensive Kriminalitätsbekämpfung im digitalen Raum nicht mehr leisten.

In diesem Jahr erhalten wir etwa 120.000 Hinweise vom NCMEC, Tendenz weiter steigend.

Wenn voraussichtlich 2024 der Digital Service Act in Kraft tritt, rechnen wir mit einer weiteren 6-stelligen Zahl von zu bearbeitenden Hinweisen. Wir müssen uns nach aktuellen Schätzungen auf 1 Mio. Hinweise pro Jahr bis zum Ende des Jahrzehnts einstellen.

Wir sind und werden künftig noch stärker aufgrund vielzähliger Herausforderungen intensiv gefordert sein: durch die Deliktsbereiche Sexualisierte Gewalt zum Nachteil von Kindern und Jugendlichen, Cybercrime, die Organisierte Kriminalität und Organisierte Rauschgiftkriminalität.

Lassen Sie mich die Dimensionen dieser Herausforderungen auch an einem Beispiel verdeutlichen: Das BKA ermittelt seit März 2020 im Auftrag der Generalstaatsanwaltschaft Frankfurt am Main gegen Nutzer von kryptierten Mobiltelefonen.

Diese werden schwerster Straftaten verdächtigt. Grundlage waren Ermittlungen eines Ermittlungsteams aus Frankreich, der Niederlande, von Europol und Eurojust.

Welche unterstützende Methode wir bei unseren Ermittlungen erfolgreich angewandt haben, zeigen wir Ihnen jetzt: mit einem Blick in die Arbeit unserer Abteilungen Schwere und Organisierte Kriminalität und Operative Einsatz- und Ermittlungsunterstützung:

[Einschub Einspieler]

Meine Damen und Herren,

bislang war nur die Spitze des Eisberges sichtbar. Die Auswertung der Daten hat uns gezeigt, was unter der Wasseroberfläche liegt und einen tiefen Einblick in die Strukturen der organisierten Rauschgiftkriminalität in Deutschland ermöglicht.

Die Zahl der Ermittlungsverfahren im Phänomenbereich der OK hat 2021 einen neuen Höchststand erreicht: im Wesentlichen ist das auf Ermittlungsverfahren im Zusammenhang mit der Nutzung von kryptierter Kommunikation zurückzuführen.

Die Täter arbeiten hochkonspirativ, sind anonym vernetzt und immer häufiger bewaffnet.

Die OK verdient Milliarden: Das kriminell erworbene Geld wird dann in neue Straftaten investiert oder für legale Geschäftsmodelle genutzt.

Damit besteht auch die Gefahr, dass das Gewaltmonopol des Staates unterwandert wird: Diese Dimension der OK wird in der Niederlande bereits beobachtet und als „Undermining“ bezeichnet. Auch in Belgien hat jüngst die vereitelte Entführung des Justizministers die von der OK ausgehende Gewalt gegen den Staat offenbart.

Meine Damen und Herren,

Frau Ministerin hat es mit der von ihr vorgestellten Strategie zur Bekämpfung der OK verdeutlicht.

Wir müssen hier einen eindeutigen Schwerpunkt setzen und es muss uns bewusst sein: Das im Film gezeigte Beispiel war kein Einzelfall.

In Zukunft werden wir mit Fallkomplexen ähnlicher Dimensionen konfrontiert sein.

Und mit solchen, deren Ausmaße wir noch gar nicht absehen können. Denn solche Erfolge im digitalen Zeitalter bedeuten immer riesige Vorgangszahlen und Datenmengen, auf die wir schnell und koordiniert im polizeilichen Verbund reagieren müssen.

Das Beispiel zeigt auch, dass die Zentralstelle der Zukunft im Sinne von Plattformstrategie, Crimefighting-as-a-Service, digitaler Eingangsstelle und Lastenausgleich ein wegweisender Ansatz ist.

Wir müssen aber innerhalb dieser Dimensionen mit- und vorausdenken, welche weiteren Anwendungsfälle, welche -varianten es geben könnte - und wie wir sich bewährende Methoden und Tools weiterentwickeln

Die Täter weichen längst zur nächsten Kryptierungstechnik aus: Es gilt deshalb, in die technische Unterstützung bei der Dekryptierung und Auswertung von Daten mittels KI zu investieren.

Für die Auswertung von Massendaten ist zudem die Implementierung eines gemeinsamen technischen Bund-Länder-Auswertenetzwerkes unabdingbar: Die für den sicheren Beweismitteltransport notwendige IT-Architektur wird im Rahmen der Plattformstrategie entwickelt.

Im Sinne von Crimefighting-as-a-Service hat das BKA die Zentrale Clearingstelle Tool- und Methodenentwicklung (ZCS TME) eingerichtet – mit dem Ziel, Doppelarbeit und Insellösungen im Bereich der Software-Entwicklung zu vermeiden.

Die Clearingstelle konsolidiert Bedarfe von Bund und Ländern und ermöglicht die unbürokratische Weitergabe von Software-Tools für die kriminalpolizeiliche Datenanalyse.

Wenn für einen Bedarf noch keine Lösung vorliegt, unterstützt die Clearingstelle bei der Lösungsfindung.

Diesen Ansatz haben wir während der deutschen EU-Ratspräsidentschaft 2020 auch auf europäischer Ebene etabliert: Mit dem European Clearing Board unter dem Dach von Europol treiben wir die Zusammenarbeit bei der Tool- und Methodenentwicklung voran und sorgen dafür, dass wir mit unseren europäischen Partnern im Gleichschritt Schritt halten!

Durch die Erhöhung der Ermittlungskapazitäten im Phänomenbereich Islamistischer Terrorismus haben wir im BKA schon Komponenten eines Lastenausgleichs eingeführt.

Es gilt nun, diesen Lastenausgleich angesichts komplexer, technisch anspruchsvoller Verfahren - zum Teil mit internationalen Bezügen – auszudehnen: auf Rauschgift- und OK-Delikte, Wirtschafts- und Finanzkriminalität, Cybercrime und Sexualdelikte zum Nachteil von Kindern und Jugendlichen.

Darüber hinaus kann das BKA anderweitig bedarfsgerecht im polizeilichen Verbund - Beispiel Netzwerkanalyse – oder mit weiteren hochspezialisierten Fähigkeiten unterstützen.

Inwieweit dies möglich ist, hängt allerdings auch von der weiteren Entwicklung der finanziellen und personellen Ressourcen für diese Bereiche im BKA sowie der Anpassung notwendiger rechtlicher Grundlagen ab.

Wie halten wir Schritt? – ist die Leitfrage der Herbsttagung. Richtung vor Geschwindigkeit ist die Antwort.

Die Anpassung an eine dynamische Umwelt, an politische und gesellschaftliche Veränderungen bleibt ein Langstreckenlauf.

Die richtige Reaktion war und ist ein systemischer Ansatz: die Entwicklung des BKA hin zu einer Zentralstelle der Zukunft – in dem Bewusstsein, dass wir nur so stark sind, wie der Verbund stark ist. Das gilt für den nationalen, den europäischen, mit Blick auf Phänomene wie Cybercrime auch für den internationalen Verbund.

Aber: Morgen ist heute bereits gestern. Um für komplexe Herausforderungen, die wir zum Teil noch nicht einmal kennen, vorbereitet zu sein, müssen wir unsere Anpassungsfähigkeit beschleunigen und neue flexible Prozesse, Methoden und Tools entwickeln.

Die Bürgerinnen und Bürger haben zurecht hohe Erwartungen an die Handlungsfähigkeit der Polizei und vertrauen darauf, dass die Kriminalitätsbekämpfung mit der Kriminalität Schritt hält.

Um diesen Erwartungen wie auch unserem eigenen Anspruch daran gerecht zu werden, muss die Polizei sich anpassen und anpassen können: Das heißt, dass die

Rahmenbedingungen – insbesondere mit Blick auf technische Entwicklungen – der Lebenswirklichkeit in einer digitalisierten und hochgradig vernetzten Gesellschaft entsprechen müssen.

Das Internet darf in Deutschland weder ein rechtsfreier noch ein rechtsdurchsetzungsfreier Raum sein.

Für eine zeitgemäße Kriminalitätsbekämpfung darf unser Ziel allerdings nicht nur sein, im Außenverhältnis, mit den kriminellen Tätern, Schritt zu halten.

Wir müssen der zunehmenden Vernetzung der Kriminalität zugleich mit einer wachsenden Vernetzung bei uns selbst begegnen: hin zu einer Netzwerkorganisation. Nur so können wir die notwendige Kreativität, Flexibilität und Geschwindigkeit in unseren Organisationen entfachen.

Meine Damen und Herren,

ich schließe mich meiner Kollegin Elena Weike und meinem Kollegen Mirko Manske an: Auch ich bin gespannt auf die Zukunft – und überzeugt davon, dass wir sie im polizeilichen Verbund gemeinsam sicher gestalten werden.

Wie uns das am besten gelingt, werden wir in den kommenden zwei Tagen analog hier auf der Bühne, aber auch virtuell vernetzt mit Ihnen diskutieren. In diesem Sinne: Legen wir los!