



Brüssel, den 22. November 2019
(OR. en)

14297/19

LIMITE

**COSI 239
ENFOPOL 508
ENFOCUSTOM 196
FRONT 333
DAPIX 346
CYBER 322
JAI 1217**

VERMERK

Absender:	Vorsitz
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Betr.:	Die künftige Ausrichtung im Bereich der inneren Sicherheit der EU – Ergebnisse der Beratungen – Bericht des Vorsitzes

Das sich rasch verändernde Sicherheitsumfeld erfordert einen integrierten Ansatz zur Bewältigung neuer Bedrohungen und Herausforderungen. Ein umfassender Ansatz für die innere Sicherheit ist ein gangbarer Weg, um immer komplexere und vielfältigere Bedrohungen zu bewältigen, sodass eine gesamtgesellschaftliche Herangehensweise für die Antworten möglich ist.

Bei der Umsetzung der Strategischen Agenda 2019-2024 im Bereich Justiz und Inneres hat der Vorsitz eine Reihe thematischer Gespräche ausgerichtet, um die Überlegungen über das weitere Vorgehen in Bezug auf die künftige Ausrichtung der inneren Sicherheit in der EU zu vertiefen. Der Vorsitz hat als Richtschnur für diese Überlegungen drei Grundprinzipien dargelegt: Angebot eines Raums der Freiheit, der Sicherheit und des Rechts für die EU-Bürgerinnen und -Bürger, Bekämpfung der sozialen Ausgrenzung und der Diskriminierung und Förderung der Werte der Union.

Die Gespräche wurden im Juli 2019 auf der informellen Tagung des Ständigen Ausschusses für die operative Zusammenarbeit im Bereich der inneren Sicherheit (COSI) zur Vorbereitung der informellen Tagung des Rates (Justiz und Inneres) (JI) aufgenommen; dabei wurde auf eine Reihe von horizontalen Kernthemen eingegangen¹. Thematische Gespräche gab es auch in den einschlägigen Arbeitsgruppen, wie etwa in den Gruppen „Strafverfolgung“ (LEWP), „Terrorismus“ (TWP) und „Informationsaustausch und Datenschutz“ (DAPIX – Informationsaustausch); die Gespräche wurden im COSI im Hinblick auf die Ministeraussprache weiter vorbereitet. Eine Reihe von Themen wurde ausführlich behandelt, z. B. die Verbesserung des Rahmens für die operative Zusammenarbeit bei der Strafverfolgung, die Auswirkungen neuer Technologien und hybrider Bedrohungen auf die innere Sicherheit, die Rolle der JI-Agenturen der EU, Informationsmanagement und -automatisierung sowie Schulungen für die Strafverfolgungsbehörden. Die Themenbereiche der Aussprachen sind in den für die verschiedenen Sitzungen erstellten Papieren im Einzelnen dargelegt und in der Anlage aufgeführt.

In diesem Bericht werden ausgewählte Aspekte behandelt, die dem Standpunkt des Vorsitzes zu den wichtigsten Fragen entsprechen, die sich aus den betreffenden Aussprachen für den Gesetzgebungszyklus 2019-2024 ergeben.

1. Proaktive Herangehensweise an die neuen Technologien

Technologische Entwicklungen haben erhebliche Auswirkungen auf das Leben der EU-Bürger und -Bürgerinnen und damit auf die Arbeit der Strafverfolgungsbehörden. All diese Entwicklungen, wie etwa künstliche Intelligenz, unbemannte Luftfahrzeuge, neue Kommunikationsnetze und Online-Umgebungen, um nur einige zu nennen, können die Arbeit der Behörden unterstützen, lassen sich aber auch für illegale Zwecke nutzen. So können sowohl Strafverfolgungsbehörden als auch Ersthelfer beispielsweise bei der Arbeit zur Bekämpfung des Terrorismus bzw. nach einem Terroranschlag von Drohnen Gebrauch machen. Das zunehmende Innovationstempo ist eine Herausforderung für die Fähigkeit der Strafverfolgungsbehörden, sich an die in rascher Entwicklung begriffene technologische Welt anzupassen. Im Zusammenhang mit der Digitalisierung wäre zu bewerten, inwieweit die rechtlichen Rahmenwerke, innerhalb deren die Strafverfolgungsbehörden und die zuständigen EU-Agenturen tätig sind, dem aktuellen Bedarf entsprechen². Die Wahrung und Förderung der Grundrechte sollte bei allen derartigen Entwicklungen die Grundlage bilden; gleichzeitig sollte den sich aus dem Datenschutzrahmen ergebenden strengen Anforderungen an die Strafverfolgungstätigkeiten entsprochen werden, wobei die Union eine Führungsposition bei der Normensetzung einnimmt.

¹ Papier des Vorsitzes über die künftige Ausrichtung der inneren Sicherheit in der EU (Dok. WK 13264/19)

² Dokumente 12496/19 und 12224/19 über neue Technologien und innere Sicherheit.

Ziel ist es, der Strafverfolgung in der EU eine proaktive Rolle zu verleihen, damit sie von den neuen Technologien profitieren kann, während gleichzeitig die damit verbundenen Risiken antizipiert und kontrolliert werden. Auf diesem Gebiet bedarf es eines integrierten, umfassenden Ansatzes auf der Ebene der EU. Die Einrichtung eines gemeinsamen Innovationslabors bei Europol, mit dem technische Entwicklungen und Tendenzen sowie Innovation und Forschung genutzt werden sollen und ihre potenzielle Bedeutung für die Strafverfolgung und den Dialog mit Industrie und Wissenschaft bewertet werden soll, dient diesem Ziel. Die vollständige Nutzung der neuen Technologien erfordert kontinuierliche Forschung und Schulung. Die Zentralisierung bestimmter Tätigkeiten und die Bündelung der Ergebnisse der Arbeit bestehender Netzwerke innerhalb des Innovationslabors würden Vorteile in Form von Rationalisierungen und Kosteneffizienz mit sich bringen, insbesondere in Bereichen, in denen die Mitgliedstaaten nicht über ausreichende Mittel verfügen, um alleine zu handeln oder in denen mit gemeinsamem Handeln und dem Austausch bewährter Verfahren ein Mehrwert verbunden ist.

Da technologische Forschung und Entwicklung häufig in Hochschulen und im Privatsektor stattfinden, sind die Strafverfolgungsbehörden erst in einem relativ späten Stadium eingebunden. Um den Anliegen der Strafverfolgungsbehörden für die Zukunft Rechnung zu tragen, sollten nach Auffassung des Vorsitzes Anstrengungen mit dem Ziel unternommen werden, die Strafverfolgungsbehörden proaktiv von Anfang an in die Prozesse der technologischen Entwicklung einzubinden; hierzu sollten insbesondere die Teilnahme von Fachleuten der Strafverfolgung und die Koordinierung zwischen ihnen bei mit EU-Mitteln finanzierten Forschungs- und Entwicklungsprogrammen im Bereich der Sicherheit weiter verstärkt werden.

Der Vorsitz ermutigt die Strafverfolgungsbehörden, proaktiv an der Entwicklung neuer Technologien mitzuwirken. Das Innovationslabor sollte als Plattform zur Unterstützung dieses Ziels dienen. Es ist wichtig, dass die Bedürfnisse der Strafverfolgungsbehörden bei der Entwicklung neuer Technologien, die ihre Arbeit beeinflussen oder für eine wirksamere Reaktion vonseiten der Strafverfolgung erforderlich sind, schon frühzeitig bekannt sind und berücksichtigt werden. Darüber hinaus sollten die Interessen der inneren Sicherheit und der Strafverfolgung in Rechtsvorschriften zu neuen Technologien besser berücksichtigt werden, um Beschränkungen im Rechtsrahmen abzumildern, indem ihnen insbesondere in Bedrohungsanalysen systematisch Rechnung getragen wird.

2. Wirksames Informationsmanagement

Die Zusammenarbeit bei der Strafverfolgung auf EU-Ebene wird zunehmend auf bessere und effizientere technische Lösungen und Informationssysteme sowie auf deren Interoperabilität gestützt³. Im Zeitalter großer Mengen digitaler Daten haben die Strafverfolgungsbehörden Zugang zu mehr Daten und Informationen als je zuvor. Dies muss sich in den technischen Lösungen und den Kapazitätsangeboten niederschlagen. Zugleich fehlt es an grundlegenden Statistiken zu verschiedenen Kriminalitätsbereichen. Daher ist es besonders wichtig, dafür zu sorgen, dass die Informationssysteme mit vollständigen Daten von hoher Qualität bestückt und wirksam genutzt werden. Wir müssen sicherstellen, dass die zuständigen nationalen Behörden Zugang zu diesen Systemen haben und ausreichend geschult werden, damit sie sie umfassend nutzen können.

Nach wie vor bildet die Kriminalanalyse den Kern der Strafverfolgung. Die Analyse liefert den Mehrwert für Rohdaten, der sie in verwertbare Informationen umwandelt, die sowohl auf nationaler Ebene als auch bei grenzüberschreitenden Einsätzen in der gesamten EU verwendet werden können. Es mangelt jedoch an einer klaren Vision für Standards auf EU-Ebene für Kriminalanalysetätigkeiten, die aber benötigt wird. Jedenfalls ist die Analyse ein integraler Bestandteil aller Informationsprozesse innerhalb der Strafverfolgung. Dies erfordert ausreichende personelle und finanzielle Ressourcen, um die Informationen zu verarbeiten und zu analysieren. Für die erfolgreiche Verbesserung und Standardisierung der Analyse bedarf es daher eines besseren Verständnisses der Erfordernisse der Strafverfolgung insgesamt und der verschiedenen beteiligten Informationsprozesse im Einzelnen, auch derjenigen der strafrechtlichen Ermittlung und der Gewinnung kriminalpolizeilicher Erkenntnisse.

Die Interoperabilitätsverordnungen⁴ sind am 11. Juni 2019 in Kraft getreten. Die Gewährleistung einer effizienten Umsetzung der Verordnungen ist von kritischer Bedeutung. Die technologische Revolution bei den IT-Systemen der EU wird sowohl auf EU-Ebene als auch in den Mitgliedstaaten eine große Menge an Ressourcen und die Einhaltung des Zeitplans erfordern. Beim Aufbau der Interoperabilitätsarchitektur ist es wichtig, dass technische Lösungen stets den Bedürfnissen der Endnutzer Rechnung tragen. Darüber hinaus ist es von entscheidender Bedeutung, den Endnutzern eine angemessene und kontinuierliche Schulung bereitzustellen, damit sie in der Lage sind, diese neuen Informationssysteme zu nutzen und ihre Interoperabilität zu vervollständigen. Es ist klar, dass Interoperabilität mehr bedeutet als die bloße Entwicklung von IT-Systemen; sie setzt auch ein Umdenken voraus. Die erfolgreiche Umsetzung erfordert daher auch eine Änderung unserer Praxis- und Verwaltungskultur.

³ Dok. 13510/19: EU-Informationsmanagement – Informationsautomatisierung, -zugang, -austausch und -analyse.

⁴ Verordnungen (EU) 2019/817 und (EU) 2019/818.

Aus einer breiteren Perspektive heraus ist ein verbesserter Informationsaustausch nicht nur eine technologische Entwicklung. Um die gewünschten Vorteile zu erzielen, muss sichergestellt werden, dass Kompetenzen, Ressourcen und Endnutzerschnittstellen auf nationaler Ebene ihren Zweck erfüllen können. Informationen sind kein absoluter Wert an sich – sie müssen genutzt werden und zu Maßnahmen führen können. Ohne eine ordnungsgemäße Umsetzung könnten die betreffenden Entwicklungen und die mit ihnen verbundenen Vorteile beeinträchtigt werden.

Außer auf wirksame Ermittlungen sollten sich die Strafverfolgungsbehörden bei ihrer Arbeit in gleichem Maße auch auf Kriminalitätsprävention und -unterbindung konzentrieren. Hochwertige, am richtigen Ort und zur richtigen Zeit verfügbare Informationen tragen zu diesem Ziel bei. In Bezug auf die erkenntnisgestützte Strafverfolgung sind Europol und Frontex in einer hervorragenden Ausgangsposition, um diese Arbeit mit ihren Analysefähigkeiten zu unterstützen, unter anderem durch einen breiteren Zugang zum Schengener Informationssystem (SIS), soweit die Mitgliedstaaten ihnen systematisch Rohdaten von hoher Qualität zur Verfügung stellen.

Der Vorsitz ruft zu einem umfassenden EU-Rahmen für das Informationsmanagement auf, um sicherzustellen, dass alle benötigten existierenden Informationen rasch zugänglich sind und schnell verarbeitet und ausgetauscht werden, damit ein erkenntnisgestütztes Handeln möglich wird.

3. Multidisziplinäre grenzüberschreitende Zusammenarbeit

Die Verbesserung der sektorübergreifenden operativen Zusammenarbeit durch die Verringerung von Doppelarbeit und die Verstärkung der wirksamen Koordinierung ist eine Grundvoraussetzung für erfolgreiche Maßnahmen. Da sich die verschiedenen Sicherheitsbedrohungen, wie etwa CBRN-Waffen und hybride Aktivitäten, ständig weiterentwickeln, erfordern die Maßnahmen, die ergriffen werden, um auf diese Tätigkeiten zu reagieren und diesen vorzubeugen, einen horizontalen Ansatz, wobei der Zuständigkeit der Mitgliedstaaten für Fragen der nationalen Sicherheit Rechnung zu tragen ist. Es bedarf eines integrierten und kohärenten Ansatzes, um eine multidisziplinäre operative Zusammenarbeit zu gewährleisten, die über die grenzüberschreitende Zusammenarbeit bei der Strafverfolgung hinausgeht und auch andere Behörden, wie etwa Akteure des Katastrophenschutzes, einbezieht.

Unterschiede in den nationalen Entscheidungsprozessen, Rechtsvorschriften und operativen Modellen stellen große Herausforderungen für die operative grenzüberschreitende Zusammenarbeit dar. Darüber hinaus behindern Inkohärenzen in der nationalen Datenerhebungs- und -verarbeitungspraxis, die sich aus den Unterschieden zwischen den einzelnen Mitgliedstaaten in Bezug auf Verwaltungssysteme, technische Lösungen und funktionale Vorkehrungen ergeben, die grenzüberschreitende Zusammenarbeit. Eine weitere Herausforderung besteht darin, die Hindernisse für die operative Zusammenarbeit zwischen den Strafverfolgungsbehörden zu ermitteln und zu beseitigen, wie etwa inkompatible Funkfrequenzen in Grenzgebieten und Sprachbarrieren, sowie in der Notwendigkeit, die bestehenden Rechtsgrundlagen durch detailliertere bilaterale Übereinkünfte zu ergänzen. In dringenden Fällen sind sich die nationalen Stellen möglicherweise nicht der Bandbreite der operativen Alternativen, die in mehrere EU-Instrumente aufgespalten sind, und der verfügbaren Informationskanäle bewusst.

Die multidisziplinäre operative Zusammenarbeit zwischen den Strafverfolgungsbehörden sollte intensiviert werden, indem neue Methoden der Zusammenarbeit und des Informationsaustauschs entwickelt und genutzt werden, wobei auf neue technologische Anwendungen und Instrumente zurückgegriffen wird. Diese Anwendungen können beispielsweise unbemannte autonome Systeme, automatische Kennzeichenerkennungstechnik oder zentrale Suchschnittstellen für die verfügbaren Datenbanken umfassen. Es gibt eine klare Dynamik, und es besteht die Chance, diese Entwicklung fortzuführen und weiter zu unterstützen.

Lebensbegleitendes Lernen und Weiterbildung sind noch wichtiger, wenn es darum geht, alle bestehenden Möglichkeiten auszuschöpfen und sich auf künftige Herausforderungen vorzubereiten. Die von den EU-Agenturen angebotenen Schulungen müssen effizient genutzt werden. Zugleich muss sichergestellt werden, dass sich die Tätigkeiten der EU-Agenturen gegenseitig ergänzen und Überschneidungen beseitigt werden.

Wir müssen regionale Unterschiede und nationale Besonderheiten berücksichtigen und gleichzeitig eine gemeinsame Strafverfolgungskultur unter den Strafverfolgungsbehörden in der EU anstreben. Die Verbesserung der Sprachkenntnisse, das Lernen von den Kulturen aller anderen und der Austausch bewährter Verfahren tragen dazu bei, regionale und kulturelle Unterschiede besser zu verstehen und das gemeinsame Ziel zu unterstützen.

Bilaterale und multilaterale Vereinbarungen sind nach wie vor wichtig für die lokale und regionale Zusammenarbeit, und es bedarf der Flexibilität bei der Gewährleistung der Achtung der regionalen Vielfalt und der unterschiedlichen operativen Interessen. Die Festlegung der Aufteilung der Verantwortung, der Zuständigkeit sowie der hoheitlichen Aufgaben muss bei allen künftigen Entwicklungen berücksichtigt werden.

Die JI-Agenturen der EU spielen weiterhin eine wichtige Rolle bei der Unterstützung der Bemühungen der Mitgliedstaaten im Rahmen ihrer jeweiligen Mandate. Es wird allgemein anerkannt, dass eine echte grenzüberschreitende Zusammenarbeit zwischen den Behörden der Mitgliedstaaten, die von den zuständigen EU-Agenturen nachdrücklich unterstützt wird, der beste Weg ist, um zu einer Sicherheitsunion zu gelangen und sowohl bestehende als auch neue Bedrohungen in einem sich ständig wandelnden Umfeld auf nachhaltige Weise anzugehen⁵.

Die künftigen Entwicklungen im Bereich der inneren Sicherheit würden daher eine weitere aktive Rolle der Agenturen erfordern, die mit einem erwarteten Anstieg des Umfangs der bestehenden Aufgaben und neuen Verantwortlichkeiten, die sich aus dem politischen und dem operativen Bedarf ergeben, verbunden wäre. Angesichts der begrenzten Ressourcen ist es notwendig, den Kontext zu erörtern, in dem die Agenturen am wirksamsten einen Mehrwert schaffen können, wie etwa in Bereichen, in denen die Mitgliedstaaten möglicherweise einen Zugang zu Ressourcen oder technischer Ausrüstung durch die Bündelung von Ressourcen benötigen und in denen die Kapazitäten für die Datenanalyse verbessert werden könnten und eine stärkere operative Unterstützung möglich wäre. Es sollten transparente Kriterien festgelegt werden, um zu entscheiden, in welchen Bereichen die Mitgliedstaaten die meiste Unterstützung benötigen, wobei der technologische Fortschritt und der spezifische materielle oder sonstige Bedarf an Ressourcen berücksichtigt werden. Bei der Entwicklung der Rolle der Agenturen sollte eine ausgewogene Lösung angestrebt werden, die den Bedürfnissen der Mitgliedstaaten Rechnung trägt. Es ist von wesentlicher Bedeutung, einen koordinierten und ganzheitlichen Ansatz zu verfolgen, um die Kernkompetenz und die Hauptstärken jeder Agentur zu stärken und auf kosteneffiziente Weise einen Mehrwert zu schaffen, ohne dass es zu Überschneidungen bei Aufgaben und Funktionen kommt.

Ein vertiefter Informationsaustausch und eine vertiefte Zusammenarbeit, die sich auf die Agenturen stützen, sind notwendig, da die bestehenden und die sich abzeichnenden Bedrohungen der inneren Sicherheit in ihrer Art zunehmend komplexer werden und immer mehr grenzüberschreitenden Charakter haben. Es besteht auch Bedarf an einer wirksameren Interaktion mit privaten Parteien im Rahmen des Informationsaustauschs. Insbesondere ist es notwendig, die Rechtsgrundlage von Europol dafür, personenbezogene Daten direkt von privaten Parteien anzufordern und zu erhalten, zu überprüfen⁶.

⁵ Die Rolle der EU-Agenturen wurde von der COSI-Gruppe (Inneres) und dem Rat (Inneres) im Juli speziell erörtert (Dok. WK 13271/19 und WK 13266/19) und war Querschnittsthema in allen Debatten.

⁶ Gespräche über die Zusammenarbeit von Europol mit privaten Parteien haben in der Gruppe „Strafverfolgung“ stattgefunden: Dok. 10494/19, 11832/19 und 12858/1/19.

Um den multidisziplinären Strafverfolgungsansatz von Europol langfristig zu stärken, sollte die Zusammenarbeit zwischen den Zollbehörden und Europol weiterentwickelt werden, indem die Zahl der Verbindungsbeamten des Zolls bei Europol erhöht, die Nutzung von SIENA durch den Zoll in allen EU-Mitgliedstaaten gefördert und der regelmäßige und strukturierte Informationsaustausch zwischen den Parteien – unter Einschluss von Risikomanagement und Erkenntnissen – verbessert wird. Ein kurzfristiges Ziel sollte darin bestehen, den Beitrag des Zolls zu stärken und ihn in die Umsetzung der operativen Aktionspläne im Rahmen von EMPACT einzubeziehen. Diese Maßnahmen würden die in den letzten Jahren zu verzeichnende positive Entwicklung der Zusammenarbeit zwischen Zoll und Europol fortsetzen.

Die Herausforderungen bei der Zusammenarbeit zwischen der Europäischen Union und Interpol müssen angegangen werden. Es ist wichtig, dass Datenbanken, die als wichtige Informationsquellen für die Strafverfolgungszusammenarbeit mit Drittländern dienen, auch künftig von den Behörden der EU-Mitgliedstaaten wirksam genutzt werden. Gleichzeitig müssen die geltenden Datenschutzvorschriften selbstverständlich in vollem Umfang eingehalten werden.

Der Vorsitz unterstreicht die Notwendigkeit einer Überprüfung des Rechtsrahmens für die grenzüberschreitende Zusammenarbeit bei der Strafverfolgung und des Mandats von Europol, um es an die aktuellen Gegebenheiten und künftigen Herausforderungen anzupassen. Die Entwicklung einer gemeinsamen Strafverfolgungskultur unter den Strafverfolgungsbehörden in der EU sollte weiter unterstützt werden.

4. Umfassender Ansatz für die innere Sicherheit

Es steht zu erwarten, dass in naher Zukunft eine Reihe von Tendenzen und Entwicklungen zu verzeichnen sind, die sich auf die Bedrohungslage in der EU auswirken werden. Die Kriminalität wird weiterhin von der Nachfrage und der Verfügbarkeit von Möglichkeiten für kriminelles Handeln angetrieben. Darüber hinaus stellen die Veränderungen der Sicherheitslage in den Nachbarregionen und verschiedene Formen der gewaltbereiten Radikalisierung in Europa weiterhin eine Bedrohung für unsere innere Sicherheit dar. Ein umfassender Ansatz für die Sicherheit mit einer verbesserten Koordinierung, besseren Ressourcen und besseren technologischen Kapazitäten erfordert ein besseres Lagebewusstsein und eine bessere Abwehrbereitschaft in Bezug auf eine Vielzahl von Herausforderungen.

Strafverfolgung, Katastrophenschutz und andere einschlägige Behörden sollten ihre Bereitschaft zur Abwehr hybrider Bedrohungen weiter ausbauen. Die Zusammenarbeit bei der Prävention und Abwehr hybrider Bedrohungen zwischen den zuständigen nationalen Behörden auf der Grundlage ihrer jeweiligen Mandate sowie den EU-Organen, -Einrichtungen und -Agenturen im gesamten Bereich der Verknüpfung von innerer und äußerer Sicherheit muss kontinuierlich verbessert und durchgängig berücksichtigt werden. Gleichzeitig ist es wichtig, dass Synergien verstärkt und Doppelarbeiten vermieden werden, unter anderem durch horizontale Arbeitsmethoden, einen verstärkten Informationsaustausch sowie bereichsübergreifende Schulungen und Übungen.

Es wird betont, dass die Beratungen über die interne Dimension hybrider Bedrohungen fortgesetzt werden müssen, insbesondere in Bezug auf die Rolle der JI-Agenturen bei der Stärkung der Fähigkeiten der EU und der Mitgliedstaaten zur Feststellung hybrider Handlungen und ihrer Quellen.

Ferner erfordert auch die wirksame Bekämpfung von Desinformation einen umfassenden Ansatz. In diesem Sinne sollte die Beteiligung der Strafverfolgungsbehörden – auch an bestehenden EU-Mechanismen wie etwa dem Schnellwarnsystem – in Betracht gezogen werden. Die Strafverfolgungsbehörden stärken die Widerstandsfähigkeit der EU und ihrer Mitgliedstaaten, und der Bekämpfung von Desinformation muss Rechnung getragen werden⁷. Der Vorsitz betont, dass das bestehende Instrumentarium besser genutzt und die ganzheitliche Koordinierung auf EU-Ebene verbessert werden muss. In diesem Zusammenhang muss auch auf die Unterstützung der JI-Agenturen für die Mitgliedstaaten eingegangen werden.

Die Nutzung von Technologie und des Internet bei kriminellen Aktivitäten wird weiter zunehmen. So wird beispielsweise die Nutzung von Online-Plattformen sowohl im Oberflächen-Web als auch im Darkweb für den Handel mit einer breiten Palette illegaler Waren voraussichtlich zunehmen. Darüber hinaus kann der Online-Bereich wirksam dazu missbraucht werden, um zu radikalisieren, zu rekrutieren und zu Gewalt anzustacheln. Der Verbreitung von terroristischen Internetinhalten und von Online-Kindesmissbrauchsinhalten sollte effizient vorgebeugt werden, und die betreffenden Inhalte sollten rasch unzugänglich gemacht werden.

⁷ Hybride Bedrohungen und innere Sicherheit : strategische Kommunikation und Bekämpfung von Desinformation bei der Strafverfolgung (Dok. 11831/19).

Darüber hinaus wird die Rolle der Prävention der gewaltbereiten Radikalisierung als integraler Bestandteil eines umfassenden Ansatzes zur Terrorismusbekämpfung hervorgehoben. Bei der Prävention und Bekämpfung des gewaltbereiten Extremismus spielen die Kontaktaufnahme mit den an vorderster Front tätigen Praktikern und deren Unterstützung weiterhin eine entscheidende Rolle. Es ist notwendig, gegen den politisch oder ideologisch motivierten gewaltbereiten Extremismus in all seinen Formen vorzugehen. Künftig sollte der Schwerpunkt weiterhin auf die Bekämpfung und Prävention von gewaltbareitem Extremismus und Terrorismus gelegt werden, wobei ein breit angelegter Ansatz verfolgt werden sollte, bei dem auch die sich abzeichnenden Tendenzen beim gewaltbereiten Extremismus berücksichtigt werden.

Die Bedrohung durch gewaltbereiten Rechtsextremismus und durch Rechtsterrorismus muss angegangen werden, indem ein besseres Lagebild geschaffen wird, bewährte Verfahren kontinuierlich ausgetauscht werden, mit wichtigen Drittstaaten zusammengearbeitet wird und die Verbreitung rechtswidriger rechtsextremistischer Inhalte – sowohl online als auch offline – bekämpft wird. Die Herausforderung der zurückkehrenden ausländischen terroristischen Kämpfer sollte angegangen werden, auch durch eine effizientere Nutzung des SIS.

Der Vorsitz betont, dass ein umfassender und gesamtgesellschaftlicher Sicherheitsansatz erforderlich ist, um verschiedene Bedrohungen der inneren Sicherheit anzugehen. Es wird betont, wie wichtig es ist, in allen relevanten Politikbereichen auf eine stärker strategische, koordinierte und kohärente Art und Weise zu arbeiten.

Subject	Meeting	Reference Number
Future Direction of internal security in the EU	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13264/19
Hybrid threats and internal security	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13265/19
Twenty Years of Europol - what next?	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13266/19
The future of EU Internal Security	Informal Council meeting on 18-19 July 2019, Helsinki	WK 13271/19
The future direction of EU internal security: new technologies and internal security	JHA Council on 2 October 2019	12496/19
Hybrid threats and Internal Security	JHA Council on 2 October 2019	12495/19
Right-wing violent extremism and terrorism	JHA Council on 2 October 2019	12494/19
EU Information Management - Automation, access to, sharing of, and analysis of information	COSI meeting on 19 November 2019	13510/19
The future of EU law enforcement: Training for law enforcement	COSI meeting on 19 November 2019	13973/19