

**Arbeitstagung  
des Vorstands der CSU-Landtagsfraktion  
am 12. Januar 2026  
in Kloster Banz**



**„Für ein sicheres Bayern: Moderne  
Antworten auf Kriminalität“**

1 Bayern gehört seit Jahren zu den sichersten Regionen Deutschlands. Dieser Anspruch  
2 bleibt für uns Maßstab und Verpflichtung zugleich. Unser Ziel ist klar: Bayern soll auch  
3 in Zukunft das sicherste Bundesland bleiben! Deshalb bleiben wir bei unserem  
4 entschlossenen, modernen und rechtsstaatlich fundierten Vorgehen gegen Kriminalität  
5 in all ihren Erscheinungsformen. Doch: Kriminalität zeigt immer neue Facetten.  
6 Sicherheitspolitik muss Schritt halten. Deshalb braucht es für unsere  
7 Polizeibeamtinnen und -beamten wie auch für die Staatsanwaltschaften eine  
8 rechtliche Arbeitsbasis, die beständig modern und zeitgemäß verändert wird, auch  
9 damit die Belastung durch digitale und komplexe Verfahren nicht weiter zunimmt.

10 Die Bedrohungslage verändert sich dynamisch. Organisierte Kriminalität nutzt  
11 internationale Netzwerke, digitale Infrastrukturen und hochgradig arbeitsteilige  
12 Netzwerke, um enorme Schäden anzurichten. Das gemeinsame Lagebild von Justiz  
13 und Polizei zeigt deutlich: Die Zahl hochprofessioneller Tätergruppen bleibt nicht nur  
14 hoch, ihr Vorgehen wird zudem brutaler und digitaler. Die Ermittlungsbehörden  
15 registrierten 2024 fast 1.000 Tatverdächtige aus 54 Staaten im Bereich der  
16 Organisierten Kriminalität. Besonders gravierend ist der massive Anstieg der  
17 Schadenssummen auf mehr als 1,4 Mrd. Euro, der u. a. auf komplexe Cyberangriffe  
18 zurückgeht. Zugleich führt der jüngste linksextremistische Terrorakt in Berlin die  
19 zunehmenden Bedrohungen für die kritische Infrastruktur und damit für unsere  
20 Daseinsvorsorge vor Augen. Umso wichtiger ist ein konsequentes Vorgehen gegen  
21 Gewalttaten aus dem rechts- wie dem linksextremistischen Lager.

22 Die Polizeiliche Kriminalstatistik zeigt auch, dass sich Kriminalität zunehmend in den  
23 digitalen Raum verlagert: Cybercrime, digitale Betrugsformen und sexualisierte Gewalt  
24 im Netz wachsen dynamisch und stellen Staat und Ermittler vor neue  
25 Herausforderungen. Tätergruppen professionalisieren sich zunehmend und nutzen  
26 verschlüsselte Messenger-Dienste für ihre Kommunikation. Durch den Einsatz von  
27 Künstlicher Intelligenz (KI) sind Cyber-Akteure zwischenzeitlich in der Lage, ohne oder  
28 mit nur geringen IT-Kenntnissen ausgefeilte Angriffe zu starten, was die Gefahr von  
29 Cyberangriffen weiter steigert. Moderne Kriminalitätsbekämpfung erfordert daher  
30 zeitgemäße Ermittlungsinstrumente, digitale Analysefähigkeiten und belastbare  
31 rechtliche Grundlagen.

32 Bayern tritt diesen Bedrohungen seit jeher entschlossen entgegen. Wir haben bereits  
33 2013 eine Cybersicherheitsstrategie (BayCSS) verabschiedet, diese zuletzt 2023 mit  
34 der BayCSS 2.0 fortgeschrieben. In deren Umsetzung haben wir eine schlagkräftige  
35 Cybersicherheitsarchitektur aufgebaut und bedarfsgerecht weiterentwickelt.

Für einen umfassenden Schutz braucht es auch präzise gesetzliche Grundlagen – etwa für die Speicherung digitaler Spuren oder den Ermittlungszugriff auf verschlüsselte Kommunikationskanäle im Rahmen rechtsstaatlicher Anordnungen. Bayern setzt sich seit langem für eine rechtliche Gleichbehandlung klassischer Telekommunikation und moderner Messenger-Dienste ein. Deswegen sprechen wir uns insbesondere für folgende Maßnahmen aus:

## **1. Schutz und Vertrauen der Bürger stärken**

### **Sichtbare Präsenz und moderne Polizeiarbeit**

Wir setzen auf bürgernahe Polizeipräsenz sowie eine fortlaufende Aus- und Fortbildung für moderne Ermittlungsarbeit. Dazu gehört auch, unsere Polizeibeamtinnen und Polizeibeamten durch moderne und technologisch fortschrittliche Arbeitsabläufe, eine bessere Verzahnung von Ermittlungs- und Auswerteprozessen sowie den gezielten Einsatz moderner IT-Werkzeuge spürbar zu entlasten, damit sie ihre Aufgaben effizient und wirksam wahrnehmen können.

### **Transparenz und Rechtsstaatlichkeit als Leitlinie**

Jede Erweiterung von Befugnissen erfolgt strikt im Rahmen von Verhältnismäßigkeit, gerichtlicher Kontrolle und Grundrechtsschutz. Sicherheit und Freiheit gehören für uns untrennbar zusammen. Für Maßnahmen, die mit erheblichen Grundrechtseingriffen verbunden sind, gilt selbstverständlich der Richtervorbehalt.

## **2. Moderne Ermittlungsbefugnisse sichern**

### **Praxistaugliche Ermittlungsbefugnisse bei verschlüsselter Kommunikation**

Wir müssen digitale Ermittlungsblindstellen dringend schließen. Strafverfolgungsbehörden brauchen klare gesetzliche Regelungen, um in schwerwiegenden Fällen – wie etwa Terrorismus, organisierter Kriminalität oder Kindesmissbrauch – unter strengen rechtsstaatlichen Voraussetzungen auch verschlüsselte Messenger-Kommunikation auswerten zu können. Dabei setzen wir auf punktgenaue, streng anlassbezogene Ermittlungsbefugnisse, die schwere Straftaten effektiv bekämpfen, ohne in die private Kommunikation unbescholtener Bürgerinnen und Bürger einzugreifen.

### **Verbindliche Speicherung von IP-Adressen**

Privatsphäre und Sicherheit gehören für uns zusammen; sie sind zwei Seiten einer Medaille. Deshalb setzen wir auf rechtsstaatlich kontrollierte und praxistaugliche Instrumente. Die Ermittlungsfähigkeit bei Online-Delikten hängt oftmals von Verkehrsdaten ab, zu denen auch IP-Adressen und Portnummern gehören. Um digitale Spuren effektiv nutzbar zu machen, brauchen wir schnell eine grundrechts- und europarechtskonforme Lösung, die am besten eine sechsmonatige Speicherfrist dieser Verkehrsdaten ermöglichen sollte. Eines sollten die Kritiker nicht vergessen: Ermittlungen zur Strafverfolgung können immer auch der Entlastung eines Beschuldigten dienen.

### **Technische und rechtliche Erweiterung automatisierter Recherche und Analyse**

Analyseplattformen leisten einen wichtigen Beitrag zur Gefahrenabwehr und zur Bekämpfung der schweren und organisierten Kriminalität, da diese ermöglichen, schnell und automatisiert eine Vielzahl von Daten aus unterschiedlichen polizeilichen Verfahren zu einem einzelfallbezogenen Gesamtbild zusammenzuführen. Wir setzen uns deshalb weiterhin für die Implementierung einer bundeseinheitlichen Recherche- und Analyseplattform ein. Gleichzeitig fordern wir dringend die Aufnahme gesetzlicher Regelungen in die Strafprozessordnung, um die automatisierte Datenanalyse zur Verfolgung von Straftaten durch die Polizeien der Länder, des Bundes und das Bundeskriminalamt zu ermöglichen. In Bayern wurde eine solche Rechtsgrundlage für den präventiven Bereich bereits im Polizeiaufgabengesetz (PAG) geschaffen.

Die im Jahr 2024 in Kraft getretene Verordnung über künstliche Intelligenz der EU eröffnet neue Chancen bei der Verbrechensbekämpfung, der Gefahrenabwehr und der Strafverfolgung. Sie lässt z. B. eine Echtzeit-Gesichtserkennung im öffentlichen Raum, aber auch einen biometrischen Internetabgleich von Fotos (unter klar definierten Voraussetzungen) zu und zwar sowohl für Maßnahmen der Strafverfolgung als auch zur Gefahrenabwehr. Wir fordern, dass entsprechende Befugnisnormen im Bundes- und Landesrecht geschaffen werden.

### **3. Organisierte Kriminalität konsequent bekämpfen**

#### **Vermögensabschöpfung weiter stärken**

Allein 2024 flossen hunderte Millionen Euro in kriminelle Strukturen. Um Geldwäsche zu verhindern und kriminelles Vermögen konsequent abzuschöpfen, wollen wir die Zentral- und Koordinierungsstellen der Justiz weiter stärken.

#### **Internationale Zusammenarbeit intensivieren**

82 % aller Verfahren im Bereich der Organisierten Kriminalität haben internationale Bezüge. Wir setzen uns deshalb für noch intensivere Kooperationen unserer Strafverfolgungsbehörden mit Europol, Interpol und europäischen Justiz- und Polizeinetzwerken ein.

#### **Schlagkraft der Ermittler erhöhen**

Wir unterstützen die personelle Stärkung von Polizei und Staatsanwaltschaften in den Bereichen Cybercrime, Geldwäsche, Schleusungskriminalität, Abrechnungsbetrug und Rauschgiftkriminalität.

### **4. Bayern resilient gegen Cyberkriminalität, Cyberspionage und -sabotage machen**

#### **Cybersicherheitsarchitektur bedarfsgerecht weiterentwickeln**

Die Bedrohungslage im Cyberraum erfordert die fortlaufende Überprüfung der Cybersicherheitsmaßnahmen und -instrumente auf Vollständigkeit und Wirksamkeit. Davon umfasst sind gleichermaßen die Organisationsstrukturen, die Arbeitsprozesse sowie staatliche Unterstützungs- und Beratungsangebote zur Prävention, aber auch zur konkreten Unterstützung im Schadensfall. Sicherheitsstrukturen sowie die

technischen Fähigkeiten der Sicherheitsbehörden müssen stetig überprüft und nötigenfalls ausgebaut werden.

### **Schutz Kritischer Infrastrukturen priorisieren**

Besondere Sicherheitsstandards sind insbesondere für die Energieversorgung, den Gesundheitsbereich, die staatlichen Rechenzentren und die sicherheitsrelevanten Bereiche von Verwaltung und Wirtschaft unverzichtbar. Um sie vor Angriffen zu schützen und resilienter zu machen, wollen wir im Rahmen der Vorgaben von KRITIS-Dachgesetz und BSI-Gesetz zentrale Sicherheits- und Monitoring-Strukturen weiter ausbauen.

### **Digitalen Selbstschutz und Prävention fördern**

Um insbesondere Kinder und Jugendliche noch mehr für das Thema Cybersicherheit zu sensibilisieren, wollen wir zielgruppenspezifische Präventionsangebote wie PIT (Prävention im Team), den Medienführerschein und Informationsplattformen zur Verbesserung des digitalen Selbstschutzes weiter ausbauen. Darüber hinaus wollen wir digitale Kompetenzen in der gesamten gesellschaftlichen Breite verbessern.

Bayern steht für Sicherheit, Stabilität und Rechtsstaatlichkeit. In einer sich wandelnden Welt braucht es moderne Antworten auf Kriminalität. Wir gehen diesen Weg entschlossen, digital, europäisch vernetzt und fest verwurzelt in den Grundwerten unseres Landes. Mit starken Ermittlungsbehörden, klaren gesetzlichen Grundlagen und einer zukunftsorientierten Cybersicherheitsstrategie sorgen wir dafür, dass das Leben in Bayern auch in Zukunft sicher ist.