

Öffentliche Akzeptanz digitaler Technologien für die deutsche Polizei

Bevölkerungsbefragung und Diskurs über Akzeptanz, öffentliche Sicherheit, technologische Notwendigkeiten, bürokratische Selbstbeschränkungen und Erfolg versprechende Lösungsansätze





POLIZEI

ST. PAULI THEATER

The 27 Club

Vorwort

Sehr geehrte Leserinnen und Leser,

diese Publikation ist ein Diskussionsbeitrag zur technologischen Modernisierung der deutschen Polizei. Sie ist das Ergebnis einer Analyse und zahlreicher Diskussionen, die bei uns 2019 begannen. Im Fokus stehen das öffentliche Image und die Akzeptanz digitaler Technologien für die Polizei in der Bevölkerung. Das war unser Interesse zu Beginn der Diskussionen und Gegenstand einer repräsentativen Umfrage, die wir in Auftrag gaben. Im Anschluss entwickelten sich Fragen mit vielfältigen Aspekten über Voraussetzungen für die Handlungsfähigkeit und für Modernisierungsbedarfe der Polizei in Deutschland: rechtliche Befugnisse, technologische Möglichkeiten, Hemmnisse und erforderliche Kompetenzen.

Die Akzeptanz, die Bürgerinnen und Bürger digitalen Technologien für die Polizei entgegenbringen, so eine unserer anfänglichen Hypothesen, ist zunächst von ihrem empfundenen Nutzen abhängig, nämlich davon, wie wirksam und relevant die jeweiligen Technologien für die Verbrechensbekämpfung und wahrgenommene Bedrohungen eingeschätzt werden. Zugleich zeigt sich in der akzeptierten Tiefe des Eindringens in den persönlichen Bereich die Einschätzung des Bedrohungslevels.

Die Zustimmung zu Technologieverwendungen dürfte Menschen dann leichtfallen, wenn sie sich selbst davon nicht konkret betroffen fühlen. Je sichtbarer und individueller die Auswirkungen, desto größer

das persönliche Schutzbedürfnis. Das Hinnehmen spürbarer Einschränkungen individueller Freiheit und persönlicher Rechte fordert zudem Vertrauen dahin gehend, dass diese Einschränkungen gerade zu unserem eigenen Schutz geschehen und nicht missbraucht werden. Die Akzeptanz digitaler Technologien wird zum Spiegel subjektiver Schutzbedürfnisse und des Vertrauens der Bevölkerung.¹

Unsere Hypothesen haben wir im Jahr 2019 in einer repräsentativen Bevölkerungsumfrage verprobt. Der daran anschließende Austausch über die Umfrageergebnisse, den wir noch 2019 und auch 2020 mit vielen Akteuren der inneren Sicherheit auf Bundes- und Länderebene hatten, zeigte recht schnell, wie umfangreich die Bandbreite an Diskussionen ist, die sich daraus ergeben.

Mit einer Interviewserie ausgewählter Experten der Community geben wir Ihnen nun einen Eindruck von den vielfältigen Perspektiven auf die Erkenntnisse der Befragung und die damit verbundenen Themenstellungen.

Was denkt unsere Bevölkerung?

Die Modernisierung der Polizeiarbeit ist eine Daueraufgabe. Ein entscheidender Faktor dabei ist das Sicherheitsempfinden der Bevölkerung. Was die Polizei im digitalen Raum leisten darf, was sie dort leisten kann und was sie davon tatsächlich praktiziert, hängt stark von diesem Empfinden ab. Denn daraus erwächst mehr oder weniger

Druck auf die Politik, die Digitalisierung der Polizei öffentlichkeitswirksam zu vertreten, zu beschleunigen und zu finanzieren. Reaktionsgetriebenes Handeln infolge bestimmter Anlässe bzw. Sicherheitsvorfälle gelangt in den stufenreichen Prozessen der Politik und Verwaltung nur dann zum Erfolg, wenn es von der grundlegenden Akzeptanz in der Bevölkerung getragen wird.

Daher setzten wir 2019 die repräsentative Bevölkerungsumfrage auf. Ziel war es, das Ausmaß dieser grundlegenden gegenwärtigen Akzeptanz auszuloten. Die Initiative stand auch unter dem Eindruck der vielerorts großen Proteste gegen die Novellierung der Polizeigesetze. Damit verbunden war teilweise eine sehr ablehnende Haltung zu vergleichsweise einfachen, aber eben deutlich sichtbaren digitalen Instrumenten – wie Bodycams an Polizeiuniformen oder Kameras im öffentlichen Raum.

In unserem Auftrag führte ein Meinungsforschungsunternehmen die Umfrage zwischen Juli und September 2019 als für alle Bundesländer repräsentative Befragung durch. Die Frageblöcke umfassten die Einstellungen zu polizeilichen Befugnissen, zur Akzeptanz moderner Polizeitechnologien, zu innovativen Mitteln der Kriminalitätsbekämpfung, zur polizeilichen Digitalkompetenz, die Sorge, Cyberkriminalitätsoffer zu werden, und mehr. Wir wollten diese Umfrage als Basis für Gespräche in der Fachcommunity nutzen – in stichhaltigem Design und eben als Echolot der öffentlichen Akzeptanz.

¹ Mit den Dimensionen „Nutzen“, „konkrete Einschränkungen/Wahrnehmbarkeit“ und „Vertrauen“ haben wir uns an die grundsätzliche Logik des Technology Acceptance Model (TAM) angelehnt, das für die Akzeptanz neuer Technologien den empfundenen Nutzen, die wahrgenommenen Nutzungsbarrieren und die Einstellung als zentrale Aspekte ansieht.

Überraschende Befragungsergebnisse

Die Befragungsergebnisse stellen wir Ihnen, liebe Leserinnen und Leser, auf den Seiten 14 bis 25 vor. Einige Ergebnisse haben uns überrascht – beispielsweise das sehr gute Polizeiimage und die hohe Technologieakzeptanz in der Bevölkerung. Mitunter vermittelt die „gefühlte“ Stimmung im Land einen ganz anderen Eindruck.

Die hohe Technologieakzeptanz hängt auch damit zusammen, dass rund die Hälfte der befragten Bundesbürger (51 %) für sich persönlich ein hohes Risiko sieht, im digitalen Raum betrogen zu werden. Das heißt, sicher fühlen sich die Bürgerinnen und Bürger im Internet nicht.

Die erhebliche Akzeptanz für den Einsatz digitaler Technologien umfasst auch solche Instrumente, die mitunter im Fokus kontroverser

Diskussionen stehen. Denken wir nur an die schon erwähnten Bodycams, an Videoüberwachung auf öffentlichen Plätzen – oder an die Diskussionen zur Sicherheit und zum Datenschutz bei der im Jahr 2020 bereitgestellten „Corona-Warn-App“. Doch auch ohne diese App wissen wir längst, wie kritisch technische Lösungen der Polizei diskutiert werden, weil Bürgerinnen und Bürger um ihre Privatsphäre fürchten.

PwC/Strategy& ist ein bewährter Partner der öffentlichen Hand

Die öffentliche Sicherheit ist gerade in Zeiten tiefgreifender gesellschaftlicher Veränderungen ein hohes Gut. PwC/Strategy& trägt in vielerlei Hinsicht dazu bei – insbesondere in Projekten für den öffentlichen Sektor. Dabei geht es beispielsweise um

- die digitale Souveränität von Behörden und anderen Institutionen,
- effiziente Beschaffung mithilfe digitaler Werkzeuge,
- zeitgemäßen und verfassungskonformem Informationsaustausch der Sicherheitsbehörden („Polizei 2020“)
- und Unterstützung bei der Verdachtsprüfung und Betrugaufdeckung – etwa im Zusammenhang mit Geldwäsche.

Der öffentliche Sektor kann sich aber auch darauf verlassen, dass PwC/Strategy& eine stark werteorientierte Organisation ist. „Building trust in society and solving important problems“: Unter diesem Motto

denken und handeln wir täglich. Ihm entsprang auch unser Antrieb, in Eigenverantwortung die Ihnen nun vorliegende Publikation über die Digitalkompetenz der deutschen Polizei und die öffentliche Akzeptanz von Technologien bei der Polizei zu entwickeln und umzusetzen.

Diese Publikation vermittelt Ihnen keine abschließende Meinung zum Thema. Im Gegenteil: Sie ist ein Beitrag zur öffentlichen Diskussion, die sich permanent weiterentwickelt. Impulse für diese Weiterentwicklung geben wir mit der empirischen Meinungserhebung in der Bevölkerung und den verschiedenen Perspektivendarstellungen bezüglich der Modernisierungserfordernisse bei der Polizei.

Und: Wir möchten mit Ihnen im Gespräch bleiben. Für eine erfolgreiche deutsche Polizei – und eine innere Sicherheit, wie wir sie alle uns wünschen.



Prof. Dr. Rainer Bernnat
Senior Partner und Industry Leader
Public Sector, PwC/Strategy&
Deutschland

Im Labyrinth der heiklen Fragen

Schnell ist man im fachlichen Austausch über das Ob und Wie der inneren Onlinesicherheit auch bei den unvermeidlichen Fragen rund um Privatsphäre, Bürger- und Freiheitsrechte. Von dort aus dauert es mitunter nur wenige Minuten, bis sich Debatten über polizeiliche Ermittlungen etwa in sozialen Netzwerken, über digitale Hilfsmittel für Kriminalitätsprävention oder über erweiterte Befugnisse in der Ermittlungsarbeit entfalten. Denken wir hier einmal mehr an Überwachungskameras für öffentliche Plätze, Bodycams an Polizeiuniformen, aber auch an Predictive Policing, bundesländerübergreifende Datenaustausche zwischen Ermittlungsbehörden und Staatsanwaltschaften, an Vorratsdatenspeicherung und, und, und.

Rechtsfreier Raum oder nicht?

Eine begleitende Fragestellung bei all diesen Themen bleibt, inwiefern das Internet ein rechtsfreier Raum ist oder nicht. Manche Diskussionspartner argumentieren normativ und sehen das Internet als freiheitliches Refugium. Andere beklagen, dass es de facto ein rechtsfreier Raum ist, da Mittel und (internationale) Normensetzung gegenwärtig nicht ausreichen, um Rechtsstaatlichkeit auch online zu schaffen. So fragten wir uns, welche Rolle die deutsche Polizei im digitalen Raum mittlerweile einnimmt.

Oder einnehmen sollte.

Oder einnehmen muss!

Wer sich darüber den Kopf zerbricht – dies machen wir als Strategie- und Digitalisierungsberater für den öffentlichen Sektor täglich –, fragt schnell auch nach innovativen Technologien, digitalen Kompetenzen und rechtlichen Rahmenbedingungen im digitalen Zeitalter. Denn eigentlich sollten unsere Rechte, auf die wir uns im herkömmlichen, „physischen“ Raum seit Bestehen der Bundesrepublik auch dank unserer Polizei verlassen können, im virtuellen Raum gewahrt bleiben.

„Mit Pfeil und Bogen auf Streife gehen“

Die Polizei hat zeitgemäße Technologien dringend nötig. Nur damit kann sie die öffentliche Sicherheit und individuelle Freiheit in einer Zeit gewährleisten, in der Kriminelle ihr Unwesen zunehmend im Internet treiben. Oder wie es der CDU-Sicherheitsexperte und seit November 2020 der amtierende Präsident des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) Armin Schuster im Interview ab Seite 26 zuspitzt: „Es ist ein unhaltbarer Zustand, dass unsere Polizei in einer Welt, in der Straftäter die ganze Klaviatur moderner technologischer Instrumentarien missbrauchen, immer noch mit Pfeil und Bogen auf Streife geht.“

Diskussionen vertiefen und öffentlich machen

Als wir die Umfragewerte 2019 und 2020 verschiedenen Polizei-entscheidern und -entscheiderinnen vorstellten, lösten wir leidenschaftliche Reaktionen bei ihnen aus. Da war einerseits die häufige Kritik aus Politik und Medien an beispielsweise polizeilichen Eingriffs- und Ermittlungsrechten. Andererseits zeigten die hohen Akzeptanzwerte selbst nach klassischen soziodemografischen Faktoren wie Alter, Geschlecht, Bildung und Wohnsitz kaum Varianz. Das heißt, die Akzeptanz ist breiter Konsens. Und: Die Ergebnisse widersprechen durchaus den vielen kritischen Eindrücken, die unter anderem durch Proteste gegen die Novellierung der Polizeigesetze infolge der Unruhen in den USA und die anschließenden Diskussionen auch in Deutschland hierzu entstanden sind. Sie umfassen allerdings noch nicht die Diskussionen über mögliche Vertrauensschäden, die durch die Aufdeckung von rechtsextremen Gruppen in der Polizei entstanden.

Unser Fokus, das muss hier klar gesagt werden, lag indes auf der Akzeptanz digitaler Technologien. Diesbezüglich offenbarten die Reaktionen unserer Gesprächspartner ein hohes Defizitempfinden insbesondere bei der digitalen Polizeiarbeit – aber auch den unbedingten Willen, die Digitalkompetenz der Polizei deutlich zu steigern. Die fruchtbaren Diskussionen mit der Community zeigten uns, wie wichtig es ist, unsere Befragungsergebnisse allen Interessierten zugänglich zu machen – vertieft durch Perspektiven aus Politik, Praxis und Wissenschaft.

Verschiedene Perspektiven und Schlussfolgerungen

Diese Vertiefung lesen Sie nun. Den Kern dieser Publikation bilden zunächst die Ergebnisse der repräsentativen Bevölkerungsumfrage – und danach, ab Seite 26, acht Interviews mit angesehenen „Sicherheitspolitikern“, Polizeipraktikern und Polizeiwissenschaftlern.

Ganz bewusst wollten wir auf diese Weise die Umfrageergebnisse einordnen lassen. Jeder Gesprächspartner hat eine eigene Sicht darauf und zieht Schlussfolgerungen mit eigenen Akzentuierungen. Dabei sind sie sich einig darüber, dass die Polizei einen erheblichen Nachholbedarf in Sachen Digitalisierung hat – beispielsweise hinsichtlich ihrer Arbeitsplatzausstattung, der Kompetenz ihrer Beschäftigten und ihrer Aus- und Weiterbildungsstrategie. Dass die Bevölkerung dies ebenso sieht, bestätigt ihre Sicht.

Acht Insider, die es wissen müssen

Die Interviews haben wir Mitte 2020 geführt. Die bekanntesten unter den Gesprächspartnern sind vielleicht

die ehemalige Bundesjustizministerin Sabine Leutheusser-Schnarrenberger (FDP), der eingangs zitierte BBK-Präsident Armin Schuster, der Bayerische Landespolizeipräsident Prof. Dr. Wilhelm Schmidbauer und Polizeigewerkschaftschef Rainer Wendt. Die anderen Gesprächspartner sind ebenso wichtig für eine starke Polizei.

Wir danken allen Interviewten sehr, dass sie sich die Zeit genommen haben, ihr perspektivenreiches Wissen zu teilen. Es streckt sich von Cyber-sicherheit, behördenübergreifender Zusammenarbeit und Kooperationen mit der Privatwirtschaft über Personal- sowie Ausbildungsstrategien und Digitalisierungsthemen bis hin zu Aspekten des Datenschutzes. In unserer Zusammenfassung ab Seite 10 ziehen wir kurze Schlussfolgerungen, in die auch unsere Beratungserfahrung im Polizeibereich einfließt.

Über Ursachen und Wirkungen

Mit der Lektüre dieser außergewöhnlichen Publikation, liebe Leserinnen und Leser, bekommen Sie einen umfassenden Überblick über die Ursachen und Wirkungen eines Digitalisierungsniveaus bei

der deutschen Polizei, das noch – lassen Sie es uns einmal salopp ausdrücken – viel Luft nach oben hat. Und Sie erfahren, was nötig ist, um die gesamte Polizei zur digitalen Exzellenz zu entwickeln. Zur Exzellenz, damit sie jenen Menschen und Organisationen wirksamer begegnen kann, die digitale Technologien missbrauchen, um Privatpersonen, Unternehmen, Behörden und anderen Institutionen in unserem Land zu schaden.

Das digitale Zeitalter erfordert eine ständig verbesserte Digitalkompetenz der Polizei, damit die Sicherheit der Gesellschaft und das Vertrauen der Bürgerinnen und Bürger in den Rechtsstaat erhalten bleiben.

PwC/Strategy& sieht diese Publikation als einen Beitrag im diskursiven Ringen um die richtige Balance zwischen nötiger Sicherheitsvorsorge und gesicherten Freiheitsrechten, um eine zielgenaue und wirtschaftliche Verwendung öffentlicher Mittel im Sinne einer zeitgemäßen Polizeiarbeit – und um Akzeptanz und Vertrauen in unsere gesellschaftliche Ordnung.

Das Autorenteam Dr. Wolfgang Zink und Kerstin Zimmermann wünschen Ihnen eine spannende und erkenntnisreiche Lektüre.



Dr. Wolfgang Zink
Partner Public Sector Consulting,
PwC Deutschland



Kerstin Zimmermann
Manager Public Sector Consulting,
PwC Deutschland



Inhalt

Die Abbildungen.....	8
Die Interviewten	9
A Zusammenfassung: Sieben entscheidende Querschnitts-herausforderungen	10
1 Cybersicherheit gewährleisten.....	11
2 Behördenübergreifende Zusammenarbeit.....	11
3 Personalstrategie für das digitale Zeitalter	12
4 Behördenreorganisation und Kompetenzoffensive	12
5 Großprojekte erfolgreich managen	12
6 Chancen der Digitalisierung nutzen	13
7 Mit Datenschutz und Informationssicherheit	13
B Die Bevölkerung in Deutschland wünscht sich eine technologisch modern ausgerüstete Polizei.....	14
C Polizeiexperten im Gespräch	26
1 Perspektiven aus der Politik.....	27
2 Perspektiven aus der Praxis	34
3 Perspektiven aus der Wissenschaft.....	49
D Thought Leadership by PwC/Strategy&.....	58
Ihre Ansprechpartner	60



Die Abbildungen

Abb. 1	Allgemeine Einstellung gegenüber der deutschen Polizei.....	15
Abb. 2	Einstellung gegenüber der Polizei nach Bundesländern	16
Abb. 3	Empfinden der Anzahl der Polizistinnen und Polizisten in Deutschland.....	17
Abb. 4	Bewertung weiterer Parameter der Polizei.....	17
Abb. 5	Wer über die Befugnisse der Polizei bestimmen sollte.....	18
Abb. 6	Beurteilung der Angemessenheit der Polizeibefugnisse	18
Abb. 7	Einschätzung zur potenziellen Erweiterung von Polizeibefugnissen.....	19
Abb. 8	Erwartete Entwicklung der Straftaten mithilfe neuer Technologien	19
Abb. 9	Empfundenes Opferrisiko im Zusammenhang mit Cyberkriminalität	20
Abb. 10	Bewertung der polizeiinternen Digitalkompetenz	20
Abb. 11	Welche Technologien die Polizei einsetzen sollte	21
Abb. 12	Welche Technologien Straftaten verhindern könnten.....	22
Abb. 13	Wie sehr verschiedene Technologien akzeptiert werden	23
Abb. 14	Welche Technologien sich für Kriminalitätsprävention und -aufklärung eignen	24
Abb. 15	Ob neue Technologien bundesweit vernetzt werden sollten.....	25



Die Interviewten

- 1 Sabine Leutheusser-Schnarrenberger, Bundesjustizministerin a. D.:
„Die Politik macht viel zu wenig, um Handwerkszeug für effiziente
Polizeiarbeit zu beschaffen.“ 27
- 2 Armin Schuster, Präsident des Bundesamts für Bevölkerungsschutz
und Katastrophenhilfe (BBK): „Vielleicht übertreiben wir es manchmal
mit dem Liberalismus.“ 31
- 3 Prof. Dr. Wilhelm Schmidbauer, Bayerischer Landespolizeipräsident:
„Wir setzen auf zielgerichteten Technikeinsatz bei Kriminalitäts-
schwerpunkten.“ 34
- 4 Markus Eisenbraun, Abteilungsleiter Cybercrime und digitale Spuren
beim Landeskriminalamt Baden-Württemberg: „Es muss darum gehen,
mit der Digitalisierung der Kriminalität mitzuhalten.“ 38
- 5 Rainer Wendt, Vorsitzender der Deutschen Polizeigewerkschaft:
„Der Rechtsstaat funktioniert auch im Internet, wenn er die nötigen
Kapazitäten dafür hat.“ 41
- 6 Dr. Harald Olschok, Hauptgeschäftsführer des Bundesverbands der
Sicherheitswirtschaft (BDSW): „Die Wirtschaft muss die Kriminalitäts-
prävention im Internet weitgehend in die eigene Hand nehmen.“ 45
- 7 Dr. Thomas-Gabriel Rüdiger, Cyberkriminologe am Institut für Polizei-
wissenschaft an der Hochschule der Polizei des Landes Brandenburg:
„Dieses Problem ist eine Jahrhundertaufgabe.“ 49
- 8 Dr. Roman Povalej, „Cybercrime-Professor“ an der Polizeiakademie
Niedersachsen: „Mir geht es um Digital Natives versus digital-naiv.“ 54

A Zusammenfassung: Sieben entscheidende Querschnittsherausforderungen



Die Idee, durch eine repräsentative Bevölkerungsumfrage das Akzeptanzlevel von digitalen Polizeitechnologien in Deutschland zu ergründen, mündete fast zwangsläufig in einer viel umfassenderen Betrachtungsweise. Denn digitale Technologien fördern Kooperationen und lösen Grenzen auf oder können sie auflösen – in unserem Fall beispielsweise zwischen

- sicherheitsspezifischen Denkmustern,
- polizeilichen und staatsanwaltlichen Organisationseinheiten,
- Sicherheitsbehörden und privatwirtschaftlichen Sicherheitsdiensten,
- Bundesländern und
- dem In- und Ausland.

Dies verdeutlichen einmal mehr die Interviews mit den acht Experten aus der Polizeipraxis, der Polizeiausbildung und der Politik. Deren ganz unterschiedliche Blickwinkel auf ein und dasselbe Thema umfassen sieben Querschnittsherausforderungen. Diese gilt es konsequent zu bearbeiten, soll die Polizei wettbewerbsfähig bleiben.

1 Cybersicherheit gewährleisten

Die Internetkriminalität nimmt drastisch zu. Insgesamt 80 % der im Auftrag von PwC/Strategy& befragten Bundesbürger glauben, dass die Anzahl der mit neuen Technologien begangenen Straftaten binnen drei Jahren zunehmen wird. Auch Dr. Thomas-Gabriel Rüdiger, Cyberkriminologe an der Hochschule der Polizei des Landes Brandenburg, stellt im Interview klar: „Das Hellfeld physischer Handlungen hat sich in das Dunkelfeld digitaler Delikte verschoben.“ Allerdings wird lediglich ein Bruchteil der digitalen Straftaten bei der Polizei angezeigt, was das Problem verschärft. Denn dadurch werden Straftäter immer dreister und gefährlicher. Schon heute empfinden viele Menschen in Deutschland das Internet als rechtsfreien Raum.

Kein Wunder also, dass 94 % der Bundesbürger einen starken Ausbau der digitalen Polizeikompetenzen befürworten. BBK-Präsident Armin Schuster gehört dazu. Im Interview warnt er: „Die Kapazitäten für eine wirksame Kriminalitätsprävention und Ermittlungen im öffentlichen und im digitalen Raum reichen nicht aus.“ Und der Bayerische Landespolizeipräsident Prof. Dr. Wilhelm Schmidbauer stellt klar: „Qualifiziertes Personal ist die Voraussetzung für eine rechtsstaatliche, bürgerorientierte und professionelle Polizeiarbeit.“

→ Technologien, Methoden, Prozesse und Polizeibeschäftigte müssen aufeinander abgestimmt sein, um ein hohes Maß an Cybersicherheit zu erreichen und Informationen zu schützen.

2 Behördenübergreifende Zusammenarbeit

Kommen neue Technologien für mehr Sicherheit im digitalen Raum zum Einsatz, sind 87 % der Bundesbürger dafür, dass diese auch bundesweit vernetzt sind – statt lediglich bundeslandweit. So sieht es auch das Programm „Polizei 2020“ vor, mit dem das Bundesministerium des Innern, für Bau und Heimat eine einheitliche und moderne Informationsarchitektur des polizeilichen Informationswesens für Bund und Länder anstrebt.

75 % der in der repräsentativen Erhebung von PwC/Strategy& befragten Bundesbürger befürworten gar eine Zentralisierung polizeilicher Aufgaben und Befugnisse durch den Bund. Hier widerspricht die frühere Bundesjustizministerin Sabine Leutheusser-Schnarrenberger im Interview allerdings: „In einem Flächenstaat von Deutschlands Größe etwas zentral von oben durchzuorganisieren, können wir vergessen. Das funktioniert noch schlechter als im föderalistischen System.“

Dr. Roman Povalej, „Cybercrime-Professor“ an der Polizeiakademie Niedersachsen, sieht funktionierende behördenübergreifende Kooperationen – etwa die Sicherheitskooperation der Landeskriminalämter von Nordrhein-Westfalen, Niedersachsen, Baden-Württemberg, Sachsen, Hessen und Rheinland-Pfalz sowie des deutschen Digitalverbands Bitkom. „Es gibt noch mehr solcher Initiativen und es müssen noch viel mehr werden“, sagt er.

Dass es auch bei der internationalen Zusammenarbeit noch Nachholbedarf gibt, meinen 60 % der Bundesbürger. So möchte eine Vielzahl der für PwC/Strategy& Befragten eine stärkere Vernetzung und eine Verbesserung des Informationsaustauschs zwischen dem Bund und internationalen Behörden. So sieht es auch das Programm „Polizei 2020“ vor. Angesichts der Globalität von Internetkriminalität wirkt nationales Strafrecht allein unzeitgemäß, meint der Brandenburger Cyberkriminologe Dr. Thomas-Gabriel Rüdiger. Seine Vision ist „ein globales Minimalstrafrecht“.

→ Damit deutsche Sicherheitsbehörden ihre Aufgaben erfüllen können, müssen sie zu jeder Zeit und von jedem Ort aus auf dafür nötige Informationen zugreifen können. Das wiederum ist nur möglich, wenn eine moderne und einheitliche Informationsarchitektur für den Bund, die Bundesländer und über die deutsche Landesgrenze hinaus verfügbar ist.

3 Personalstrategie für das digitale Zeitalter

Zudem erfordern die Prävention und Aufklärung von Cyberkriminalität eine hinreichende Anzahl an Polizeibeamtinnen und -beamten, die sich mit den neuen Herausforderungen kompetent befassen. Die Rückendeckung der Bevölkerung hat die Polizei. 80 % der Bundesbürger halten die derzeit 280.000 Polizistinnen und Polizisten mindestens für notwendig. Rainer Wendt, Vorsitzender der Deutschen Polizeigewerkschaft, mahnt im Interview: „Wir brauchen mehr Personal, weil sich unser Betätigungsfeld auch mit dem digitalen Raum massiv erweitert hat.“

Ein in diesem Zusammenhang großes Problem thematisiert unter anderem Markus Eisenbraun, Abteilungsleiter Cybercrime und digitale Spuren beim Landeskriminalamt Baden-Württemberg: „Bei der Personalrekrutierung tun wir uns oftmals schwer. Sicherlich ist die Bezahlung ein Grund dafür. Aber auch das Image von Arbeitsplätzen im öffentlichen Sektor.“ Und er ergänzt: „Die Polizei ist ein attraktiver Arbeitgeber. Das müssen wir viel stärker zeigen als bisher.“

Das Nachwuchsbarometer für den öffentlichen Dienst 2019 hat übrigens ergeben, dass mehr als die Hälfte der für das Barometer befragten Studentinnen und Studenten großen Wert auf flexible Arbeitsgestaltung und individuelle Weiterbildung legen. Ähnlich wichtig ist ihnen aber auch eine moderne IT-Ausstattung am Arbeitsplatz und mobiles Arbeiten. Unter anderem mobile IT wünscht sich Markus Eisenbraun auch für eine moderne Polizei.

→ Die wichtigste und wertvollste Ressource einer jeden Behörde sind ihre Mitarbeiterinnen und Mitarbeiter. Um sie zu motivieren, zu fördern und langfristig zu binden, müssen Behörden innovative und nachhaltige Personal- und Laufbahnkonzepte umsetzen.

4 Behördenreorganisation und Kompetenzoffensive

87 % der für die PwC/Strategy&-Umfrage zur Akzeptanz von Polizeitechnologien befragten Menschen in Deutschland plädieren dafür, neue Technologien bei der Polizei bundesweit zu vernetzen. So könne sie unter anderem Internetkriminalität gezielter bekämpfen.

Doch nicht nur das: Laut Polizeigewerkschaftschef Rainer Wendt würde digitale Vernetzung sogar die Sicherheit im physischen öffentlichen Raum erhöhen. Als Beispiel dafür nennt er Raserei im Straßenverkehr. Um entsprechende Lagebilder bundeslandübergreifend auf Knopfdruck zu erstellen, müsse die Neuorganisation der IT-Struktur in den Ländern noch intensiver vorangetrieben werden. Dafür nötig sei aber auch eine einheitliche Aus- und Fortbildungsstrategie. „Sehr viele Daten sind zwar vorhanden, aber nicht vernetzt. Und das liegt nicht nur am föderalen System“, sagt Rainer Wendt. Es müssten zum Beispiel auch bei den Staatsanwaltschaften digitale Fähigkeiten und die IT-Infrastrukturen verbessert und mit der Polizei vernetzt werden.

→ Für das Management digitaler Transformationsprojekte müssen Behörden häufig neue Referate, Abteilungen und Organisationsstrukturen aufbauen. Dabei sollten sie auch Strategien und Visionen systematisch miteinander verknüpfen – mithilfe digital gestützter Methoden und Werkzeuge.

5 Großprojekte erfolgreich managen

All die bislang erwähnten Defizite und Lösungsansätze sind Bestandteile von Großprojekten. Allerdings verfehlt im Schnitt jedes fünfte Großprojekt die vor seinem Start fixierten Ziele – weil sie zum

Beispiel die Kontrolle über ihren Umfang verlieren. Begünstigt werden solche Probleme häufig – auch bei der Polizei – von einer hohen Projektkomplexität und Stolpersteinen bei einer fachlich adäquaten, aber auch handhabbaren Realisierung bis zur Umsetzung.

Dabei spielt auch der Datenschutz eine Rolle. So sagt Bayerns Landespolizeipräsident Prof. Dr. Wilhelm Schmidbauer im Interview: „Zum Beispiel können wir aus Datenschutzgründen nicht ohne Weiteres marktübliche Standardprodukte einsetzen. Deshalb müssen digitale Hilfsmittel mit mitunter aufwendigen, komplexen Anpassungen genau an die polizeifachlichen Bedarfe, den hohen Sicherheitsstandard und die rechtlichen Rahmenbedingungen angepasst werden.“ Und er ergänzt: „Hinzu kommen ständige Prozessveränderungen, um neuen Kriminalitätsphänomenen und veränderten technischen Rahmenbedingungen gerecht zu werden. Wir haben es also mit etlichen polizei-, strafprozess- und datenschutzrechtlichen Vorgaben zu tun. Das ist mitunter sehr komplex.“

Infolge der Komplexität und der sich ständig weiterentwickelnden Anforderungen ist das klassische Vorgehen mit sehr detaillierten Spezifikationen und anschließender Umsetzung zu überdenken. Sogenannte funktionale Ausschreibungen, bei denen der Dienstleister für bestimmte Ergebnistypen entsteht, den Weg dorthin aber gemeinsam mit dem Auftraggeber im Projektverlauf in Iterationen bestimmt, gehören zum Repertoire zeitgemäßen (Groß-)Projektmanagements. Hier tut sich die öffentliche Hand häufig noch schwer.

→ Mut zu zeitgemäßen Formen des Projektmanagements und iterativen Vorgehensweisen ist extrem wichtig geworden. Sie ermöglichen Tempo und vermeiden zu detaillierte, aber auch sehr schnell obsoletere Spezifikationen.

6 Chancen der Digitalisierung nutzen

Rund die Hälfte der Bevölkerung (51 %) sieht ein hohes Risiko, in naher Zukunft Opfer globaler Cyberkriminalität zu werden. Damit rangiert diese Unsicherheitsursache vor der Angst vor Diebstahl, Körperverletzung oder Terrorismus. Deshalb wünschen sich die für die PwC/Strategy&-Erhebung befragten Menschen auch mehr moderne Überwachung in der Öffentlichkeit. „Integrierte Sicherheitslösungen, die Menschen und Technologie verbinden, werden immer wichtiger“, sagt unser Interviewpartner Dr. Harald Olschok, Hauptgeschäftsführer des Bundesverbands der Sicherheitswirtschaft (BDSW). Er hat hier vor allem den Werkschutz, also den Schutz von Unternehmen, im Blick. BBK-Präsident Armin Schuster sieht weitere Anwendungsfelder: „Technologie hilft natürlich, auch bei der Prävention. Es ist ein erheblicher Unterschied, ob eine S-Bahn mit oder ohne Videoausstattung fährt.“ Und er verweist auf die Schweiz, weil die Behörden dort beispielsweise automatische Kennzeichenerkennung an Grenzübergängen einsetzen.

Einen weiteren Vorteil thematisiert Dr. Roman Povalej von der Polizeiakademie Niedersachsen: „Wenn die Polizei klug digitalisiert, kann sie dadurch menschliche Ressourcen für die Kriminalitätsbekämpfung im digitalen Raum gewinnen.“

Besonders eindrücklich sind die Effekte, die zum Beispiel durch künstliche Intelligenz bei der Auswertung von Verdachtsmaterial für Straftatbestände wie Kinderpornografie erzielt werden können. Mit der Assistenz des abschließenden menschlichen Urteils können Polizistinnen und Polizisten in kurzer Zeit aus Unmengen von Ermittlungsmaterial – häufig zig Terabyte auf

diversen Festplatten und anderen Datenträgern – eine Vorauswahl für die Weiterbearbeitung treffen. Das verringert nicht nur den zeitlichen Aufwand des aufwendigen Vorab-Durchsehens, sondern sorgt auch für die psychische Entlastung der damit befassten Polizeiangehörigen.

→ Ein entscheidender Nutzen der Digitalisierung liegt darin, dass Mitarbeiter und Mitarbeiterinnen sich auf jene Aufgaben konzentrieren können, die ihre menschliche Beurteilungskompetenz dringend erfordern.

7 Mit Datenschutz und Informationssicherheit

Ein Detail der Digitalisierung der deutschen Polizei kann eine umfassendere Videoüberwachung sein. Mehr als drei Viertel der Bürger halten den flächendeckenden Einsatz von Kameras in der Öffentlichkeit für sinnvoll. So geht es auch der ehemaligen Bundesjustizministerin Sabine Leutheusser-Schnarrenberger, wenn sie zum Beispiel an Plätze denkt, an denen mit Drogen gehandelt wird. „Wir wissen zwar, dass Videokameras allein viele Täter nicht abschrecken. Aber dennoch tragen die Kameras zur Aufklärung von Straftaten bei.“

Große Akzeptanz in der Bevölkerung finden der PwC/Strategy&-Umfrage zufolge auch Predictive Policing, automatisierte Erkennungssysteme und Bodycams an Polizeiuniformen. Auch für Bodycams äußert Leutheusser-Schnarrenberger Verständnis, „weil es immer mehr Übergriffe auf Polizeibeamte gibt“. Dass Datenschutz ein Hemmnis für eine effiziente digitale Polizeiarbeit ist, verneint die FDP-Politikerin: „Der Datenschutz ist ein beliebtes Totschlagargument, wenn in Behörden etwas nicht funktioniert.

Natürlich begrenzt er den Umgang mit personenbezogenen Daten. Und das ist gut so. Aber unser Datenschutz lässt auch eine Menge an Digitalisierung zu, die wir noch lange nicht ausgeschöpft haben.“

Seit dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 kommt diesem Aspekt beim polizeilichen Informationsaustausch noch größere Bedeutung zu. Denn nach dem Richterspruch aus Karlsruhe muss der Grundsatz der hypothetischen Datenneuerhebung in den neuen Polizeigesetzen bzw. in den Systemen der Polizei abgebildet werden. Danach orientieren sich die Anforderungen an die Weiterverarbeitung von Daten zu anderen Zwecken als dem Erhebungszweck nach den Grundsätzen der Zweckbindung und -änderung. Die Reichweite der Zweckbindung richtet sich dabei nach der jeweiligen Ermächtigungsnorm der Datenerhebung.

→ Der Datenschutz ist beim Einsatz digitaler Technologien selbstverständlich entsprechend der Gesetzgebung zu berücksichtigen. Er ist aber kein Totschlagargument gegen die Digitalisierung.

Informieren Sie sich nun vollständig über die wichtigsten Ergebnisse der repräsentativen Bevölkerungsumfrage von PwC/Strategy& zur Akzeptanz von Polizeitechnologien im folgenden Grafikeil.

B Die Bevölkerung in Deutschland wünscht sich eine technologisch modern ausgerüstete Polizei



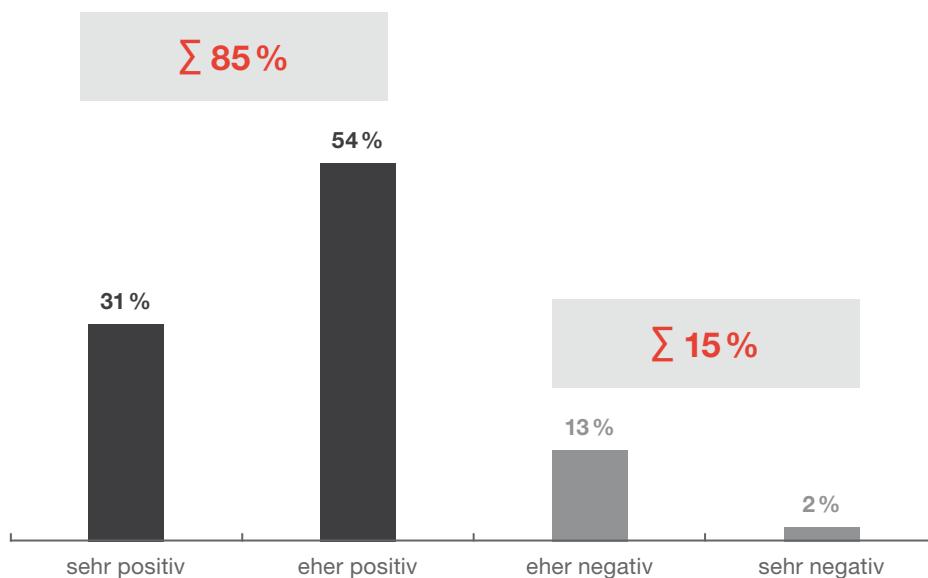
15 Fragen, viel mehr Antworten: Auf den folgenden Seiten erfahren Sie unter anderem, welches Image die deutsche Polizei in der Bevölkerung hat, wie die Menschen die polizeilichen Befugnisse empfinden, warum die Befragten sich eine höhere Digitalkompetenz wünschen und welche digitalen Hilfsmittel für welche polizeilichen Aufgaben stark oder weniger deutlich befürwortet werden.

Methodik der PwC/Strategy&-Umfrage

Die dieser Publikation zugrunde liegende repräsentative Bevölkerungsumfrage wurde im Jahr 2019 im Auftrag von PwC/Strategy& unter dem Titel „Akzeptanz von Technologie für die Polizei“ durchgeführt. Die Ergebnisse basieren auf Antworten von 3.000 Bürgerinnen und Bürgern (ab 18 Jahre) aus ganz Deutschland. Die Fragen thematisierten ihre Einstellung zur Polizei, den dort eingesetzten Technologien sowie die Akzeptanz und geschätzte Effizienz der Technologien in Bezug auf die Prävention und Aufklärung von Straftaten.

Abb. 1 Allgemeine Einstellung gegenüber der deutschen Polizei

Wie ist Ihre generelle Einstellung zur Polizei in Ihrem Bundesland?



Basis: alle Befragten, n = 1.000 (Einfachnennung)

Bevölkerungsmehrheit hat positives Bild von der Polizei

Die deutlich überwiegende Mehrheit der Bundesbürger (85 %) sieht die Polizei in ihrem jeweiligen Bundesland im Allgemeinen positiv. 13 % der Befragten haben ein negatives Bild. Die sehr negativen Stimmen fallen mit 2 % verschwindend gering aus.

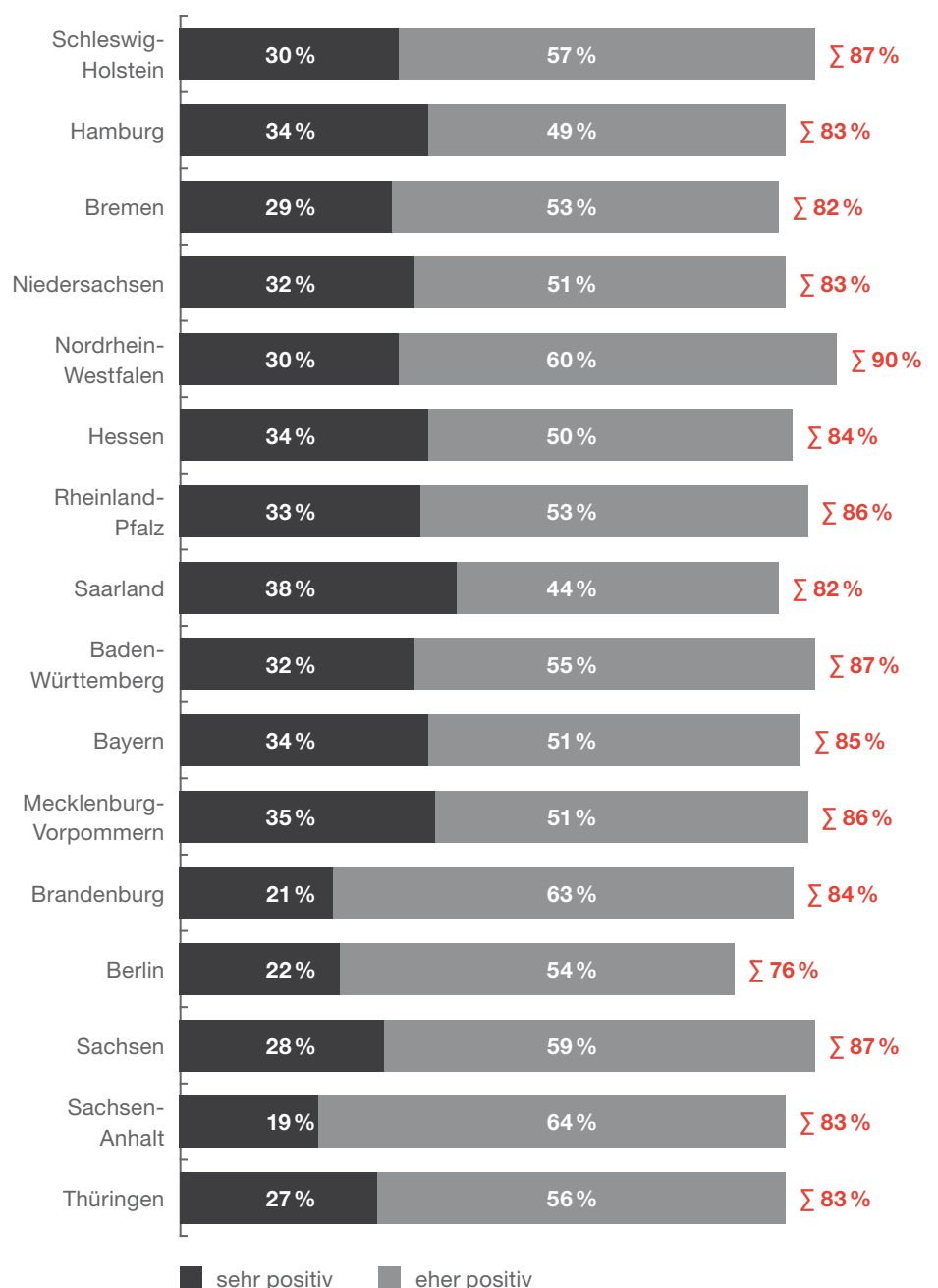


Polizei in Nordrhein-Westfalen genießt besten Ruf

Ein Blick auf das Polizeiimage in den einzelnen Bundesländern zeigt zum Beispiel: 90 % der befragten Bürger in Nordrhein-Westfalen stehen ihrer Landespolizei grundsätzlich positiv gegenüber. Im Mittelfeld rangieren etwa Thüringen und Sachsen-Anhalt mit 83 % Zustimmung. Am schlechtesten stehen die Beamten in der Hauptstadt da. In Berlin sehen nur 76 % der Befragten das Image ihrer Landesbeamten eher positiv oder sehr positiv.

Abb. 2 Einstellung gegenüber der Polizei nach Bundesländern

Wie ist Ihre generelle Einstellung zur Polizei in Ihrem Bundesland?



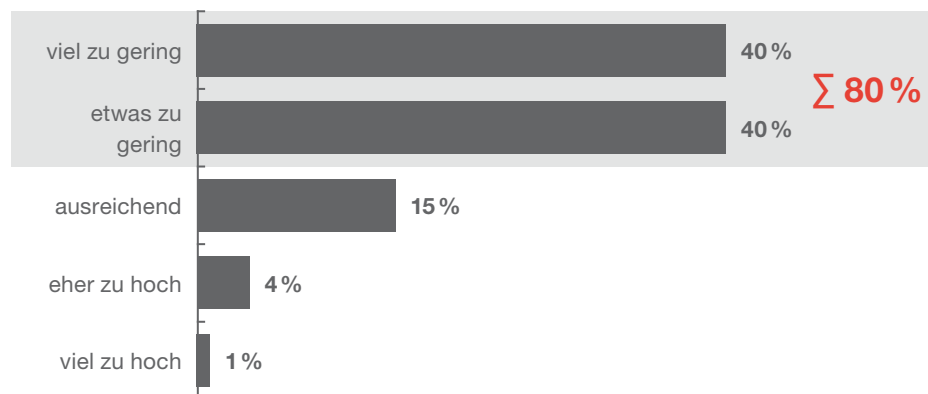
Basis: Befragte aus den jeweiligen Bundesländern; n=200 pro Bundesland; Saarland und Bremen nur jeweils n=100 (skalierte Abfrage)

Bürger registrieren klaren Personalmangel bei der Polizei

Acht von zehn Bundesbürgern finden, dass die Anzahl der bundesweit insgesamt rund 280.000 Polizistinnen und Polizisten nicht ausreichend ist. Nur 15 % sagen, dass es genug Polizeibeamte in Deutschland gibt. Eine eher zu hohe Anzahl sehen gerade einmal 4 % der Befragten. Für nur 1 % ist der Personalbestand viel zu hoch.

Abb. 3 Empfinden der Anzahl der Polizistinnen und Polizisten in Deutschland

In Deutschland gibt es momentan etwa 280.000 Polizisten. Wie schätzen Sie diese Anzahl ein?



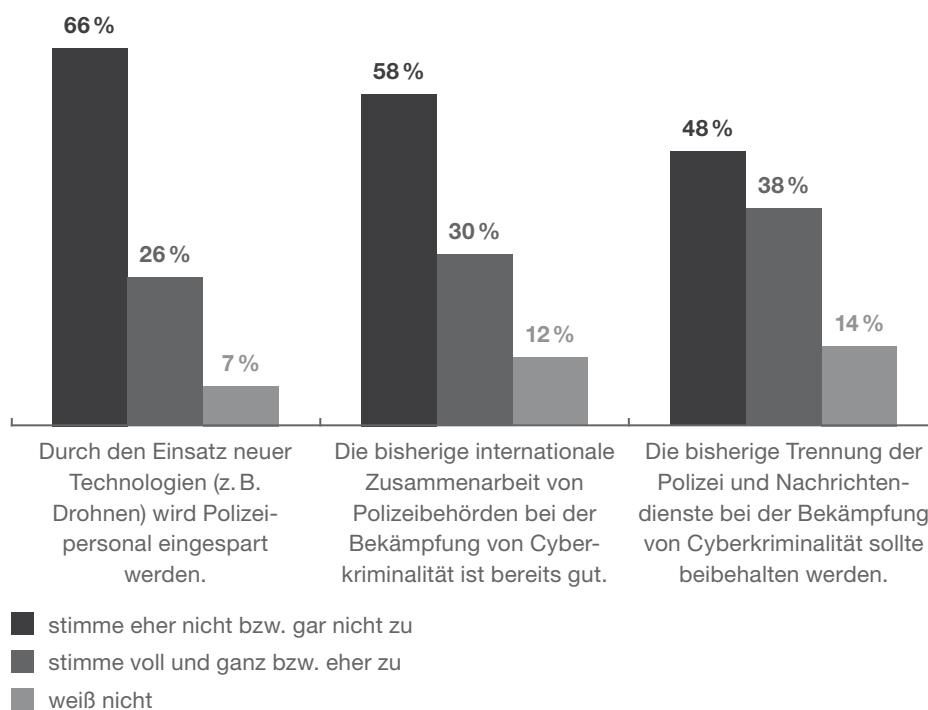
Basis: alle Befragten, n = 1.000 (Einfachnennung)

Kein Personalabbau vermutet, aber kritische Beurteilungen

66 % der Bundesbürger glauben nicht, dass durch den Einsatz neuer Technologien Personal bei der Polizei eingespart wird. 48 % lehnen die bisherige Trennung von Polizei und Nachrichtendiensten bei der Bekämpfung von Cyberkriminalität ab. Und 58 % finden die bisherige internationale Zusammenarbeit der Behörden bei der Bekämpfung von Cyberkriminalität verbesserungswürdig.

Abb. 4 Bewertung weiterer Parameter der Polizei

Inwieweit stimmen Sie den folgenden Aussagen zur Polizei zu?



Basis: alle Befragten, n = 1.000 (skalierte Abfrage)

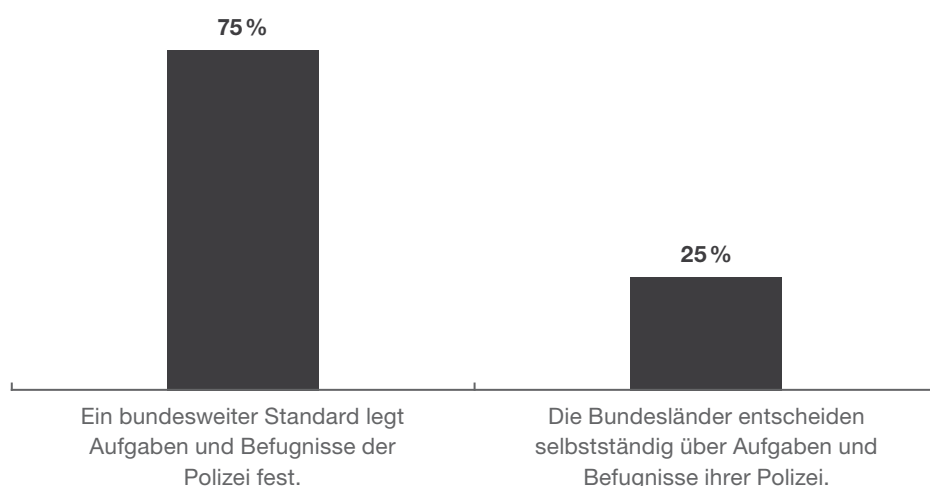


Zentrale Entscheidungsgewalt besser beim Bund

Drei Viertel der befragten Bundesbürger befürworten eine Zentralisierung polizeilicher Aufgaben und Befugnisse durch den Bund. Insgesamt 25 % der Deutschen aber sagen, dass die entsprechenden Verantwortungsbereiche in den Händen der Bundesländer bleiben sollen.

Abb. 5 Wer über die Befugnisse der Polizei bestimmen sollte

Jedes Bundesland hat eine eigene Polizei, bei der die Länderregierung über Aufgaben und Befugnisse entscheidet. In der Politik gab es aber bereits Überlegungen, mit einem Musterpolizeigesetz einen bundesweiten Standard zu schaffen. Welche der beiden Lösungen würden Sie persönlich bevorzugen?



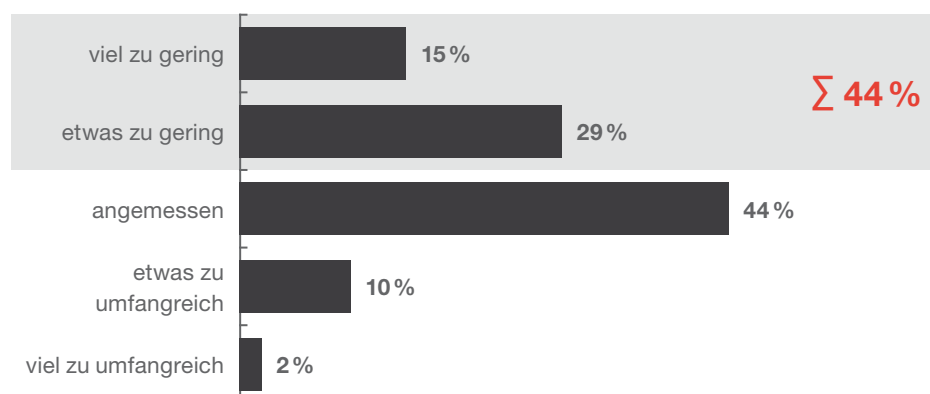
Basis: alle Befragten, n = 1.000 (Einfachnennung)

Fast die Hälfte der Befragten konstatiert zu wenig Rechte

Fast die Hälfte der Deutschen (44 %) stuft die Befugnisse der Polizeibeamten als zu gering ein. Ebenfalls 44 % halten die Kompetenzen für angemessen. Rund jeder Zehnte (12 %) findet diese zu umfangreich.

Abb. 6 Beurteilung der Angemessenheit der Polizeibefugnisse

Denken Sie bitte an die Befugnisse, die Polizisten Ihrer Meinung nach für die Ausübung ihrer Arbeit haben. Wie schätzen Sie diese Befugnisse in Ihrem Bundesland ein?



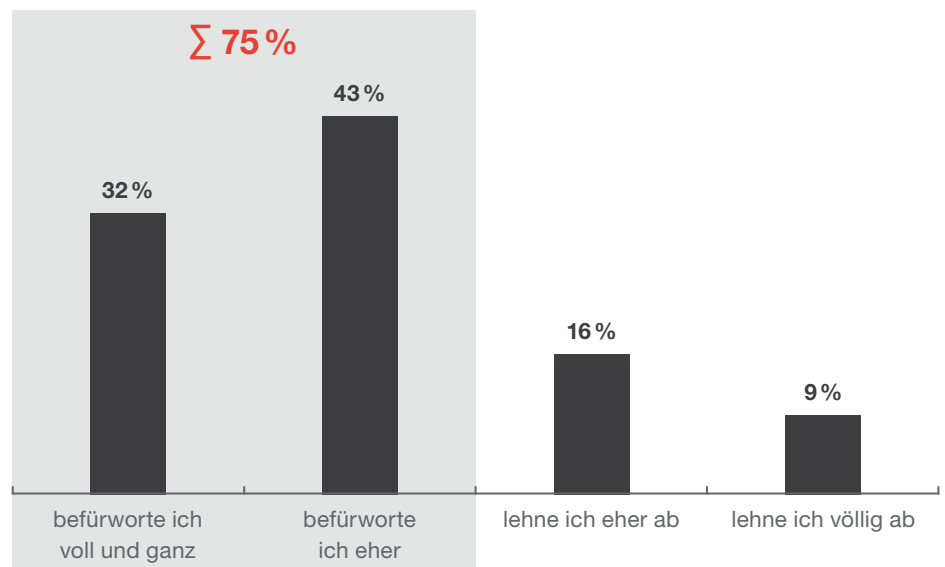
Basis: alle Befragten, n = 1.000 (Einfachnennung)

Mehrheit für mehr Handlungsfreiheit bei Ordnungshütern

Drei Viertel der Bundesbürger (75 %) sprechen sich für eine Ausweitung polizeilicher Befugnisse aus. Jedoch lehnen rund 16 % dieses Ansinnen eher ab, während 9 % der Befragten völlig gegen eine Ausweitung der polizeilichen Kompetenzen sind.

Abb. 7 Einschätzung zur potenziellen Erweiterung von Polizeibefugnissen

Verschiedene Landesregierungen haben bereits neue Polizeigesetze beschlossen, die der jeweiligen Landespolizei zusätzliche Rechte einräumen (z. B. Aufzeichnen von Gesprächen in Privatwohnungen, Sicherstellung von Paketen bzw. Briefen bei drohender Gefahr). Diese neuen Befugnisse sollen die innere Sicherheit besser gewährleisten. Wie stehen Sie persönlich zu solchen Ausweitungen der polizeilichen Befugnisse?



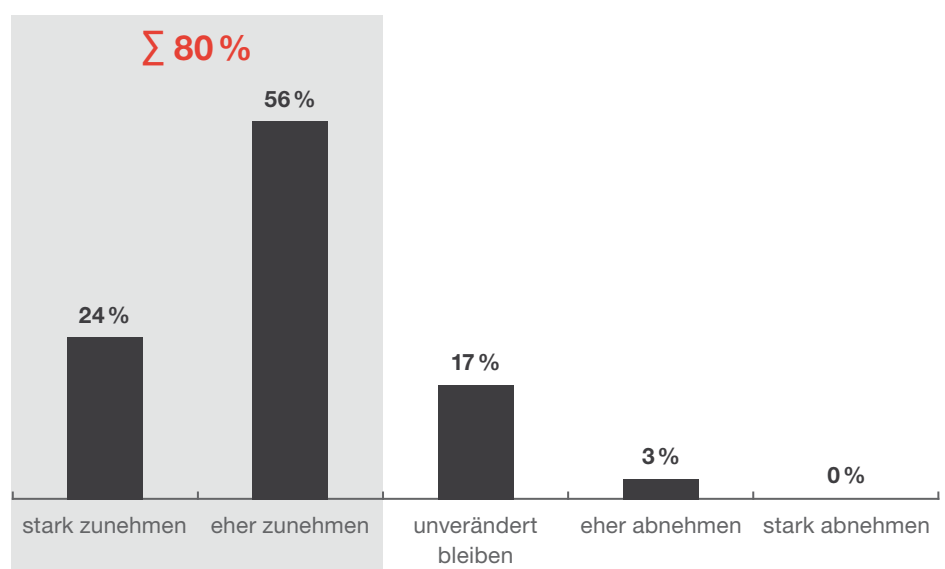
Basis: alle Befragten, n = 1.000 (Einfachnennung)

Bevölkerung fürchtet starke Zunahme von Digitalstraftaten

Insgesamt 80 % der Deutschen glauben, dass Kriminelle in den kommenden drei Jahren deutlich mehr Straftaten mithilfe digitaler Technologien verüben werden. Rund ein Viertel (17 %) hält es für möglich, dass die Anzahl der Verbrechen trotz fortschreitender polizeilicher Digitaltechnik unverändert bleibt. Nur 3 % sind der Meinung, dass die Zahl der Straftaten im digitalen Raum eher abnehmen wird.

Abb. 8 Erwartete Entwicklung der Straftaten mithilfe neuer Technologien

Denken Sie bitte an die fortschreitende Digitalisierung. Wie wird sich die Anzahl der Verbrechen, die mithilfe neuer Technologien (z. B. Onlinetrojanern) begangen werden, in den nächsten drei Jahren entwickeln?



Basis: alle Befragten, n = 1.000 (Einfachnennung)

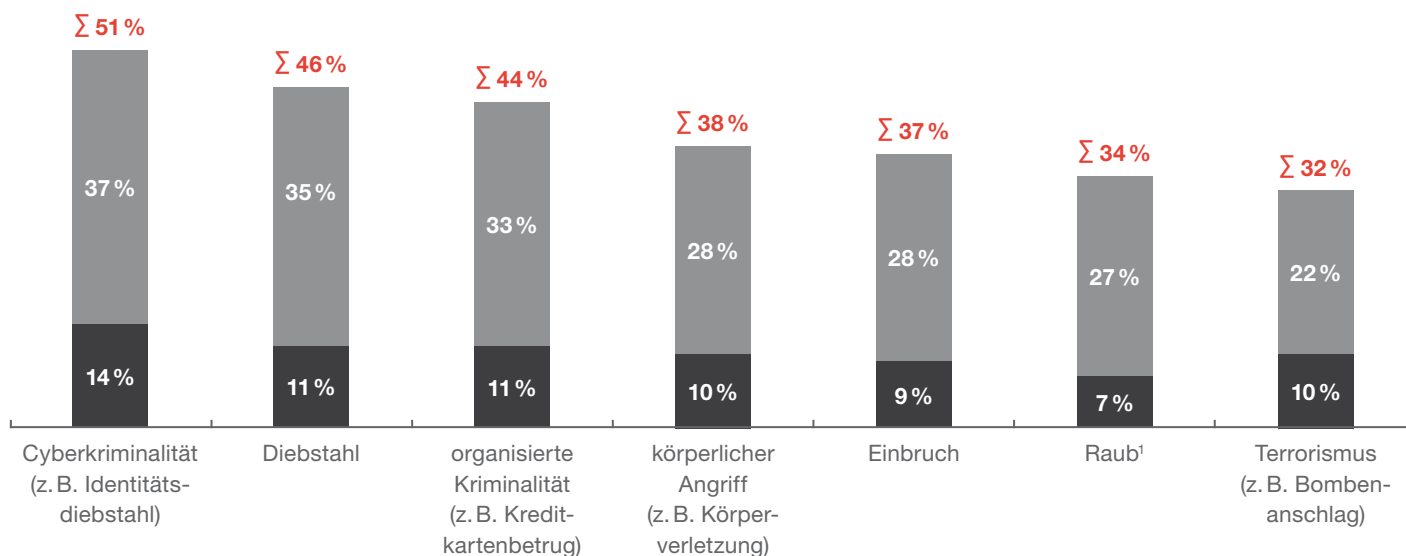
Jeder Zweite fühlt sich durch Cyberkriminalität bedroht

Rund die Hälfte der befragten Bundesbürger (51 %) sieht ein hohes Risiko, Opfer von Cyberkriminalität zu werden. Insgesamt 46 % halten es

beispielsweise für möglich, bestohlen zu werden. 44 % befürchten, sie könnten zum Ziel organisierter Kriminalität werden. Und fast ein Drittel (32 %) glaubt sogar, von Terrorismus bedroht zu sein.

Abb. 9 Empfundenes Opferrisiko im Zusammenhang mit Cyberkriminalität

Wie hoch schätzen Sie das Risiko ein, in den nächsten drei Jahren Opfer der folgenden Straftaten zu werden?



¹ Diebstahl unter Androhung oder Anwendung von Gewalt.

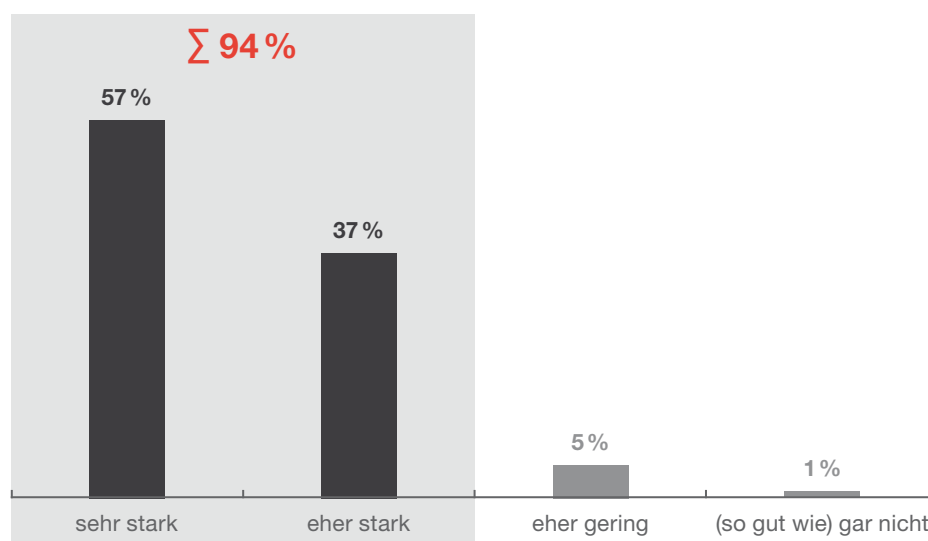
Basis: alle Befragten, n = 1.000 (Einfachnennung)

Bürger halten Ausbau digitaler Kompetenzen für notwendig

94 % der befragten Bundesbürger meinen, dass die digitalen Fähigkeiten der deutschen Polizei stark ausgebaut werden sollten. Dagegen finden 6 %, ein entsprechender Ausbau solle allenfalls in geringem Maße erfolgen.

Abb. 10 Bewertung der polizeiinternen Digitalkompetenz

Wie stark müssen die digitalen Fähigkeiten der Polizei Ihrer Meinung nach ausgebaut werden, damit sie Kriminalität auch in Zukunft effektiv bekämpfen kann?



Basis: alle Befragten, n = 1.000 (Einfachnennung)

Klarer Wunsch nach modernen Überwachungstechnologien

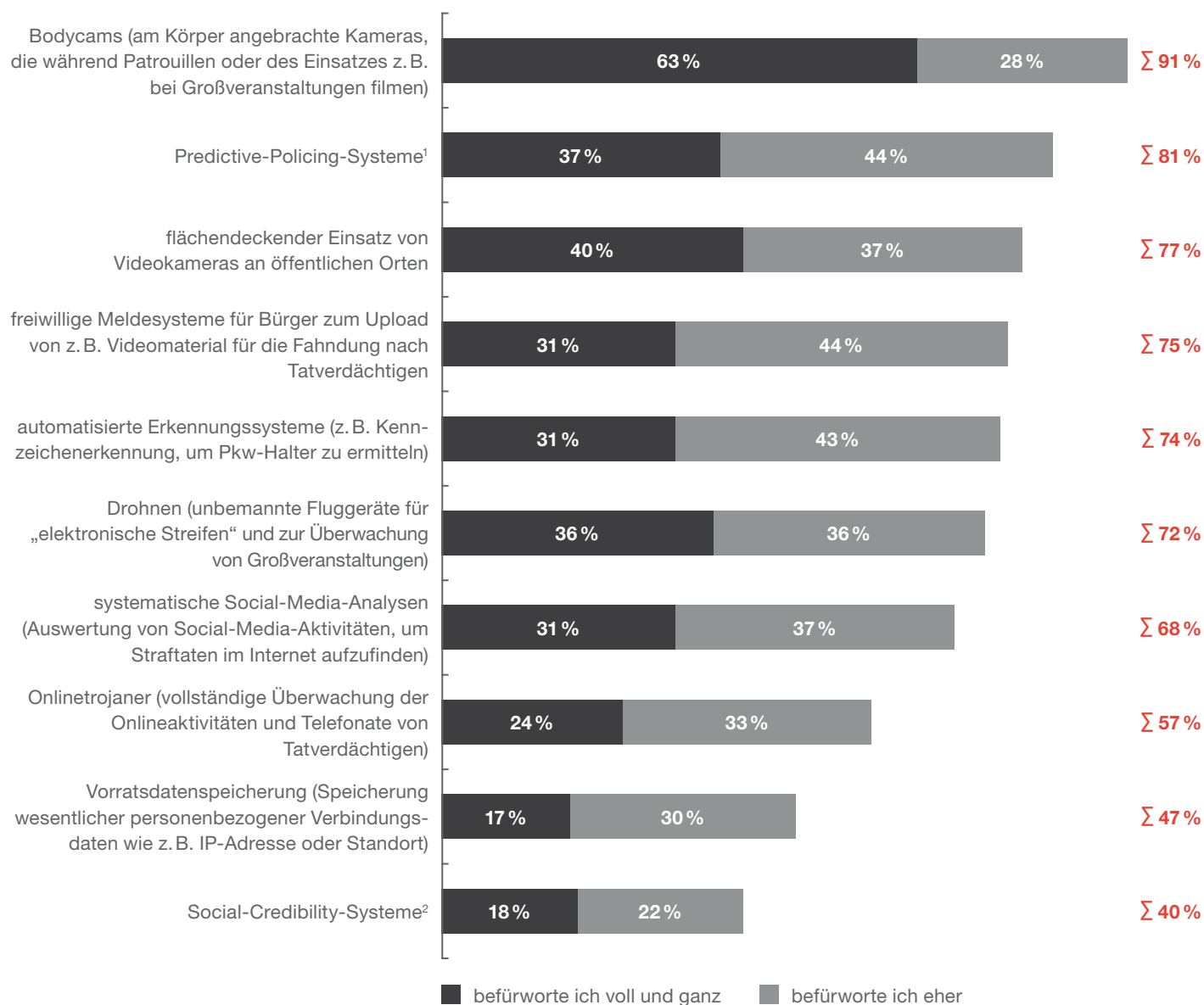
Neun von zehn Bundesbürgern (91 %) sagen, die Polizei solle während ihrer Patrouillen oder bei Großveranstaltungen mit am Körper

angebrachten Kameras unterwegs sein. Fast drei Viertel (74 %) befürworten zudem automatisierte Erkennungssysteme, um Pkw-Halter nach Vergehen im öffentlichen Straßenverkehr schneller zu ermitteln.

Auch andere neue technologische Lösungen finden breiten Anklang. Überwiegend ablehnend sehen die Bundesbürger Vorratsdaten-speicherung und Social-Credibility-Systeme.

Abb. 11 Welche Technologien die Polizei einsetzen sollte

Inwieweit würden Sie die Verwendung der folgenden neuen Technologien durch die Polizei zur Vermeidung oder Aufklärung von Straftaten befürworten?



¹ Vorhersagende Polizeiarbeit auf Basis gesammelter Daten bisheriger Straftaten, z. B. Bewegungsprofile, Muster von Straftaten wie Einbruchserien.

² Polizeiliche Informationen zum Verhalten der Bürger werden gesammelt und ausgewertet. Bei gutem Verhalten gibt es beispielsweise bessere Konditionen bei Banken, Versicherungen usw.

Basis: alle Befragten, n = 1.000 (skalierte Abfrage)

Bevölkerung glaubt an Kriminalitätsvermeidung durch Technologie

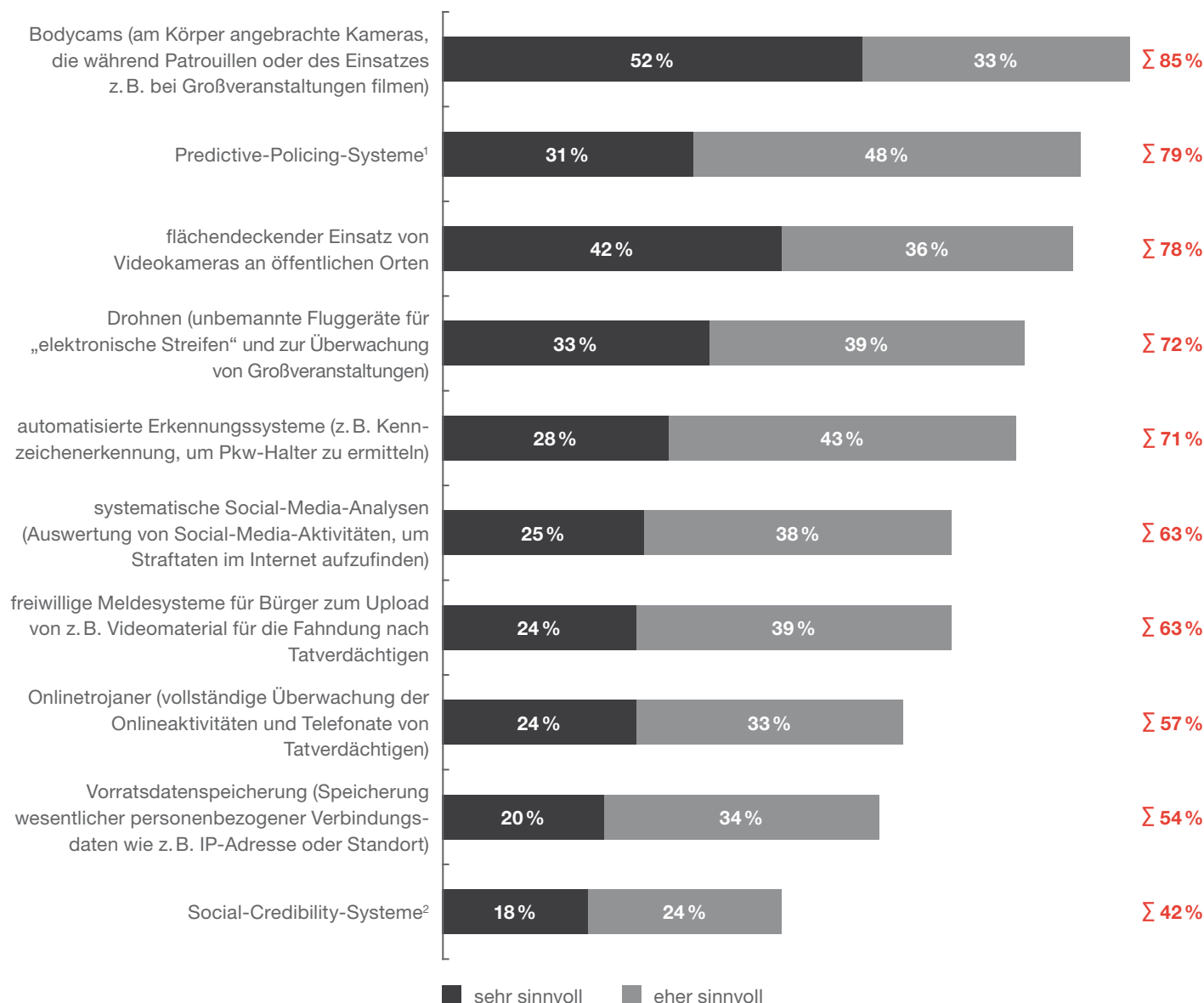
Die große Mehrheit der Bevölkerung glaubt, dass neue Technologien – beispielsweise Bodycams, Predictive-Policing-Systeme und Videokameras

zur Überwachung öffentlicher Orte – so eingesetzt werden können, dass sie zur Kriminalitätsvermeidung beitragen. 63 % der Befragten meinen auch, systematische Social-Media-Analysen im Internet könnten helfen,

Straftaten vorzubeugen. Den Einsatz von Onlinetrojanern unterstützen 57 % in diesem Zusammenhang. Noch 54 % Zustimmung sind es bei der Vorratsdatenspeicherung im Internet.

Abb. 12 Welche Technologien Straftaten verhindern könnten

Wie sinnvoll sind Ihrer Meinung nach die folgenden neuen Technologien für die Vermeidung von Straftaten?



¹ Vorhersagende Polizeiarbeit auf Basis gesammelter Daten bisheriger Straftaten, z. B. Bewegungsprofile, Muster von Straftaten wie Einbruchserien.

² Polizeiliche Informationen zum Verhalten der Bürger werden gesammelt und ausgewertet. Bei gutem Verhalten gibt es beispielsweise bessere Konditionen bei Banken, Versicherungen usw.

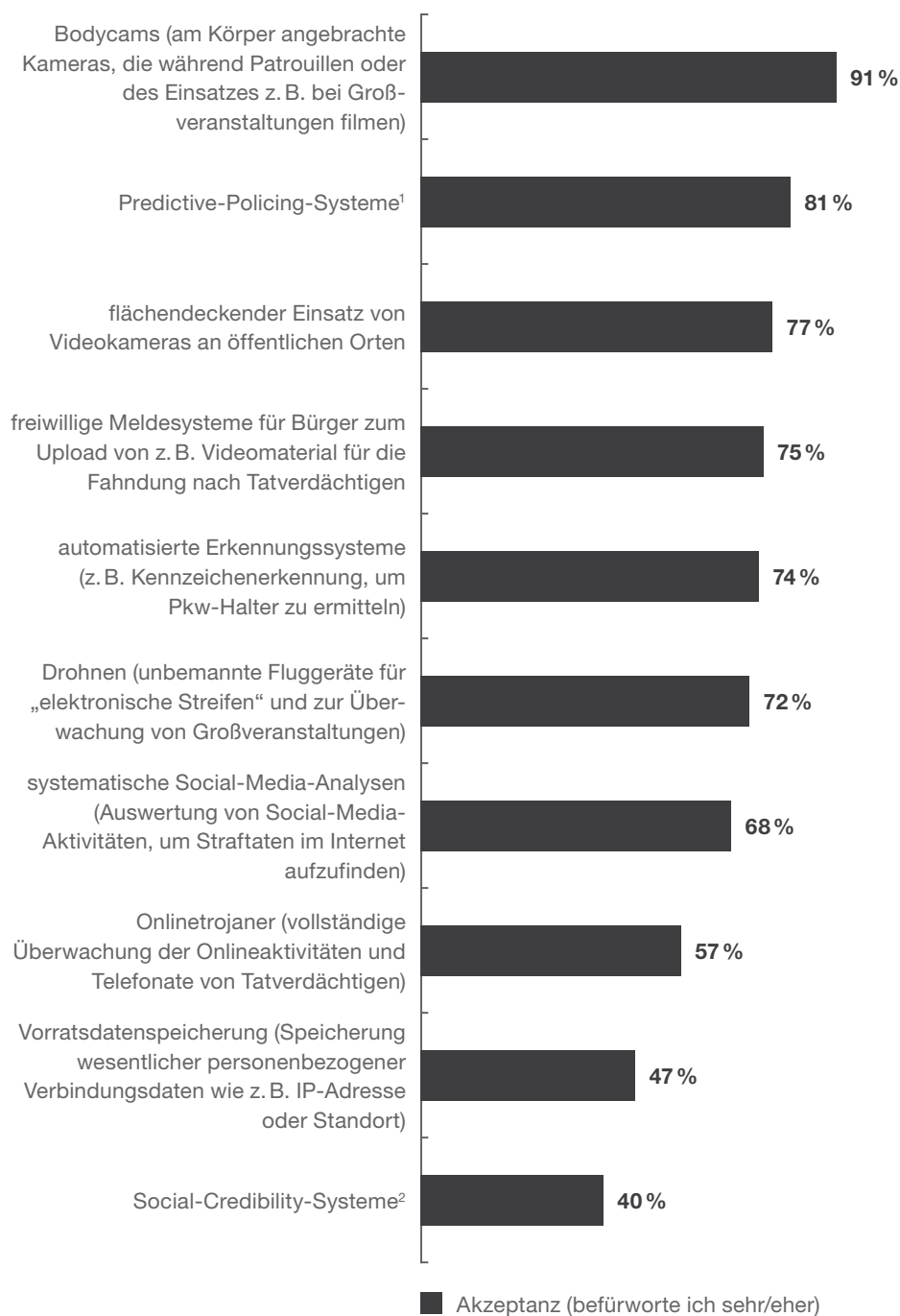
Basis: alle Befragten, n = 1.000 (skalierte Abfrage)

Hohe Akzeptanz auch mit Blick auf Prävention und Aufklärung

Bezüglich beispielsweise Bodycams an Polizeiuniformen und bei Predictive-Policing-Systemen glaubt die Bevölkerung nicht nur, dass diese Technologien Straftaten vermeiden helfen können. Auch die Akzeptanz der tatsächlichen Nutzung solcher Technologien ist sehr hoch (81 %). Im Rahmen von Predictive Policing analysiert die Polizei beispielsweise Muster bisheriger Einbruchserien mit digitalen Anwendungen, um die Wahrscheinlichkeit künftiger Straftaten zu berechnen. Am wenigsten akzeptiert die Bevölkerung hingegen Social-Credibility-Systeme (40 %), die ihr Wohlergehen protokollieren.

Abb. 13 Wie sehr verschiedene Technologien akzeptiert werden

Inwieweit würden Sie die Verwendung der folgenden neuen Technologien durch die Polizei zur Vermeidung oder Aufklärung von Straftaten befürworten? Wie sinnvoll sind Ihrer Meinung nach die folgenden neuen Technologien für die Vermeidung von Straftaten? Und wie sinnvoll sind diese neuen Technologien Ihrer Meinung nach für die Aufklärung von Straftaten?



¹ Vorhersagende Polizeiarbeit auf Basis gesammelter Daten bisheriger Straftaten, z. B. Bewegungsprofile, Muster von Straftaten wie Einbruchserien.

² Polizeiliche Informationen zum Verhalten der Bürger werden gesammelt und ausgewertet. Bei gutem Verhalten gibt es beispielsweise bessere Konditionen bei Banken, Versicherungen usw.

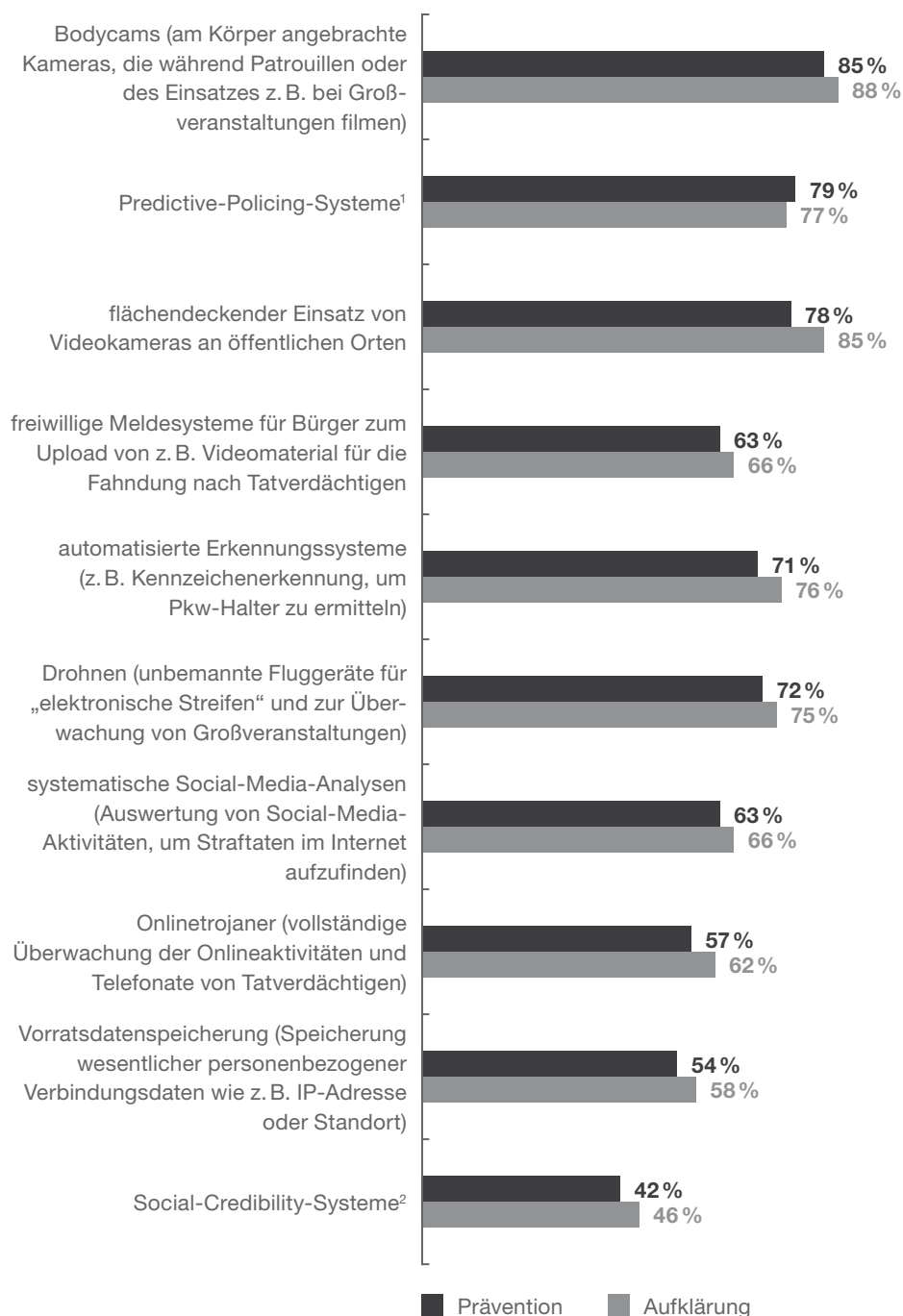
Basis: alle Befragten, n = 1.000 (skalierte Abfrage)

Bodycams und mehr für Prävention und Aufklärung

Die meisten der befragten Bürger meinen, dass polizeiliche Bodycams bei der Prävention (85 %) und Aufklärung (88 %) von Straftaten besonders sinnvoll sind. Aber auch andere Lösungen – beispielsweise öffentliche Videoüberwachung, Bürger-Meldesysteme, automatische Erkennungssysteme und Drohneinsätze – würden von einer Mehrheit der Bevölkerung mitgetragen.

Abb. 14 Welche Technologien sich für Kriminalitätsprävention und -aufklärung eignen

Inwieweit würden Sie die Verwendung der folgenden neuen Technologien durch die Polizei zur Vermeidung oder Aufklärung von Straftaten befürworten? Wie sinnvoll sind Ihrer Meinung nach die folgenden neuen Technologien für die Vermeidung von Straftaten? Und wie sinnvoll sind diese neuen Technologien Ihrer Meinung nach für die Aufklärung von Straftaten?



¹ Vorhersagende Polizeiarbeit auf Basis gesammelter Daten bisheriger Straftaten, z. B. Bewegungsprofile, Muster von Straftaten wie Einbruchserien.

² Polizeiliche Informationen zum Verhalten der Bürger werden gesammelt und ausgewertet. Bei gutem Verhalten gibt es beispielsweise bessere Konditionen bei Banken, Versicherungen usw.

Basis: alle Befragten, n = 1.000 (skalierte Abfrage)

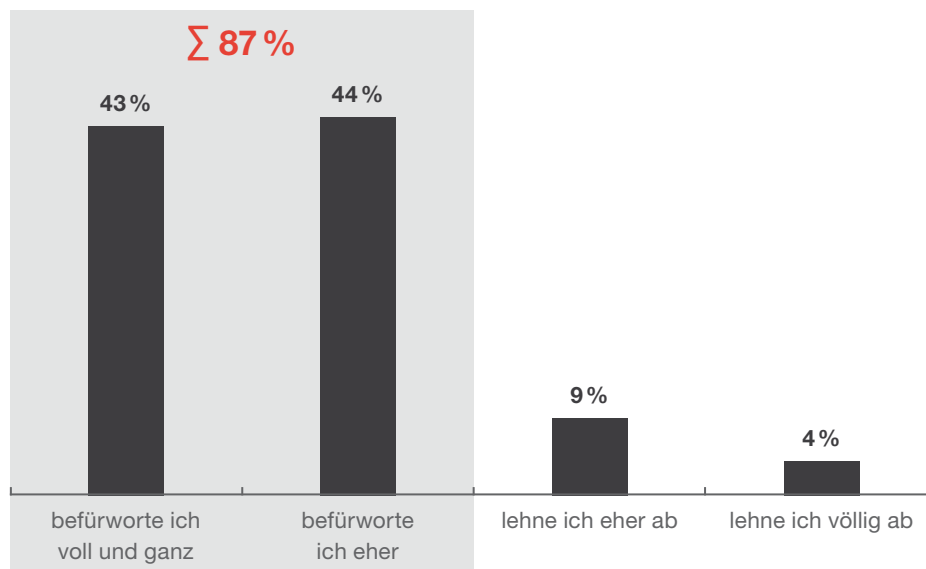
Große Mehrheit befürwortet bundesweite Vernetzung

Eine große Mehrheit der Bürger (87 %) ist dafür, neue Technologien bei der

deutschen Polizei bundesweit zu vernetzen. Insgesamt 9 % lehnen diese Idee allerdings eher ab, während 4 % eine Vernetzung völlig ablehnen.

Abb. 15 Ob neue Technologien bundesweit vernetzt werden sollten

Inwieweit würden Sie es befürworten, wenn diese neuen Technologien (z. B. Bodycams, automatisierte Erkennungssoftware) bundesweit vernetzt eingesetzt werden würden, um die Prävention und Aufklärung von Straftaten zu verbessern? Dabei hätten Polizeibeamte sämtlicher Polizeibehörden, die die entsprechenden Zugangsrechte haben, unabhängig von ihrem Zuständigkeitsbereich Zugang zu den erhobenen Daten.



Basis: alle Befragten, n = 1.000 (Einfachnennung)

Der Auftrag ist klar

Eine große Mehrheit der Menschen in Deutschland vertrauen der Polizei. Und ihnen ist klar, dass die Polizei sich an den technischen Fortschritt anpassen muss. Sie erwarten es geradezu. Aber was bedeutet die Digitalisierung im Polizeibereich eigentlich? Welche Chancen und Herausforderungen ergeben sich aus der technologischen Modernisierung für die Polizeiarbeit? Und was muss passieren, damit die Polizei die Erwartungen der Bevölkerung dauerhaft erfüllt?

Im Folgenden beleuchten acht hochkarätige Gesprächspartner aus Politik, Praxis und Wissenschaft die Polizei im technologischen Wandel jeweils aus ihren ganz eigenen Perspektiven. Lesen Sie die Interviews, prüfen Sie bei der Lektüre Ihre eigenen Thesen und lassen Sie sich inspirieren, wenn Sie sich – wie wir – an der Gestaltung einer zukunftsfähigen Polizei beteiligen möchten.

C Polizeiexperten im Gespräch



1 Perspektiven aus der Politik

„Die Politik macht viel zu wenig, um Handwerkszeug für effiziente Polizeiarbeit zu beschaffen.“



Die ehemalige Bundesjustizministerin Sabine Leutheusser-Schnarrenberger über sinnvolle Überwachungstechnologien, mangelnde Digitalfähigkeiten bei der Polizei und die Verantwortung der Politik für die Mängel

PwC/Strategy&: Frau Leutheusser-Schnarrenberger, beim Einsatz moderner Technologien für die Polizeiarbeit denken viele Menschen an Schlagworte wie Überwachungsstaat und Beschränkung der Privatsphäre. Zu Recht?

Sabine Leutheusser-Schnarrenberger: Wenn die Polizei das Verhalten von Menschen digital überwachen, erfassen und auswerten darf, sind solche Reflexe verständlich. Doch wir sollten in Ruhe differenzieren, was im Zeitalter der Digitalisierung wichtige Polizeiarbeit ist, was davon Grundrechte verletzt oder verletzen könnte und wie angesichts dessen die digitale Polizeiarbeit gestaltet sein muss.

Gibt es digitale Technologien, die Sie positiv beurteilen?

Durchaus. Wo zum Beispiel mit Drogen gedealt wird, wirkt Videoüberwachung im gesetzlichen Rahmen begrenzt präventiv. Wir wissen zwar, dass Videokameras allein viele Täter nicht abschrecken, aber dennoch tragen die Kameras zur Aufklärung von Straftaten bei.

Was halten Sie von Kameras an Polizeiuniformen, von sogenannten Bodycams?

Auch für die Nutzung von Bodycams habe ich Verständnis, weil es immer mehr Übergriffe auf Polizeibeamte gibt. Sogar auf Rettungssanitäter! Wenn ein Angreifer sich

zurückhält, weil die Polizei Bodycams trägt, haben diese Geräte einen guten Zweck erfüllt. Genauso sollen sie aber auch dokumentieren, wenn Polizeibeamte übergriffig gegenüber Bürgerinnen und Bürgern werden. Dazu gibt es inzwischen Regelungen in den Polizeigesetzen der meisten Bundesländer, was ich ebenfalls sehr begrüße.

Wann geht Ihnen Überwachung zu weit?

Zum Beispiel ginge mir zu weit, wenn Telekommunikationsdaten ohne nachweislichen Gefahrenhintergrund gespeichert würden, damit sich jemand irgendwann daraus bedienen kann. Anlasslose Vorratsdatenspeicherung lehne ich ab.

”

Die Vorratsdatenspeicherung wurde als Instrument der Strafermittlung überschätzt.

Bis vor dem Europäischen Gerichtshof (EuGH) in Luxemburg geklärt wird, ob die Vorratsdatenspeicherung zulässig ist, ist sie in Deutschland ohnehin ausgesetzt.

Das ist auch gut so. Interessant finde ich, dass dennoch kaum jemand danach ruft. Auch die Polizei nicht, weil sie gemerkt hat, dass sie als Instrument der Strafermittlung überschätzt war.

(Anmerkung der Studienautoren: Am 6. Oktober 2020 – Interview wurde vor diesem Datum geführt – hat der EuGH in vier Urteilen entschieden und seine Rechtsprechung aus dem Jahr 2016 fortgeschrieben: Eine pauschale und unbegrenzte Vorratsdatenspeicherung bleibt im Grundsatz unzulässig. Indes wurden Ausnahmen angeführt, insbesondere bei einer ernsthaften Bedrohung der nationalen Sicherheit und der Bekämpfung schwerer Kriminalität. Den nationalen Gesetzgebern gibt dies einen möglichen Handlungsrahmen vor. Die EuGH-Urteile beziehen sich auf Verfahren aus Frankreich, Großbritannien und Belgien. Die beiden Verfahren aus Deutschland waren zu Redaktionsschluss dieser Publikation noch anhängig.)

Die Coronaviruspandemie hat gezeigt, dass viele Menschen in der Not eine gewisse staatliche Überwachung wollen. Widerspricht sich das: einerseits diese gehörige Portion Digitalisierungsskepsis in Deutschland und andererseits der Wunsch nach mehr Überwachung?

Das war natürlich eine erste Reaktion auf eine Gefahr, die nicht sichtbar und in ihrer Dimension sogar von Experten nicht klar einschätzbar war. Trotzdem hat sie mich nachdenklich gemacht. Ich möchte infolge der Coronavirus-pandemie nicht noch mehr Staat.

Andere, die das auch nicht wollen, brachten bei Demonstrationen das Wort „Diktatur“ ins Spiel.

Auch das geht mir zu weit. Durch die Maßnahmen gegen COVID-19 sind wir weder in eine Diktatur noch in einen Überwachungsstaat noch in ein autoritäres System geraten. Ich fand es richtig, dass der Staat im Frühjahr 2020 zügig gehandelt hat. Dennoch war und ist die Debatte um die Rücknahme von Kontaktbeschränkungen und um die Ausübung individueller Freiheitsrechte notwendig.

Wie haben Sie die Polizeiarbeit während des Lockdowns im Frühjahr 2020 wahrgenommen?

Sagen wir so: Die Polizei hat von der Politik den Schwarzen Peter bekommen. Es gab ja seltsame Situationen. Da sitzt eine Dame allein auf einer Parkbank, liest ein Buch, kein Mensch ist in der Nähe und die Polizei jagt sie weg, weil das nicht mit den Social-Distancing-Maßnahmen vereinbar sei. Wer soll das verstehen? Aber das mache ich nicht der Polizei zum Vorwurf, sondern der Politik, weil die Politik unbestimmte Regelungen vorgegeben hat. Immerhin hat die Polizei dann doch recht schnell einen angemessenen Umgang mit der Situation gefunden.

Zurück zu modernen Technologien bei der Polizei: Wie beurteilen Sie die Ausstattung der Polizei damit – und ihre digitalen Fähigkeiten?

Nach wie vor haben wir da riesige Probleme. Das geht bei den personellen Ressourcen los.

Etliche Innenpolitiker wollen neue Stellen bei der Polizei schaffen.

Das kommt spät. Und: Wenn man immer noch besonderen Situationen – denken wir an die Morde der rechts-extremistischen Terrorzelle NSU oder an den Terroranschlag am Berliner Breitscheidplatz – neue Stellen bei der Polizei bewilligt, bringt das für die nächsten zwei, drei Jahre erst mal wenig. Denn die Stellen müssen erst einmal eingerichtet, die richtigen Personen dafür gefunden, eingearbeitet und eventuell auch ausgebildet werden.

Das heißt, die Polizei hinkt ihren Herausforderungen hinterher?

So ist es seit Längerem. Das wäre anders, hätten die Innenpolitiker ihre Versprechen, neue Polizeistellen zu schaffen, immer erfüllt. Das gilt übrigens auch für Investitionen in digitale und andere Instrumente.

Woran denken Sie hier?

Wenn die Polizei beispielsweise DNA-Proben genommen oder Computerfestplatten für Strafverfolgungen beschlagnahmt hat, darf es doch nicht wahr sein, dass diese potenziellen Beweismittel monatelang irgendwo herumliegen, weil die technologischen Mittel für die Auswertung fehlen.

”

Offenbar ist es einfacher, neue Gesetze zu machen als solche tiefgreifenden Mängel zu beheben.

Es fehlen sogar Diensthandys. Mitunter müssen Polizeibeamte an Tatorten die üblichen Fotos mit ihren privaten Smartphones knipsen.

Eine Katastrophe, weil es um polizeitaktische und überwiegend geheime Informationen geht. Dieser Missstand hängt damit zusammen, dass die Digitalfunkt-einführung, die vom früheren Bundesinnenminister Otto Schily begonnen worden ist, sich wegen technischer Probleme über Jahrzehnte hingezogen hat.

Private Smartphones mit dienstlichen Geräten zu tauschen, hört sich doch eigentlich einfach an.

Offenbar ist es einfacher, neue Gesetze zu machen, als solche tiefgreifenden Mängel zu beheben. Die Politik macht viel zu wenig, um unverzichtbares Handwerkszeug für effiziente Polizeiarbeit zu beschaffen. Der Modernisierungstau ist immens.

Weil Geld fehlt?

Was finanziell möglich ist, wenn der Wille das ist, hat einmal mehr die Coronakrise gezeigt.

Für eine zeitgemäße, effiziente Polizeiarbeit ist ein zentralistisches System vielleicht besser, als sich im föderalen Klein-Klein der Bundesländer zu verlieren.

Das sehe ich anders. In einem Flächenstaat von Deutschlands Größe etwas zentral von oben durchzuorganisieren, können wir vergessen. Das funktioniert noch schlechter als im föderalistischen System.

Oft heißt es, der deutsche Datenschutz würde eine effiziente digitale Polizeiarbeit verhindern. Stimmt das?

Der Datenschutz ist ein beliebtes Totschlagargument, wenn in Behörden etwas nicht funktioniert. Natürlich begrenzt er den Umgang mit personenbezogenen Daten. Und das ist gut so. Aber unser Datenschutz lässt auch eine Menge an Digitalisierung zu, die wir noch lange nicht ausgeschöpft haben.

Zum Beispiel?

Der Datenschutz lässt etwa zu, dass Informationen von einer Polizeistelle zu einer anderen und unter bestimmten Voraussetzungen sogar von der Polizei an den Verfassungsschutz weitergeleitet werden. Trotzdem gibt es immer wieder Fälle, in denen Informationen doch nicht weitergeleitet werden – teils mit schlimmen Folgen. Ich erinnere nochmals an den NSU und den Berlin-Terroristen Anis Amri. In beiden Fällen war nicht der Datenschutz für die verheerenden Informationspannen verantwortlich. Der Datenschutz erlaubt viel, wenn man ihn von Anfang an mitdenkt. Dafür braucht es Datenkompetenz, Willen zur Datenübermittlung und Rechtsexpertise.

Informationspannen sind eher menschliches Versagen?

Genau. Es ist ja nie eine Technologie, ein Gesetz, ein föderales System oder eine Information, die Fehler macht. Es sind die Menschen, die Technologien entwickeln, Gesetze verabschieden und Informationen verschweigen oder weitergeben.

Welche grundsätzlichen Verbesserungen wünschen Sie sich bei der deutschen Polizei?

Dass es weniger wichtig wird, ob sie grüne oder blaue Uniformen trägt. Und dass sie entsprechend ihrer gesetzlichen Befugnisse handeln kann, weil sie über die dafür notwendige technologische Ausstattung verfügt. Zudem wünsche ich mir mehr Austausch zwischen Polizei und Öffentlichkeit, Bürgergespräche zum Beispiel. Beide Seiten müssen einander zuhören, um Vorbehalte abzubauen und Überreaktionen zu vermeiden. Last, but not least brauchen wir eine gut ausgebildete und rechtsstaatlich handelnde Polizei. Sonst drohen Verhältnisse wie in den USA, wo viele Menschen der Polizei nicht mehr vertrauen.

Es gibt Politiker und Politikerinnen in Deutschland, die auch an der deutschen Polizei zweifeln.

Pauschalangriffe und Diffamierungen gegen die Polizei zerstören ihre Moral und vermitteln ein Bild, das sie nicht verdient hat. Diesen Appell richte ich durchaus auch an die Politik.

Vielen Dank für das Gespräch.



Sabine Leutheusser-Schnarrenberger, geboren am 26. Juli 1951 in Minden, hat Rechtswissenschaft in Göttingen und Bielefeld studiert. Von 1979 bis 1990 arbeitete sie beim Deutschen Patentamt in München, zuletzt als Leitende Regierungsdirektorin.

1990 zog sie für die FDP in den Deutschen Bundestag ein und wurde zwei Jahre später Bundesjustizministerin. Von diesem Amt trat sie 1996 nach der Entscheidung der Koalition für den Großen Lauschangriff zurück und konzentrierte sich auf ihre Abgeordnetenarbeit in anderen verantwortlichen Positionen, etwa 2005 bis 2009 als stellvertretende Fraktionsvorsitzende. 2009 bis 2013 war sie abermals Bundesjustizministerin.

Seit 2014 ist Sabine Leutheusser-Schnarrenberger Vorstandsmitglied der Friedrich-Naumann-Stiftung für die Freiheit. Zudem arbeitet die vielfach ausgezeichnete Politikerin ehrenamtlich in mehreren Stiftungen zur Förderung der Demokratie.

Sabine Leutheusser-Schnarrenberger
Bundesministerin a. D.

„Vielleicht übertreiben wir es manchmal mit dem Liberalismus.“



Der Präsident des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) Armin Schuster über politische Einflüsse auf die Polizeiqualität, Übergriffe auf Sicherheitskräfte, Pfeil und Bogen auf Streife und digitale Lösungen für mehr öffentliche Sicherheit

PwC/Strategy&: Herr Schuster, zunächst ganz allgemein: Wie schätzen Sie den Zustand der deutschen Polizei ein?

Armin Schuster: Die Frage ist pauschal schwer zu beantworten, weil sich die Polizei im föderalen System unserer 16 Bundesländer unterschiedlich entwickelt. Hinzu kommen die eigenständige Bundespolizei und das Bundeskriminalamt. Aber um eine Tendenz zu nennen: Zum Beispiel der Bayerischen Polizei würde ich eine deutlich bessere Note geben als anderen und auch in Baden-Württemberg oder Nordrhein-Westfalen wird mehr investiert als in anderen Ländern.

In welchen anderen Ländern?

Da bleibe ich jetzt mal zurückhaltend. Die Quantität und die Qualität der Polizei kann etwas mit der politischen „Farbenlehre“ in den Bundesländern zu tun haben. Die Berliner Landesregierung zeigt ja zum Beispiel, dass es unterschiedliche Haltungen zur Polizei gibt.

Was macht eine Landesregierung besser, die eine aus Ihrer Sicht bessere Polizei verantwortet?

Sie erkennt an, dass die Polizei für unsere Lebensqualität hochrelevant ist und lebt eine entsprechende Fürsorge für die Polizei, die sehr viel mit rechtlichen Befugnissen, Investitionen und öffentlicher Rückendeckung zu tun hat. Da gibt es erhebliche Unterschiede in den Landesregierungen.

Und auf Bundesebene?

Ich darf seit sieben Jahren ein wesentlicher politischer Treiber für insgesamt Tausende von neu geschaffenen Stellen bei der Bundespolizei, beim Verfassungsschutz und beim Bundesnachrichtendienst sein. Und ich habe das Glück, mit den richtigen Innenministern und Haushaltspolitikern zusammenzuarbeiten. Wir führen die Bundessicherheitsbehörden systematisch in die Zukunft, indem wir die Sicherheitsgesetze modernisieren und viel investieren – vor allem in polizeiliche Arbeitsplätze, in Technologie, aber auch in Kultur. Wir sollten wieder mehr eine Aktionspolizei haben als sie über Investitionsvermeidung zur Reaktionspolizei zu degradieren.

Wo sehen Sie den Unterschied?

Die Kapazitäten für wirksame Kriminalitätsprävention und Ermittlungen im öffentlichen und im digitalen Raum reichen nicht aus. Die Polizei kann überwiegend nur noch auf bereits begangene Straftaten reagieren, weil sie kaum Kapazitäten für eigentlich nötige Präventivmaßnahmen hat. Da denke ich vor allem an alltägliche Situationen wie Volksfeste, andere Events und an soziale Brennpunkte in Städten. Das alte Prinzip des Schutzmanns an der Ecke fehlt mir; das war noch institutionalisierter Austausch mit der Öffentlichkeit. Eine Aktionspolizei kann Straftaten durch solche Maßnahmen vermeiden helfen.

Seit einigen Jahren werden Polizisten häufiger angegriffen. Wie sehen Sie diese Entwicklung?

Deutschland ist ein sehr liberales Land und zum Glück kein Polizeistaat. Vielleicht übertreiben wir es aber auch manchmal mit dem Liberalismus. Übergriffe auf die Polizei, gerade von größeren Gruppen, sind aus meiner Sicht ein Indiz dafür.

Wie kann die Polizei gewalttätigen Übergriffen begegnen, damit sie nicht mehr passieren?

Wir haben ja 2017 die Strafen für Übergriffe auf Polizei- und Rettungskräfte verschärft. Deshalb sollte die Justiz hier unnachgiebiger verurteilen und die Politik entschiedener reagieren. Wie viele Politiker findet man denn noch, die Begriffen wie Recht und Ordnung eine hohe Bedeutung zumessen? Das fängt beim öffentlichen Urinieren, beim Beschmieren von Hauswänden, beim Konsumieren von Drogen und beim Dealen in öffentlichen Parks an.

Vielerorts wird das hingenommen.

Obwohl deshalb das Sicherheitsempfinden rechtschaffener Bürgerinnen und Bürger sinkt.

”

Das ist der Preis für das Mantra der Deeskalation. Jeder krisen-erfahrene Sicherheitsexperte weiß, dass Deeskalationsstrategien allein kein Allheilmittel sind.

Wie kann das sein?

Das ist der Preis für das Mantra der Deeskalation. Jeder krisenerfahrene Sicherheitsexperte weiß, dass Deeskalationsstrategien allein kein Allheilmittel sind und von bestimmten Personengruppen gnadenlos ausgenutzt werden. Das ist inzwischen nicht mehr nur ein polizeiliches,

sondern ein gesellschaftliches Problem. Denken wir beispielsweise auch kurz an die Schulen: Lehrer bekommen ja inzwischen Probleme mit Eltern, wenn sie, die Lehrer, von Kindern einen gewissen Respekt einfordern.

Können digitale Technologien der Polizei helfen, schwierige Situationen besser zu bewältigen?

Technologie hilft natürlich, auch bei der Prävention. Es ist schon ein erheblicher Unterschied, ob eine S-Bahn mit oder ohne Videoausstattung fährt. Ähnliche Beispiele gibt es viele. Großflächige Videoüberwachung, vor allem an sensiblen öffentlichen Orten, hätte eine präventive Wirkung und würde bei polizeilichen Ermittlungen enorm helfen. Andere europäische Länder sind da viel weiter: Die Schweizer Polizei etwa setzt längst digitale Kennzeichenerkennungssysteme an ihren Grenzübergängen ein.

Sie sind für mehr digitale Technologien bei der Polizei?

Unbedingt. Auch ich befürworte biometrische Videoüberwachung, also automatische Gesichtserkennung, zum Beispiel an Bahnhöfen und sozialen Brennpunkten, zur Fahndung nach Kapitalverbrechern oder Terrorgefährdern. Doch es ist schwierig, diese Technologie in Deutschland einzusetzen, weil sich bestimmte Parteien dagegen wehren.

Befürworten Sie den Einsatz von Bodycams?

Selbstverständlich auch dies. Sie wirken ebenfalls präventiv und sind unbestechliche Zeugen, sollte es zu Auseinandersetzungen zwischen Polizei und beispielsweise Randalierern kommen.

Sehen Sie auch Einsatzpotenzial für künstliche Intelligenz?

Predictive Policing würde ich sehr gern ausweiten. In einigen Bundesländern wird es bereits eingesetzt, mit teilweise guten Erfolgen. Wenn wir die Wahrscheinlichkeit künftiger Straftaten besser analysieren können, können wir auch die Polizeiarbeit zielgenauer steuern. Zudem denke ich an die systematische Analyse von Social-Media-Daten, um Straftaten zu verhindern und zu verfolgen. Kriminelle Gruppen verabreden sich ja gern über sogenannte soziale Netzwerke.



Es ist ein unhaltbarer Zustand, dass unsere Polizeibeamten in einer Welt, in der Straftäter die ganze Klaviatur moderner technologischer Instrumentarien missbrauchen, immer noch mit Pfeil und Bogen auf Streife gehen.

Wie stehen Sie zur Vorratsdatenspeicherung? Der Europäische Gerichtshof klärt zurzeit, ob sie mit EU-Recht vereinbar ist.

Ich hoffe, der Gerichtshof legitimiert sie und erkennt unser Gesetz als verfassungskonform an, damit wir beispielsweise Kinderpornografie und sexuellen Missbrauch besser verhindern und aufklären können. Es ist ein unhaltbarer Zustand, dass unsere Polizeibeamten in einer Welt, in der Straftäter die ganze Klaviatur moderner technologischer Instrumentarien missbrauchen, immer noch mit Pfeil und Bogen auf Streife gehen.



Armin Schuster, geboren am 20. Mai 1961 in Andernach am Rhein, hat Öffentliche Verwaltung und Wirtschaftswissenschaften studiert sowie die Laufbahnbefähigung für den höheren Polizeidienst erlangt. Zwischen 1985 und 1989 war er im Bundesinnenministerium tätig. 1987 trat er der CDU bei. Nach diversen Leitungspositionen bei der Bundespolizei wurde er 2009 in den Deutschen Bundestag gewählt. Sein Schwerpunkt dort ist die innere Sicherheit. So war er von 2015 bis 2017 Obmann im zweiten NSU-Untersuchungsausschuss für die CDU/CSU-Fraktion.

Technologische Tools sind das eine, Anwenderkompetenz das andere. Kann die deutsche Polizei mit ihren aktuellen Fähigkeiten digitale Technologien überhaupt wirkungsvoll nutzen?

Es gibt immer mehr technologiekompetente Polizistinnen und Polizisten. Aber wir müssen die nötigen Qualifikationen schnellstmöglich der gesamten Polizei vermitteln – und die rechtlichen Voraussetzungen für eine wirksame digitale Polizeiarbeit verbessern. Ich wünsche mir einen neuen Lehrstuhl Smart Policing an der Deutschen Hochschule der Polizei in Münster. Das könnte eine echte Initialwirkung haben, weil dort künftige Führungskräfte der Polizei aus ganz Deutschland ausgebildet werden.

Wie sehen Sie die Unterstützung der Polizei durch Unternehmen aus der Privatwirtschaft?

Grundsätzlich positiv, weil die Polizei nicht alle Ressourcen in den eigenen Reihen vorhalten kann – gerade im Zusammenhang mit der digitalen Transformation. Aber es ist auch heikel. Beauftragte Unternehmen müssen besonders vertrauenswürdig sein und der Polizei messbaren fachlichen Nutzen bringen.

Vielen Dank für das Gespräch.

Nach der Bundestagswahl 2017 (19. Wahlperiode) wurde Armin Schuster erneut das Amt des Obmanns im Innenausschuss von seiner Fraktion übertragen. Außerdem wurde er zum Vorsitzenden des Parlamentarischen Kontrollgremiums gewählt, das die Bundesregierung hinsichtlich der Tätigkeit der Nachrichtendienste des Bundes kontrolliert. Armin Schuster ist mit Ablauf des 9. November 2020 aus dem Deutschen Bundestag ausgeschieden, um sich auf seine neue Aufgabe als Präsident des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe zu konzentrieren. Dafür hatte ihn Bundesinnenminister Horst Seehofer nominiert. Am 10. November 2020 trat Armin Schuster das Amt an.

Armin Schuster

Präsident des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe

„Wir setzen auf zielgerichteten
Technikeinsatz bei Kriminalitäts-
schwerpunkten.“



Der Bayerische Landespolizeipräsident Prof. Dr. Wilhelm Schmidbauer über Fähigkeiten der Bayerischen Polizei bei der Cyberkriminalitätsbekämpfung, das Polizeiimage in der Öffentlichkeit, Vorteile moderner Polizeitechnologien und das Trennungsgebot zwischen Polizei und Nachrichtendiensten

PwC/Strategy&: Herr Prof. Dr. Schmidbauer, laut unserer repräsentativen Umfrage meinen 80 % der Bevölkerung in Deutschland, die rund 280.000 Polizistinnen und Polizisten hierzulande reichen nicht. Wie sehen Sie das mit Blick auf die personelle Ausstattung in Bayern?

Prof. Dr. Wilhelm Schmidbauer: Grundsätzlich ist die Bayerische Polizei personell gut ausgestattet. Mit mehr als 43.500 Stellen hat sie zurzeit sogar den bislang höchsten Stellenbestand aller Zeiten erreicht. Allerdings wächst auch die bayerische Bevölkerung. Unter anderem deswegen bin ich der Bayerischen Staatsregierung und dem Bayerischen Landtag sehr dankbar, dass unsere Polizei zwischen 2017 bis 2023 insgesamt 3.500 zusätzliche Stellen erhalten soll. Damit werden wir gut für die kommenden Herausforderungen aufgestellt sein.

Wie viele der versprochenen Stellen gibt es tatsächlich schon?

2.000 davon hat der Bayerische Landtag mit den Doppelhaushalten 2017/2018 und 2019/2020 bereits ausgebracht. Ich bin froh darüber, dass zahlreiche andere Bundesländer – und auch der Bund – ebenfalls zusätzliche Planstellen für Polizeivollzugsbeamte bereitgestellt haben.

Inwiefern spielen neue Herausforderungen wie Cyberkriminalität eine Rolle in der Bayerischen Polizei?

Qualifiziertes Personal ist die Voraussetzung für eine rechtsstaatliche, bürgerorientierte und professionelle Polizeiarbeit. Das Fundament hierfür wird bei der Bayerischen Polizei mit der Ausbildung gelegt. Dort werden natürlich auch zukunftsorientierte Themen wie Cybercrime behandelt. Aufbauend auf der Ausbildung werden die Beamten in Fortbildungen weiter spezialisiert. Es gibt bei jeder Polizeiinspektion geschulte Schwerpunktsachbearbeiter für Cybercrime, bei jeder Kriminalpolizeiinspektion gibt es ein Kommissariat Cybercrime mit IT-Kriminalisten. Das sind studierte Informatiker, die zu Polizeivollzugsbeamten weitergebildet wurden.

Sind Sie zufrieden mit dem bundesweiten Qualifikationsniveau für die Kriminalitätsbekämpfung im digitalen Raum?

Die Polizei kann natürlich immer noch besser werden. Insgesamt hat die Aus- und Fortbildung bei der Bayerischen Polizei allerdings inzwischen ein beachtliches Niveau erreicht.



Halten Sie die technologische Ausstattung für ausreichend?

Die Bayerische Polizei nutzt moderne digitale Technologien konsequent. Ein Beispiel hierfür ist das Programm „Mobile Police“, mit dem wir das mobile Einsatzmanagement schnell und nachhaltig voranbringen. Derzeit setzen wir beispielsweise mehr als 15.000 Smartphones mit zahlreichen Apps und über 5.000 Notebooks für das mobile und sichere Arbeiten ein. Damit sind wir deutschlandweit führend. Bundesweit gesehen gibt es, unter anderem bei der polizeilichen Ausstattung, freilich noch Optimierungsbedarf.

”

Eine grundlegende Kritik an der Arbeitsweise der Polizei ist damit nicht verbunden.

Laut unserer Bevölkerungsbefragung ist das Image der Polizei in der Bevölkerung stark überwiegend positiv. Verfolgt man regelmäßig die Nachrichten, könnte man allerdings meinen, das Gegenteil sei der Fall. Wie passt das Befragungsergebnis mit dem medialen Bild zusammen?

Auch das mediale Bild der Bayerischen Polizei ist überwiegend positiv. Die implizierte Kritik ist in vielen Fällen an unterschiedliche Ansichten und Wahrnehmungen bezüglich polizeilicher Maßnahmen anlässlich eines konkreten Ereignisses geknüpft, welche entweder als zu hart oder zu nachsichtig verstanden werden oder die hinsichtlich ihrer Durchführung mit anderen Erwartungen verbunden sind. Eine grundlegende Kritik an der Arbeitsweise der Polizei ist damit nicht verbunden, wodurch sich der in der Frage formulierte Widerspruch auflöst.

77 % der in der PwC/Strategy&-Umfrage befragten Menschen befürworten flächendeckende Videoüberwachungen, 74 % automatische Erkennungssysteme und 72 % Drohneneinsätze. Wären das auch für Bayern nützliche Anwendungen?

Gott sei Dank haben wir in Bayern eine so hervorragende Sicherheitslage, dass wir über flächendeckende Überwachungsmaßnahmen überhaupt nicht nachdenken müssen. Wir setzen vielmehr auf zielgerichteten Technikeinsatz bei Kriminalitätsschwerpunkten.

Welche Vorteile sehen Sie dabei?

Der offene Einsatz polizeilicher Videotechnik an kriminalitätsbelasteten Brennpunkten und gefährdeten Orten ermöglicht ein schnelles polizeiliches Eingreifen und – bei Bedarf – eine schnelle, zielgerichtete Fahndung. Zudem wirkt polizeiliche Videoüberwachung für Straftäter abschreckend und trägt deshalb in vielen Fällen zu einer sich verringernenden Kriminalität und – folglich – zu einem erhöhten Sicherheitsempfinden vor Ort bei. Genauso Erfolg versprechend sind anlassbezogene Drohneneinsätze, sei es zur Luftaufklärung oder Beweissicherung, sowie der Einsatz von automatischen Kennzeichenerkennungssystemen beispielsweise zum Aufspüren gestohlener Fahrzeuge.

Wo sehen Sie die größten Hindernisse für einen bedarfsgerechten, effizienten und ermittlungsspezifisch erfolgreichen Technologieeinsatz?

Zum Beispiel können wir aus Datenschutzgründen nicht ohne Weiteres marktübliche Standardprodukte einsetzen. Deshalb müssen digitale Hilfsmittel mit mitunter aufwendigen, komplexen Anpassungen genau auf die polizeifachlichen Bedarfe, den hohen Sicherheitsstandard und die rechtlichen Rahmenbedingungen angepasst werden. Hinzu kommen ständige Prozessveränderungen, um neuen Kriminalitätsphänomenen und sich verändernden technischen Rahmenbedingungen gerecht zu werden. Wir haben es also mit etlichen polizei-, strafprozess- und datenschutzrechtlichen Vorgaben zu tun. Das ist mitunter sehr komplex.

Wie gehen Sie mit solchen Komplexitäten um?

Ich sehe es als Aufgabe der Polizeien der Länder und des Bundes, den gesetzgeberischen Handlungsbedarf zu erklären, der durch den technologischen Fortschritt ausgelöst wird. Übrigens ist nicht jede Gesetzesänderung gleichzeitig eine Erweiterung polizeilicher Befugnisse. Aber wir müssen natürlich die polizeilichen Befugnisse an den technologischen Fortschritt anpassen, um unsere Mitbürgerinnen und Mitbürger wirksam zu schützen.

”

Diese Art der Arbeitsteilung wirkt qualitätssichernd, machtbegrenzend und stellt verfassungsrechtlich eine Art Grundrechtsschutz durch Verfahren dar.

Mitunter scheitert die Wirksamkeit an der föderalen Kompetenzverteilung oder dem Trennungsgebot zwischen Polizei und Nachrichtendiensten. Finden Sie diese beiden Grundsätze noch zeitgemäß?

Ja, die föderale Kompetenzverteilung erscheint mir weiterhin sinnvoll zu sein. Denn nur durch die – auch rechtsgeschichtlich begründete – Polizeiarbeit der Bundesländer können diese ihre unterschiedlichen Prägungen und Lagespezifika, aber auch ihre lokalen Brennpunkte bei der Gefahrenabwehr und Strafverfolgung ausreichend und zielgerichtet berücksichtigen. Ebenso stehe ich weiterhin positiv zum Trennungsgebot zwischen Polizei und Nachrichtendiensten.

Warum?

Dass operativ-polizeiliche Befugnisse bei den Verfassungsschutzämtern ausgeschlossen sind, hat eine wichtige verfassungsrechtliche Funktion: Die Informationserhebung wird von den Folgemaßnahmen, die auf Basis der Informationen durchgeführt werden, organisatorisch getrennt.

Aber wo sehen Sie heute den Vorteil dieser verfassungsrechtlichen Funktion?

Diese Art der Arbeitsteilung bei der Abwehr von fundamentalen Bedrohungen für den Staat und seine freiheitliche demokratische Ordnung wirkt weiterhin qualitätssichernd, machtbegrenzend und stellt verfassungsrechtlich eine Art Grundrechtsschutz durch Verfahren dar. Deswegen erlaubt das Bundesverfassungsgericht den Nachrichtendiensten weitergehende Überwachungsmaßnahmen als der Polizei. Die Trennung zwischen Polizei und Nachrichtendiensten ist eine verfassungsrechtliche Notwendigkeit, um frühzeitig elementare Bedrohungen erkennen und abwehren zu können.

Wenn Polizei und Nachrichtendienste in Deutschland aus rechtsstaatlichen Überzeugungen heraus organisatorisch getrennt sind, müssen die Befugnisse zur Datenübermittlung aber gesetzlich klar geregelt werden, oder?

Natürlich! Hier sehe ich an der einen oder anderen Stelle innerhalb Deutschlands noch Optimierungsbedarf, der einer breiten demokratischen Diskussion bedarf.

Ein Ziel der Polizeien der Länder und des Bundes ist es, den Informationsaustausch und die Vernetzung der Sicherheitsbehörden untereinander zu verbessern. Halten Sie das ebenfalls für sinnvoll?

Auf Vorschlag der Polizeichefs der Länder und des Bundes hat die Innenministerkonferenz in ihrer Herbstsitzung 2016 die sogenannte „Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der Inneren Sicherheit“ beschlossen. Deren Kernpunkt ist, die Informationsarchitektur der Polizeien in Deutschland zu modernisieren. Dadurch optimieren wir auch den digitalen und medienbruchfreien Austausch von Informationen zwischen den Polizeien von Bund und Ländern. Dem dient das Programm „Polizei 2020“, welches das Ziel verfolgt, die polizeiliche IT-Architektur zu harmonisieren und zu optimieren. Bayern unterstützt das Programm ausdrücklich – auch mit Manpower und Anwendungen, die wir beisteuern.

Und wie ist es mit dem Informationsmanagement innerhalb der EU?

Das muss – unter Beachtung der Grundrechte – ebenfalls effizienter gestaltet werden.

Sehen Sie hier Fortschritte?

Auf EU-Ebene gibt es bereits Informationssysteme – und weitere werden entwickelt, um für die Polizei relevante personenbezogene Informationen bereitzustellen. Allerdings führt die heutige Fragmentierung zu Informationslücken. Genau hier gilt es anzusetzen. Ich begrüße, dass bereits 2018 auf europäischer Ebene Rechtsakte vorgelegt wurden, die die Schaffung einer Interoperabilität der EU-Datensysteme zum Ziel haben. Auch das Kernstück des europäischen Datenaustauschs, das Schengener Informationssystem, wird weiterentwickelt, modernisiert und verbessert.

Muss die Polizei auch mehr öffentliche Aufklärungsarbeit leisten?

Öffentlichkeitsarbeit, also Transparenz und Bürgernähe in Bezug auf Digitalisierung und Technologieeinsatz, ist ein sehr wichtiger Teil der täglichen Polizeiarbeit. Dabei müssen wir auch vermitteln, dass die polizeiliche Technologiennutzung allein der Gefahrenabwehr und Strafverfolgung dient. Hierbei sind selbstverständlich die Vertraulichkeit und die Integrität von personenbezogenen Daten zu gewährleisten und rechtliche Rahmenbedingungen einzuhalten.

Herr Schmidbauer, wenn Sie noch mal 18 Jahre jung wären: Würden Sie mit Ihrem heutigen Wissen wieder eine Polizeilaufbahn einschlagen?

Selbstverständlich. Ja! Das Bewusstsein, für die Sicherheit der Bevölkerung zu arbeiten, ist – bei allen Herausforderungen – schließlich eine enorme Motivation.

Vielen Dank für das Gespräch.



Prof. Dr. Wilhelm Schmidbauer, geboren am 20. Februar 1958 in Regensburg, studierte – ebenfalls in Regensburg – Rechtswissenschaften. Seine berufliche Laufbahn startete er im Jahr 1986 im Münchener Polizeipräsidium. 1987/88 war er Referent für polizeiliche Einsatzangelegenheiten im Bayerischen Staatsministerium des Innern. 1988 wurde er promoviert. Danach war er bis 1991 persönlicher Referent des CSU-Generalsekretärs Erwin Huber. Es folgten etliche Führungspositionen bei der Bayerischen Polizei sowie ein Lehrauftrag an der Universität Regensburg für Polizei- und Sicherheitsrecht. Im März 2003 wurde Wilhelm Schmidbauer Polizeipräsident in München sowie 2007 Honorarprofessor an der Universität Regensburg. Im Juli 2013 übernahm Prof. Dr. Schmidbauer das Amt des Landespolizeipräsidenten von Bayern.

Prof. Dr. Wilhelm Schmidbauer
Bayerischer Landespolizeipräsident

„Es muss darum gehen, mit der Digitalisierung der Kriminalität mitzuhalten.“



Markus Eisenbraun, Leiter der Abteilung Cybercrime und digitale Spuren beim Landeskriminalamt Baden-Württemberg, über seine drei größten Wünsche bezüglich digitaler Polizeiarbeit, die Gründe dafür, Schwierigkeiten bei der Personalrekrutierung und die Relevanz sektorübergreifender Kooperationen

PwC/Strategy&: Herr Eisenbraun, über 90 % der in Deutschland lebenden Menschen meinen, die Polizei solle ihre digitalen Fähigkeiten ausbauen. Wo ist das Ihrer Ansicht nach besonders dringend?

Markus Eisenbraun: Die Polizei muss den digitalen Wandel in zweierlei Hinsicht meistern: Zum einen ist da die Digitalisierung der polizeilichen Vorgangsbearbeitung, zum anderen muss es darum gehen, mit der Digitalisierung der Kriminalität mitzuhalten.

Zunächst zur Vorgangsbearbeitung: Worum geht es Ihnen da genau?

Vor allem um Prozessautomatisierung, digitale Ausstattung – beispielsweise mit mobiler IT – und um die digitale Präsenz der Polizei. Hier wiederum geht es unter anderem um Social-Media-Auftritte und Plattformen für Onlineanzeigen. Bei all diesen Themen muss die Polizei genauso digital werden wie viele Unternehmen und zunehmend auch Verwaltungen. Wir wissen das und sehen uns auf dem richtigen Weg.

Und in Bezug auf die Digitalisierung der Kriminalität?

Kriminelle Personen und Organisationen nutzen digitale Technologien mittlerweile sehr intensiv. Denken wir nur an die Anonymisierung über das Darknet oder die Grenzenlosigkeit von Cybercrime. Digitale Spuren spielen mittlerweile bei jeglichen Kriminalitätsphänomenen eine Rolle.

Oder nehmen wir sogenannte Hass-Postings: Natürlich gibt es Beleidigungen seit Menschengedenken, aber die in sozialen Medien mögliche Anonymität und die reale räumliche Distanz zwischen Kommunikationsbeteiligten scheinen regelrechte Katalysatoren für strafbare Meinungsäußerungen zu sein.

Wenn Sie sich digitale Anwendungen für die deutsche Polizei wünschen dürften, die sie heute noch nicht oder nicht ausreichend nutzt: Welche wären das?

Als Erstes eine umfassende Plattform für E-Discovery, also für die Semantik digitaler Daten. Denn die Sicherung, Aufbereitung und Auswertung von digitalen Spuren überfordert den klassischen Ermittler heutzutage. Die schiere Menge der Daten, die Komplexität der Datenstrukturen und die Vielfalt der Anwendungen, die eine moderne Ermittlungsarbeit inzwischen braucht, sind mit den aktuell genutzten Methoden schlicht nicht mehr zu bewältigen.

Sehen Sie weitere Anwendungen?

Natürlich mobile IT mit einem durchgängigen Prozess vom Ereignisort bis zur Gerichtsverhandlung. Das würde die Ressourcen der Polizei eindeutig schonen. Diesen Weg beschreiten wir bereits mit dem Projekt „Polizei 2020“, aber auch vielen anderen IT-Projekten im Bund und bei den Ländern. Dennoch sind wir von einer umfänglichen Digitalisierung der polizeilichen Arbeit noch ziemlich weit entfernt.



Digitale Produkte von der Stange passen bei uns eher selten.

Warum geht das bei vielen Unternehmen schneller als bei der Polizei?

Weil polizeiliche Arbeit in vielerlei Hinsicht nicht mit den Prozessen und Aufgaben in der Wirtschaft vergleichbar ist. Wir müssen deshalb viele Anwendungen aufwendiger entwickeln und ausdifferenzieren. Digitale Produkte von der Stange passen bei uns eher selten.

Und der Mehraufwand für individualisierte Produkte passt in den öffentlichen Geldbeutel?

Tja, das ist häufig ein Problem. Aus diesem Grund wäre mein dritter Wunsch die Bereitschaft der Digitalwirtschaft, auf polizeiliche Bedürfnisse angepasste Produkte auch mit zu uns passenden Budgets zu entwickeln.

Was kann die Polizei tun, um die Bedürfnisse unterschiedlicher Generationen in den eigenen Reihen hinsichtlich digitaler Ausbildung zu berücksichtigen?

Wir müssen es schaffen, die digitalen Anforderungen bereits in der Ausbildung zu vermitteln. Beispielsweise wird es an der Hochschule der Polizei in Baden-Württemberg ab 2021 einen Studiengang für IT-Ermittler geben. Zugleich sollten die älteren, berufserfahrenen Kolleginnen und Kollegen das vorhandene Fortbildungsangebot nutzen. Glücklicherweise haben wir einen eigenen Bereich, der sich um die Fortbildung digitaler Ermittler kümmert.

Glauben Sie, dass mehr digitale Technologien und kompetente Anwender bei der Polizei die Sicherheit in Deutschland tatsächlich erhöhen können?

Zunächst einmal kommt die Polizei damit auf Augenhöhe mit Kriminellen. Technologien und digitalaffines Personal sind ja nicht die einzigen Erfolgsfaktoren. Es braucht auch einen zum digitalen Zeitalter passenden Rechtsrahmen sowie angepasste Eingriffsbefugnisse der Polizei.

Spätestens hier wird es allerdings auch um die Freiheitsrechte der Bürgerinnen und Bürger gehen.

Unbedingt – daran habe ich auch als Staatsbürger ein riesiges Interesse. Leider gibt es immer auch Menschen, die unsere Freiheit zulasten anderer und des Gemeinwohls ausnutzen. Es ist eine dringende gesellschaftliche Aufgabe, die richtige Balance zwischen Freiheitsrechten und Eingriffsbefugnissen auszuloten.

Im digitalen Raum eskaliert nicht nur die Kriminalität gegen Privatpersonen, sondern auch gegen Unternehmen und staatliche Institutionen, etwa Behörden. Schützt Deutschland sich gut genug dagegen?

Ich war viele Jahre für die IT in unserer Landesverwaltung zuständig und kann voller Überzeugung sagen: Die Verwaltung und insbesondere die Polizei in Baden-Württemberg versuchen alles, um im digitalen Raum sicher unterwegs zu sein.

Aber noch mal: Mitunter dauert das zu lange.

Da öffentliche Institutionen das Steuergeld der Bürgerinnen und Bürger verbrauchen, müssen sie das Risiko-Nutzen-Verhältnis bei großen Investitionen wie jenen in die Digitalisierung besonders genau abwägen. Das mag ein Grund dafür sein, dass die öffentliche Verwaltung langsamer als viele Unternehmen vorankommt. Insbesondere Unternehmen, die einem harten Wettbewerb unterliegen, haben oft gar keine Zeit abzuwägen. Sie sind gezwungen, sich schnellstmöglich zu digitalisieren, um am Markt zu überleben.



Dass die Frage nach dem Sinn einer beruflichen Tätigkeit vor allem die junge Generation immer stärker bewegt, ist eine Chance für die Polizei.

Das eine sind Technologien, das andere das Personal. Bei den Landeskriminalämtern sind viele Stellen unbesetzt, obwohl ausreichend Haushaltsmittel verfügbar sind. Warum?

Bei der Personalrekrutierung tun wir uns oftmals schwer. Sicherlich ist die Bezahlung ein Grund dafür. Aber auch das Image von Arbeitsplätzen im öffentlichen Sektor. Die Polizei ist alles in allem ein attraktiver Arbeitgeber. Das müssen wir viel stärker zeigen als bisher.

Was genau müssen Sie zeigen?

Es geht um Faktoren wie Arbeitsplatzausstattung, Work-Life-Balance und flexible Arbeitszeitmodelle. Da hat sich in den vergangenen Jahren viel Positives getan, mit dem wir punkten können. Und dann wäre da noch unsere sinnstiftende Aufgabe. Dass die Frage nach dem Sinn einer beruflichen Tätigkeit vor allem die junge Generation immer stärker bewegt, ist eine Chance für die Polizei. Klar ist aber auch: Die zunehmende Digitalisierung benötigt ein Fachkräftepotenzial, das der deutsche Arbeitsmarkt bislang noch nicht hergibt.

Wie sehen Sie angesichts des Fachkräftemangels Partnerschaften, die über die staatlichen Schutzinstitutionen hinausgehen?

Solche Partnerschaften sind seit der Gründung unserer Abteilung Cybercrime und digitale Spuren beim Landeskriminalamt Baden-Württemberg im Jahr 2012 eine zentrale Säule unserer Strategie. Beispielsweise arbeiten wir in der Aus- und Fortbildung mit öffentlichen Hochschulen zusammen. Wir haben eine Sicherheitskooperation mit fünf weiteren Landeskriminalämtern und dem Verband der IT-Wirtschaft, Bitkom. Aber auch Kooperationen zum Beispiel mit einem Unternehmen aus dem KRITIS-Sektor fallen mir da ein.

Sehen Sie solche Kooperationen als Anshub für die Digitalisierung der Polizei oder als Dauerzustand?

Cybercrime ist keine Herausforderung allein für staatliche oder private Institutionen. Dauerhaft können wir sie nur gesamtgesellschaftlich, also im sektorübergreifenden Schulterschluss wirksam bekämpfen.

Vielen Dank für das Gespräch.



Markus Eisenbraun (51) leitet die Abteilung Cybercrime und digitale Spuren beim Landeskriminalamt Baden-Württemberg. Zu den Schwerpunkten der Abteilung gehören die Sicherung und Aufbereitung von digitalen Spuren sowie Kommunikationsüberwachungen und

Ermittlungen im digitalen Raum. Markus Eisenbraun ist seit mehr als 30 Jahren bei der Polizei in Baden-Württemberg beschäftigt. Seine Laufbahn ist geprägt von der anfänglichen Arbeit im Streifendienst, von verschiedenen Stabsfunktionen, Projektleitungstätigkeiten und der mittlerweile hochspezialisierten Ermittlungsaufgabe in der digitalen Welt. Die dafür notwendigen Kompetenzen hat er im Rahmen seiner langjährigen Tätigkeit in der polizeilichen IT erworben.

Markus Eisenbraun

Leiter der Abteilung Cybercrime und digitale Spuren
beim Landeskriminalamt Baden-Württemberg

„Der Rechtsstaat funktioniert auch im Internet, wenn er die nötigen Kapazitäten dafür hat.“



Rainer Wendt, Vorsitzender der Deutschen Polizeigewerkschaft, über Ressourcenbedarf im digitalen Zeitalter, schädliches Silodenken, digitale Vernetzung mit Staatsanwaltschaften und die Polizei als Arbeitgeber für digitalaffine junge Menschen

PwC/Strategy&: Herr Wendt, unserer Bevölkerungsumfrage zufolge sehen 94 % der Menschen in Deutschland bei der deutschen Polizei einen Nachholbedarf in puncto Digitalkompetenz. Überrascht Sie der hohe Wert?

Rainer Wendt: Im Gegenteil. Mich überrascht, dass der Wert nicht höher ist. Bei der Polizei selbst dürften 100 % diesen Nachholbedarf sehen. Die Beschäftigten fordern vor allem mehr Ressourcen. Sie wissen sehr gut, welche digitalen Möglichkeiten es gibt – und auf wie viele davon sie bislang im Berufsalltag verzichten müssen.

Worauf zum Beispiel?

Zuerst denke ich da an Analysetools für verschiedenste polizeirelevante Daten, etwa für Prognosen zu Einsatzverläufen und Verkehrsunfällen. Solche Anwendungen wünscht sich sogar die ältere Polizeigeneration, der oft weniger Veränderungsbereitschaft unterstellt wird als den jungen Leuten. Und ja, natürlich, wir haben digitale Fähigkeiten und es gibt gute Ansätze, sie in der Breite zu etablieren. Aber wir haben auch einen riesigen Nachholbedarf. So viel, dass wir aufpassen müssen, nicht den Anschluss an jene Individuen und Organisationen zu verlieren, vor deren kriminellen Aktivitäten wir unsere Gesellschaft schützen sollen.

Welche Rolle spielt die Polizeigewerkschaft bei der Digitalisierung?

Wir machen Druck: grenzüberschreitend, öffentlich und in kleineren Kreisen. Auch die Deutsche Polizeigewerkschaft hat einen Anteil daran, dass Projekte wie „Polizei 2020“ zur Neuorganisation der bislang völlig zersplitterten IT-Infrastrukturen vorankommen.

Bislang ist die IT-Infrastruktur föderal zersplittert.

Richtig. Und das ist schlecht, weil die bisherigen IT-Strukturen – und übrigens auch föderale Eitelkeiten – gute Polizeiarbeit erschweren.

”

Ermittler können noch nicht mal auf Knopfdruck herausfinden, ob und wo in Deutschland eine verdächtige Person schon Ermittlungsverfahren am Hals hat.

An welcher Stelle merken Sie das konkret?

Wenn beispielsweise Vorgangsbearbeitungssysteme verschiedener Bundesländer inkompatibel sind und deshalb Recherchemöglichkeiten verhindert werden. Man muss sich das mal vorstellen: Ermittler können noch nicht mal auf Knopfdruck herausfinden, ob und wo in Deutschland eine verdächtige Person schon Ermittlungsverfahren am Hals hat. Ein anderes Problem ist, dass wir kaum bundesländerübergreifende Lagebilder zu Kriminalitätsphänomenen wie Raserei im Straßenverkehr auf Knopfdruck erstellen können. Sehr viele Daten sind zwar vorhanden, aber nicht vernetzt. Und das liegt nicht nur am föderalen System.

Woran liegt es noch?

Dass die Polizei nicht nur untereinander vernetzt sein muss, sondern ebenso mit den Staatsanwaltschaften. Diese haben die Hoheit über Strafverfahren. Und die Polizei führt die Ermittlungen für die Staatsanwaltschaften durch. Deshalb müssen digitale Fähigkeiten und die IT-Infrastrukturen im Sinne einer hohen Ermittlungsqualität und -effizienz auch bei der Justiz vorhanden und mit der Polizei vernetzt sein. Und bei diesem Thema ist der Reformstau vielleicht sogar noch größer, als wenn man die Polizei allein für sich betrachtet.

Sind die angesprochenen Defizite technologisch bedingt oder hängen sie auch mit dem Selbstverständnis der Organisationen zusammen?

Beides trifft zu. Es kommt immer wieder vor, dass einzelne Institutionen auf einem Berg von Informationen sitzen, aber niemanden von außerhalb draufschaauen lassen. Ein weiteres Manko ist, dass die Polizeien der einzelnen Bundesländer strukturell und qualitativ, gelinde gesagt, unterschiedlich organisiert sind. Und nicht zuletzt ist es die Haushaltspolitik, die den Möglichkeiten immer wieder Grenzen setzt.

Gibt es auch Positives zu berichten?

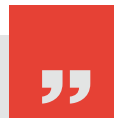
Durchaus. Nehmen wir Nordrhein-Westfalen: Dort haben Politik und Polizei mit dem Landesamt für Zentrale Polizeiliche Dienste eine aus meiner Sicht hochmoderne Behörde geschaffen. Die komplette IT-Struktur wurde zentralisiert und harmonisiert. Aber noch mal: An vielen anderen Orten steht die Digitalisierung der Polizei hintenan, weil beispielsweise erst mal die Toilettenspülungen wieder funktionieren und die Heizungen wieder heizen sollen und der Wandputz in Dienstzimmern ausgebessert werden muss.

Ein weiterer riesiger Investitionsstau ...

Allein in Berlin haben die Gebäude der Polizei mehr als eine Milliarde Euro Investitionsstau. Wenn wir warten, bis Hundertschaften von Handwerkern unsere Immobilien aufgepeppt haben, warten wir ewig auf die Digitalisierung der Polizei.

Digitale Anfänge gibt es ja bereits – Bodycams und Einsatz von Videotechnik an Brennpunkten etwa. Die kommen in der Bevölkerung sogar richtig gut an, wie unsere Umfrage zeigt. Ist das nicht erstaunlich? Begriffe wie „Polizeistaat“ und „Überwachungsstaat“ machen ja schnell die Runde, wenn es um Technologie bei der Polizei geht.

Das täuscht, weil die Leute, die so reden, mehr Beachtung in den Medien finden und deshalb mehr auffallen. Die PwC/Strategy&-Umfrage zeigt, dass die große Mehrheit der Menschen in Deutschland eher die Vorteile moderner Technologien für die innere Sicherheit sieht.



Es fehlt an Konzepten, Personal, Technik – und an politischem Willen, die nötigen finanziellen Mittel bereitzustellen.

Neue Technologien erfordern neue Fähigkeiten. Sind Sie zufrieden damit, wie diese der Polizei vermittelt werden?

Damit das hier nicht zu kurz kommt: Die Polizei kann eine ganze Menge und ist sicher deutlich besser als ihr Ruf. Polizeiangehörige, die digitalaffin sind, finden interessante Einsatzgebiete und können sich in hochwertigen Fortbildungen auf dem Laufenden halten. Was wir jedoch auch brauchen, ist eine einheitliche Aus- und Fortbildungsstrategie innerhalb der Polizei. Hierfür fehlt es an Konzepten, Personal, Technik – und an politischem Willen, die nötigen finanziellen Mittel bereitzustellen.

Stichwort Personal: Sie meinen, die aktuell rund 280.000 Polizistinnen und Polizisten in Deutschland sind nicht genug?

Wir brauchen mehr Personal, weil sich unser Betätigungsfeld auch mit dem digitalen Raum massiv erweitert hat. Und in den vergangenen Jahren ist ja Personal abgebaut worden. Mit Blick auf die Bundespolizei hat die Politik das mittlerweile verstanden, auch einige Bundesländer stellen mittlerweile mehr ein.

Um wie viele Neueinstellungen geht es dabei?

Die Bundespolizei hat ihre Einstellungszahlen schon in den vergangenen Jahren um rund 5.000 Frauen und Männer erhöht. Sie zählt mittlerweile deutlich mehr als 50.000 Beschäftigte. Der Personalaufbau bei der Bundespolizei soll weitergehen, weil sie zum Beispiel mithelfen muss, die europäischen Außengrenzen zu schützen. Auch dafür ist übrigens Digitalkompetenz gefragt.

Die Digitalkompetenz der Polizei sollte mit der Neueinstellung von jungen Polizistinnen und Polizisten steigen. Bekommen Sie ausreichend digitalaffinen Nachwuchs?

Der Polizeiberuf ist glücklicherweise für viele junge Frauen und Männer noch immer ein Traumberuf. Aber wir müssen uns anstrengen, die Besten von ihnen für uns zu gewinnen. Die Polizei hat dafür einiges zu bieten.

Sie meinen den Beamtenstatus?

Den auch. Aber vor allem die Polizeiausbildung, die sehr viele junge Leute immer schon interessant fanden und weiterhin finden. Einige starten mit der klassischen Polizeiausbildung und schließen IT-Zusatzbildungen an. Oder wir stellen IT-Experten aus der Privatwirtschaft ein und bilden sie nachträglich polizeilich aus. Beides funktioniert! Letztlich zählt aber das Gesamtpaket aus Ausbildung, Fortbildungen, Dienstgrad, ansprechenden Einkommen, Beamtenstatus auf Lebenszeit und spannenden Aufgaben.

”

Es ist viel passiert: Laufbahnen wurden durchlässiger, Aufstiegsmöglichkeiten flexibler.

Sind die streng hierarchischen Laufbahnmodelle bei der Polizei noch zeitgemäß?

Es ist ja schon viel passiert in den vergangenen Jahren. Laufbahnen wurden durchlässiger, Aufstiegsmöglichkeiten flexibler, im normalen Polizeialltag fallen Dienstgradunterschiede nicht mehr so auf wie früher. Dennoch: Das hierarchische System wird bleiben. Sonst würden viele Einsätze gar nicht funktionieren. Da braucht es klare Anweisungsberechtigungen, Verantwortlichkeiten und Selbstverständnisse.

Seit einigen Jahren etablieren sich Kooperationen zwischen der Polizei und privaten Sicherheitsdiensten. Wie sehen Sie die Zusammenarbeit?

Positiv. Natürlich bleibt die Polizei als hoheitlich tätige Behörde immer etwas anderes als ein gewinnorientiertes Unternehmen. Das schmälert deren Bedeutung für unser Sicherheitsgefüge aber nicht. Genauso wenig übrigens wie die sogenannten Einsatzassistenten, die als Tarifbeschäftigte im Öffentlichen Dienst zwar bei der Polizei beschäftigt, aber keine Polizeivollzugsbeamte sind.

Zudem gibt es auch bürgerschaftliches Engagement ...

... wie den Freiwilligen Polizeidienst in Baden-Württemberg. Dort übernehmen Bürgerinnen und Bürger gemeinsam mit der Polizei einfachere Aufgaben wie das Aufstellen von Absperrungen. Diese dort schon lange Tradition entlastet die Polizei stellenweise.

Wie sehen Sie Kooperationen der Polizei mit privatwirtschaftlichen Unternehmen im IT-Sektor?

Die werden wahrscheinlich zunehmen. Allein weil die Polizei nicht alle Kapazitäten vorhalten kann, die sie in unterschiedlichsten Spezialisierungen braucht. Deshalb lassen wir beispielsweise schon heute bestimmte Datenträger von privaten Unternehmen auswerten, allerdings eher ungern.

Können Sie sich solche Kooperationen auch bei der Cybercrime-Bekämpfung vorstellen?

Wenn es nicht anders geht, begrüße ich das. Im Mittelpunkt muss der Ermittlungserfolg stehen. Und es müssen alle Gesetze und Vorschriften eingehalten werden.

Wenn die Polizei im digitalen Raum unterwegs ist, ist das häufig umstritten. Muss die Polizei Ihrer Ansicht nach trotzdem mehr, zum Beispiel in sozialen Netzwerken, auf Streife gehen?

Soziale Netzwerke sind öffentliche Räume. Und überall dort, wo die Öffentlichkeit ist, muss die Polizei eingreifen können, wenn es zu Rechtsverstößen kommt. Das fängt bei Beleidigungen und Hassverbreitung an.

Beleidigungen und Hass sollen die Betreiber der Netzwerke in den Griff bekommen, heißt es oft.

Was in Deutschland strafbar ist und was nicht, sollten auch im digitalen Zeitalter die Gerichte feststellen und nicht irgendwelche Privatunternehmen. Die Politik neigt schon wieder dazu, den Rückzug anzutreten und den Staat zu schwächen. Wir sollten den Mut, die Kraft und das Personal aufbringen, um auch im Internet für Recht und Ordnung zu sorgen.

Sie persönlich werden im Internet häufiger angefeindet. Wie gehen Sie damit um?

Das meiste prallt ab, ich bin da entspannt. Glücklicherweise habe ich eine sehr gut funktionierende Geschäftsstelle mit einem Juristen als Geschäftsführer, der Rechtsverstöße sofort anzeigt. Mit Erfolg übrigens. Der Rechtsstaat funktioniert auch im Internet, wenn er die nötigen Kapazitäten dafür hat.

Vielen Dank für das Gespräch.



Rainer Wendt, geboren am 29. November 1956 in Duisburg, absolvierte ab 1973 eine Polizeidienstausbildung in Nordrhein-Westfalen. 1976 wurde er Hauptwachmeister. Als Polizeiobermeister studierte er an der Fachhochschule für öffentliche Verwaltung und schloss das Studium als Diplom-Verwaltungswirt und mit der Ernennung zum Polizeikommissar ab. Danach wirkte er in verschiedenen Führungsfunktionen der Schutzpolizei, zuletzt als Polizeihauptkommissar. Seit 2007 ist er Bundesvorsitzender der Deutschen Polizeigewerkschaft.

Rainer Wendt

Bundesvorsitzender der Deutschen Polizeigewerkschaft



„Die Wirtschaft muss die Kriminalitätsprävention im Internet weitgehend in die eigene Hand nehmen.“



Dr. Harald Olschok, Hauptgeschäftsführer des Bundesverbands der Sicherheitswirtschaft (BDSW), über die Zusammenarbeit mit der Polizei, Drohnen und andere Technologien im Einsatz sowie Ausbildungsqualität als Kooperationsargument

PwC/Strategy&: Herr Dr. Olschok, 85 % der Menschen in Deutschland haben ein positives Bild von der Polizei. Gehören Sie dazu?

Dr. Harald Olschok: Und ob. Das ist meine Wahrnehmung als Bürger, aber auch als Vater von drei Söhnen, die mehrere Freunde bei der Landes- und Bundespolizei haben.

Und sind die Freunde mit dem Polizistenimage zufrieden?

Mein Eindruck ist: Ja. Vor allem aber macht ihnen die Polizeiarbeit Spaß, obwohl sie herausfordernd ist. Die Entlohnung könnte allerdings besser sein.

Wie arbeiten private Sicherheitsdienste mit der Polizei zusammen?

Verlässlich und mitunter eng, etwa im Bereich der Luftsicherheit. Wenn zum Beispiel am Frankfurter Flughafen – in normalen wirtschaftlichen Zeiten – Personen kontrolliert werden, erledigen das rund 5.000 Beschäftigte privater Sicherheitsdienste. Die Aufsicht darüber hat die Bundespolizei, weil die gesetzliche Verantwortung für die Luftsicherheit natürlich beim Staat liegt. Ein anderes Beispiel ist der Schutz von Veranstaltungen. Insbesondere bei Fußballspielen ist vor dem Stadion die Polizei zuständig und drinnen sorgen private Unternehmen für Sicherheit. Weniger intensiv ist der Kontakt etwa beim Werkschutz – solange keine Straftaten passieren.

Am Flughafen München erfolgen die Personenkontrollen durch die Sicherheitsgesellschaft am Flughafen München (SGM). Das ist eine Gesellschaft des Freistaates Bayern. Welche Bedenken gibt es dort gegenüber privaten Sicherheitsunternehmen?

Die SGM war bei der Gründung zunächst eine Gemeinschaftsgesellschaft zwischen dem Freistaat und einem privaten Sicherheitsunternehmen. Dies wurde irgendwann geändert. In Nürnberg gibt es die Sicherheitsgesellschaft SGN noch als Gemeinschaftsunternehmen zwischen dem Freistaat und einem Mitgliedsunternehmen des BDSW. In Bayern haben wir als Verband seit vielen Jahren auch eine Kooperationsvereinbarung mit dem Landespolizeipräsidium. Bundesinnenminister Horst Seehofer hat am 1. Juli 2020 die Zuständigkeit für die privaten Sicherheitsdienste vom Bundeswirtschaftsminister übernommen. Beides hätte es bei Bedenken gegenüber unserer Branche nicht gegeben.

”

Integrierte Sicherheitslösungen, die Menschen und Technologie verbinden, werden immer wichtiger.

Straftäter sind heute zunehmend auch im digitalen Raum unterwegs, weshalb die Polizei unter Zugzwang kommt, ihre Digitalkompetenzen zu verbessern. Müssen private Sicherheitsdienste dies ebenfalls tun?

Die Digitalisierungstreiber für unsere Mitgliedsunternehmen sind vor allem Versicherer. Sie haben etliche Anforderungen entwickelt, die den Versicherungsschutz im Schadenfall positiv beeinflussen, zum Beispiel Alarm-, Brandmelde- oder Videoüberwachungsanlagen auf Firmengeländen. Die müssen installiert und vernetzt werden. Unsere Mitgliedsunternehmen betreiben solche Anlagen und reagieren bei Alarmen. Integrierte Sicherheitslösungen, die Menschen und Technologie verbinden, werden immer wichtiger.

Sind die Kunden privater Sicherheitsdienste bereit, für Digitalkompetenz mehr zu bezahlen als für Wachpersonal ohne Digitalkompetenz?

Grundsätzlich ja. In manchen Fällen können aber auch Einsparungen entstehen. Wenn zum Beispiel ein Firmengelände 24 Stunden am Tag von einer Person bewacht werden soll, kostet das rund um die Uhr Geld. Moderne Überwachungstechnologien sind über ihre Laufzeit deutlich günstiger. Am Ende der Meldekette muss eine leistungsfähige Alarmempfangszentrale mit Hightech und qualifizierten Mitarbeitern stehen.

Fragen Kunden nach neuen Überwachungstechnologien? Nach Drohnen etwa?

Über Drohnen im privatwirtschaftlichen Bereich wird mittlerweile viel diskutiert. Ich sehe da großes Potenzial und erste positive Beispiele: So überwacht das Sicherheitsunternehmen Securitas in Bitterfeld in Sachsen-Anhalt mit Drohnen einen großen Chemiepark. Ein positiver Effekt neben der reinen Überwachung ist: Sollten dort einmal Chemikalien austreten, kann zunächst eine Drohne anstelle eines Sicherheitsmitarbeiters den gefährlichen Austrittsort unter die Lupe nehmen. Auch beim Schutz von Veranstaltungen werden vermehrt Drohnen eingesetzt, um die Zahl der Besucher zu überwachen.

Sind digitale Technologien als Überwachungsinstrument für Sie immer nur positiv oder haben Sie auch mal Bedenken?

Leider hat das Wort „Überwachung“ für viele Menschen einen negativen Beigeschmack. Für mich sind digitale Technologien vor allem ein Sicherheitinstrument. Bedenklich finde ich vor allem, dass sie auch für kriminelle Handlungen genutzt werden. Einer Studie des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien, Bitkom, zufolge belaufen sich die jährlichen Schäden durch Cyberkriminalität allein in Deutschland mittlerweile auf über 100 Milliarden Euro.

Meinen Sie, der Staat könnte derartige Auswüchse verhindern?

Das hängt von der Art der Cyberkriminalität ab. Für bestimmte Angriffe ist der Staat zuständig. Der Polizei fehlt es an moderner Hard- und Software sowie an IT-Spezialisten. Ich meine, die Wirtschaft muss die Kriminalitätsprävention im Internet weitgehend in die eigene Hand nehmen. Die Eigenverantwortung der Wirtschaft ist gefordert.

Stichwort Kriminalitätsprävention: Wünschen Sie sich mehr digitale Lösungen, auch für Beschäftigte von privaten Sicherheitsdiensten? Bodycams zum Beispiel?

Ein klares Ja. Bodycams würden wir gern einsetzen, weil es an einigen Einsatzorten immer wieder Übergriffe gibt – im öffentlichen Personenverkehr, bei Veranstaltungen oder in Flüchtlingsunterkünften etwa. Da ist nicht nur die erst später auf Anforderung anrückende Polizei gefährdet, sondern vorher schon der jeweils vor Ort beschäftigte private Sicherheitsdienst. Mit Bodycams ließe sich beweisen, von wem Aggressionen ausgegangen sind. Zudem wirken Bodycams abschreckend und deeskalierend, was inzwischen hinreichend belegt ist. Deshalb sollten sie auch für private Sicherheitsdienste erlaubt sein.



Viele Datenschutzbestimmungen bremsen den sinnvollen Einsatz neuer Technologien.

Das sind sie noch nicht?

Teilweise ja, aber aus Datenschutzgründen nicht flächendeckend. Wir fordern ein Sicherheitsdienstleistungsgesetz für unsere Branche, das uns unter anderem Bodycams für Einsätze mit erhöhtem Risiko für Leib und Leben erlaubt. Schließlich übernimmt unsere Branche immer mehr Aufgaben für die innere Sicherheit. Viele Datenschutzbestimmungen bremsen den sinnvollen Einsatz neuer Technologien.

Aus unserer Bevölkerungsumfrage geht hervor, dass 77 % der Befragten flächendeckende Videoüberwachung, 74 % automatische Erkennungssysteme und 72 % den Einsatz von Drohnen durch die Polizei befürworten.

Dann sollte der Datenschutz in bestimmten Bereichen mal auf den Prüfstand kommen. Es muss ja nicht gleich eine flächendeckende Videoüberwachung wie in Großbritannien sein. Aber an Orten, an denen Menschen nicht sicher sind, weil es dort zum Beispiel häufig zu Taschendiebstählen oder Schlägereien kommt, wären Bodycams, Videoüberwachung und eine verantwortungsvolle Datenauswertung in höherem Ausmaß als bislang sinnvoll.

Die Alternative wäre physische Polizeipräsenz. Hat Deutschland genug Polizisten, um die innere Sicherheit zu gewährleisten?

Das glaube ich schon. Aber ist die Polizeiarbeit auch effizient genug? Müssen zum Beispiel studierte Polizisten auf Streife gehen, während der Bedarf an IT-Spezialisten ungedeckt bleibt? Da werbe ich gern für unsere qualifizierten Mitgliedsunternehmen: Wir könnten die Polizei bei ihrer Basisarbeit noch viel mehr entlasten, als wir es bislang dürfen. Das von uns geforderte Sicherheitsdienstleistungsgesetz zeigt die Voraussetzungen auf.

Es gibt Pilotprojekte, zum Beispiel mit sogenannten Hilfspolizisten.

Hilfspolizisten sind in der Regel kommunale Ordnungskräfte, die bei den Kommunen angestellt sind. In Frankfurt zum Beispiel laufen sie unter dem Namen Stadtpolizei. Die Stadtpolizei übernimmt überwiegend Aufgaben im Verkehrsbereich – Strafzettel verteilen zum Beispiel. Aber welche Kommune kann sich schon eine eigene Stadtpolizei leisten? Ein paar Groß- und Mittelstädte vielleicht.

Deshalb setzen immer mehr Kommunen private Unternehmen ein, die allerdings kaum Befugnisse haben.

Richtig. Die Stadtpolizei hat immerhin Minimalbefugnisse: So kann sie, wenn jemand über die Stränge schlägt, dessen Ausweisdaten aufnehmen und einen Platzverweis erteilen. Wenn private Sicherheitsunternehmen sowohl die Kommunen als auch die Polizei besser unterstützen sollen, sollten sie ebenfalls gut überlegte Minimalbefugnisse bekommen.

Stichwort Platzverweise. Die gab es häufig während des Lockdowns infolge der Coronaviruspandemie im Frühjahr 2020. Hat COVID-19 etwas für Ihre Branche verändert?

Die Pandemie hat für uns neue Aufgaben gebracht, die ich mir vor der Pandemie nicht hätte vorstellen können: So sind wir beauftragt, an vielen öffentlichen Orten – etwa in Parks, an Stränden der Ost- und Nordsee sowie auf Einzelhandelsflächen – die Abstands- und Hygienegebote durchzusetzen. Manche unserer Mitgliedsunternehmen übernehmen sogar Fiebermessungen innerhalb von Werkschutzaufgaben. Da kommen beispielsweise intelligente Thermalkameras mit künstlicher Intelligenz zum Einsatz.



Jammern hilft nicht. Wir müssen weitermachen und mit Qualität punkten.

Das heißt, Ihre Branche profitiert von der Coronakrise?

Bitte nicht gleich „profitieren“. Aufträge für den Schutz von Veranstaltungen und Einsätze für die Luftsicherheit brechen wegen des Coronavirus massiv weg, weil es im Jahr 2020 kaum Großveranstaltungen gab und die Fluggastzahlen eingebrochen sind. Aber Jammern hilft nicht. Wir müssen weitermachen und mit Qualität punkten.

Was macht Qualität in Ihrer Branche aus?

Zum Beispiel die Ausbildung. Seit 2002 gibt es den Ausbildungsberuf „Fachkraft für Schutz und Sicherheit“, den seither mehr als 11.000 junge Leute erlernt haben. Zudem gibt es seit einigen Jahren an mehreren Hochschulen den Bachelor- und den Masterabschluss als Sicherheitsmanager. Man kann heute private Sicherheit studieren: ein Quantensprung in unserer 119-jährigen Geschichte.

Was war die Motivation für diese Professionalisierung?

Wir wollten unser Image verbessern und den immer anspruchsvolleren Aufgaben gerecht werden. Das gelingt uns. Viele Aufträge betreffen ja nicht die Security, also den Schutz vor körperlichen Angriffen, Diebstahl oder Raub. Es geht auch oft um Safety, also um den Brand- und Umweltschutz etwa. Da ist die Qualifikation zum Beispiel angesichts des dichten Regulierungsnetzes ein Riesenthema.

Finden private Sicherheitsdienste genügend qualifizierte Mitarbeiterinnen und Mitarbeiter auf dem Arbeitsmarkt?

In den vergangenen Jahren ist es immer schwieriger geworden. Auch deshalb haben wir das Konzept der integrierten Sicherheit entwickelt. Das heißt, wir bieten

den Kunden aktiv Sicherheitsdienstleistungen mit digitalen Technologien wie Drohnen an. Sollte die Arbeitslosigkeit infolge der Coronapandemie steigen, wonach es leider aussieht, dürfte die Personalgewinnung für uns wieder etwas einfacher werden.

Wird die Digitalisierung bei Ihren Mitgliedsunternehmen zu Personalabbau führen?

Hier und da schon. Dafür braucht es anderswo neues Personal mit digitalen Kompetenzen.

Und wird die Digitalisierung die Branche Umsatz kosten, weil manche Dienstleistungen durch Technologieeinsatz günstiger für die Kunden werden?

Auch das ist möglich. Wichtiger sind allerdings die Gewinne. Hier bieten neue Technologien Steigerungspotenzial, weil sie die Effizienz bestehender Aufgaben erhöhen und neue lukrative Sicherheitsdienstleistungen ermöglichen. Ich bin sehr optimistisch für die Zukunft moderner privater Sicherheitsdienste. Denn die öffentlichen und privaten Auftraggeber brauchen uns. Eine wirksame Prävention entlastet die Polizei!

Vielen Dank für das Gespräch.



Dr. Harald Olschok, geboren am 14. Dezember 1955 in Bad Wildbad (Schwarzwald), hat Volkswirtschaftslehre in Freiburg und Wien studiert. Seit 1992 ist er Chefredakteur des Fachmagazins *DSD – Der Sicherheitsdienst* sowie Hauptgeschäftsführer des Bundesverbands der

Sicherheitswirtschaft (BDSW) und der Bundesvereinigung Deutscher Geld- und Wertdienste (BDGW). Im April 2018 wurde er zum Geschäftsführenden Präsidiumsmitglied des BDSW berufen. Zudem ist Dr. Harald Olschok Mitherausgeber mehrerer Fachbücher und Fachbeirat für den Masterstudiengang Sicherheitsmanagement an der Hochschule für Wirtschaft und Recht in Berlin.

Dr. Harald Olschok

Hauptgeschäftsführer des Bundesverbands der Sicherheitswirtschaft (BDSW)

3 Perspektiven aus der Wissenschaft

„Dieses Problem ist eine
Jahrhundertaufgabe.“



Dr. Thomas-Gabriel Rüdiger, Cyberkriminologe am Institut für Polizeiwissenschaft an der Hochschule der Polizei des Landes Brandenburg, über digitale Kompetenz der Polizei, warum die Kriminalstatistik auf den ersten Blick täuscht – und wie es gelingen könnte, Kriminalität im Netz besser zu verfolgen

PwC/Strategy&: Herr Dr. Rüdiger, wie beurteilen Sie die digitale Ausbildung bei der deutschen Polizei?

Thomas-Gabriel Rüdiger: Die digitale Ausbildung steht noch ganz am Anfang. Die Polizei sollte tatsächlich mehr Medienkompetenz entwickeln, schon während der beruflichen Ausbildung und des Studiums. Und das sage ich, obwohl die meisten Entscheider tendenziell offenbar davon ausgehen, dass junge Menschen sich im digitalen Raum auskennen, weil sie mit dem Internet aufgewachsen sind.

Sie sehen das anders?

Ja. Meiner Erfahrung nach ist die durchschnittliche Internetkompetenz der jungen Leute ernüchternd. Viele haben lediglich eine Art „Wischkompetenz“.

Was ist „Wischkompetenz“?

Viele wischen im wahrsten Sinne des Wortes oberflächlich über ihre Endgeräte. Sie wissen, wie sie Fotos ins Internet laden, Videos streamen und Facebook, Instagram und TikTok benutzen können. Aber ob und wann sie das überhaupt dürfen oder wie sie Informationen effizient recherchieren und sichern – da besteht meist Unsicherheit. Das gilt prinzipiell auch für Polizisten und Polizeianwärter. Die Polizei müsste einmal grundsätzlich definieren, was sie unter Medienkompetenz versteht.

Was verstehen Sie darunter?

Eine Basiskompetenz. Als in der ersten Hälfte des 20. Jahrhunderts Pferdekutschen von Autos abgelöst wurden, haben sicherlich viele Polizisten gesagt: „Lasst mich mit diesem neumodischen Schnickschnack in Ruhe.“ Heute hat meiner Schätzung nach ungefähr ein Drittel der Polizeiarbeit in irgendeiner Form mit dem Straßenverkehr zu tun. Der digitale Raum wird einen noch viel größeren Stellenwert einnehmen.

Über welches digitale Basiswissen sollten Polizistinnen und Polizisten verfügen?

Dazu gehört aus meiner Sicht beispielsweise, wie private Daten in sozialen Medien missbraucht werden können, wie man Hinweise auf kriminelle Handlungen im Internet erkennt, wie man Phishing-Mails sichert und ausliest, wie digitale Kriminalität überhaupt entsteht, wie genau Informationen im Netz recherchiert und verifiziert werden können oder wie sich Sexualtäter vernetzen und im Netz den Kontakt zu Kindern anbahnen. Solche Themen gehören ja längst zum digitalen Alltag, aber viele Polizistinnen und Polizisten wissen noch zu wenig darüber.

Cybercrime-Aufklärung gehört für Sie zum Basiswissen?

Nicht die Aufklärung – das ist Spezialisten-Know-how. Aber jeder Polizeiangehörige muss wissen, wie man Anzeigen im Zusammenhang mit digitalen Delikten aufnimmt und welche Modi Operandi dahinterstehen. Die Polizisten wissen ja auch, wie sie einen Ladendiebstahl oder Mord aufnehmen müssen, obwohl sie solche Straftaten nicht selbst ermitteln.

Das Internet gibt es mittlerweile seit mehr als 20 Jahren. Aber der Polizei fehlt Digitalkompetenz. Warum eigentlich?

Wegen der Präventivwirkung des Nichtwissens.

Wie bitte?

Die Theorie der Präventivwirkung des Nichtwissens von Popitz besagt vereinfacht: Wenn wir uns mit etwas nicht beschäftigen, sehen wir die negativen Effekte nicht. Angenommen, ich ahne, dass ich eine ernsthafte Erkrankung habe, fürchte mich aber vor der Diagnose und Behandlung: Dann verdränge ich die Symptome einfach und tue so, als wäre nichts. So geht es mir erst einmal besser.

Übertragen auf die Kriminalität bedeutet das?

In Sachen Kriminalität geht es Deutschland seit Jahren scheinbar immer besser. So sind die Straftaten in Deutschland seit einigen Jahren rückläufig – zumindest, wenn man nur die polizeiliche Kriminalstatistik anschaut. Zwischen 2015 und 2019 verringerten sich die Delikte von 6,3 Millionen auf etwa 5,4 Millionen pro Jahr, was einem Rückgang von fast 15 % entspricht.

”

Das Hellfeld physischer Handlungen hat sich in das Dunkelfeld digitaler Delikte verschoben.

Das klingt doch erst mal gut.

Klingt gut, aber eigentlich müsste es statistisch gesehen mehr gemeldete und als strafbar angenommene Verhaltensweisen geben, wenn Bevölkerungszahl und Bevölkerungsdichte zunehmen. Wenn Politiker sich wundern, dass die Kriminalstatistik besser ausfällt als je zuvor, aber das Sicherheitsempfinden der Bürger dennoch anscheinend abnimmt, kann ich nur sagen: Meiner Ansicht nach ist die Kriminalität als soziales Phänomen nicht zurückgegangen. Vielmehr hat sich das Hellfeld physischer Handlungen in das Dunkelfeld digitaler Delikte verschoben.

Und warum zeigt uns die Statistik das nicht?

Weil die polizeilichen Kriminalstatistiken Straftaten im Internet noch weniger realistisch erfassen als Kriminalität im physischen Raum. Die Statistik weist ja nicht die tatsächliche Kriminalität aus, sondern lediglich die angezeigten Sachverhalte. Im digitalen Raum ist die Anzeigenquote aber noch sehr viel geringer als im physischen Raum. Zugleich gibt es dort immer mehr Rechtsverstöße – und die Verstöße erhalten einen globalen Charakter. Das heißt, die Kriminalstatistik erfasst heute in Wirklichkeit viel weniger Straftaten als früher, als es noch kein Internet und keine Cyberkriminalität gab.

Weil die Polizei im Internet kaum auf Streife geht?

Auch daran liegt es. Es hat aus meiner Sicht stark damit zu tun, wie die Bevölkerung die Polizei wahrnimmt. Wenn die Menschen davon ausgehen, dass die Polizei Straftaten ohnehin nicht ahnden kann, zeigen sie Vergehen seltener an. Das gilt für das Internet besonders aufgrund der angenommenen Anonymität und Globalität der Phänomene. Wenn die Polizei mehr Straftaten im Netz sichtbar ahnden würde, stiege der Abschreckungseffekt – der bislang sehr niedrig ist – deutlich. Ein paar verdeckte Ermittler genügen dafür aber nicht.

Wie könnte mehr Präsenz aussehen?

Einige positive Beispiele gibt es: Nachdem illegale Streamingplattformen stillgelegt wurden, steht hinter der Internetadresse mitunter eine Beschlagnahmeseite der Polizei. Und die Berliner Polizei hat einmal Aufrufe auf Facebook, den Reichstag zu stürmen, mit einem eigenen

Account kommentiert. Einflussnahmen über Social-Media-Accounts der Polizei können viel bewirken, doch es gibt noch zu wenige davon. Die Polizei in den Niederlanden hat zehnmal mehr Social-Media-Accounts als die deutsche.

Aber warum tut sich da so wenig bei der deutschen Polizei?

Vielleicht fehlt der politische Wille. Denn wäre die Polizei im digitalen Raum präsenter, würde die Anzeigenquote im Internet steigen und – jetzt kommt die Krux – vermutlich die Aufklärungsquote sinken, weil die Polizei eben noch nicht genug Ressourcen und Kompetenz fürs Netz und die vielen Straftaten dort hat. Bislang ist – je nach Delikt – die Aufklärungsquote recht hoch.

”

Beim sogenannten Cybergrooming, so wird die onlinebasierte Anbahnung des sexuellen Missbrauchs von Kindern genannt, haben wir derzeit eine Aufklärungsquote von fast 90 %. Die Zahl suggeriert Erfolg, doch sie trügt.

Puh. Das muss man erst mal verstehen. Wie passt eine hohe Aufklärungsquote mit mangelnder Digitalkompetenz zusammen?

Ein Beispiel: Beim sogenannten Cybergrooming, so wird die onlinebasierte Anbahnung des sexuellen Missbrauchs von Kindern genannt, haben wir derzeit eine Aufklärungsquote von fast 90 %. Die Zahl suggeriert Erfolg, doch

sie trügt. Denn kriminologisch gesehen deutet eine derart hohe Aufklärungsquote bei einem niedrigen Hell- und hohen Dunkelfeld darauf hin, dass Straftäter so selten angezeigt werden, dass sie unvorsichtig werden.

Und wenn sie dann aber doch angezeigt werden?

Dann kann die Polizei sie aufgrund teilweise unvorsichtiger Vorgehensweisen der Kriminellen recht schnell ermitteln. Wenn spürbar und/oder sichtbar gegen mehr Straftäter ermittelt würde, würden diese Leute cleverer vorgehen und die Aufklärungsquote fiele. Und welcher Politiker will schon eine sinkende Aufklärungsquote verkünden? Auch gegen solche Hiobsbotschaften wirkt das Nichtwissen von Straftaten präventiv. Und es gibt noch ein Problem.

Welches?

In Deutschland muss jeder Polizist bei einem Anfangsverdacht Ermittlungen einleiten, sonst macht er sich eventuell selbst strafbar. Das nennt man „Legalitätsprinzip“. Es ist ein Konzept, das für den physischen, aber nicht für den digitalen Raum gedacht ist. Studien gehen davon aus, dass durchschnittlich 10 % aller analogen Delikte tatsächlich angezeigt werden. Davon wiederum werden nur ganz wenige durch die Polizei selbst, wenn sie beispielsweise eine Straftat auf Streife bemerkt, angezeigt. Die meisten Anzeigen kommen von Opfern und Zeugen.

Und wo sehen Sie ein Problem?

Die Akzeptanz der Polizei in der Öffentlichkeit hängt eben auch davon ab, dass der Bevölkerung nicht alle Straftaten bekannt werden – im Sinne einer absoluten Verhaltenstransparenz. Wenn man wüsste, was der Spaziergänger im Park oder der Sitznachbar im Bus alles begangen hat und dass er für die meisten Delikte eventuell gar nicht bestraft wurde, würde dies die Hemmschwelle und das Vertrauen in die Gültigkeit der Normen senken. Es bleibt also in den meisten Fällen unsichtbar, dass Straftaten begangen und nicht verfolgt werden – daher entsteht auch das Gefühl, dass der Staat mit allen Straftaten umgehen kann.

Und genau das gilt für das Internet nicht?

Genau. Denn im Netz ist die Kriminalität stärker sichtbar – ich spreche hier von einer Art digitaler Kriminalitätstransparenz – und sie wird auch kaum geahndet. Wer zum Beispiel in seinen Spamordner schaut, findet dort normalerweise schon etliche Betrugs- oder Erpressungsversuche. Oder denken wir an beleidigende Social-Media-Posts, bei denen die Polizei eigentlich handeln müsste. Das heißt, im Netz funktioniert die Präventivwirkung des Nichtwissens nicht so gut wie im physischen Raum. Eben weil im digitalen Raum Kriminalität und Straflosigkeit allgegenwärtig sind.

Das klingt fatal.

Das ist es auch. Die Folge ist, dass viele Menschen das Internet als rechtsfreien Raum ansehen – ich spreche von einem Broken-Web-Phänomen.

”

Die Wahrscheinlichkeit, dass Straftaten verfolgt werden, ist im Netz exorbitant niedriger als im physischen Raum, sodass es einem strafverfolgungsfreien Raum gleicht. Dieses Problem ist eine Jahrhundertaufgabe.

Und ist es faktisch ein rechtsfreier Raum?

Nun, förmlich gilt das Strafrecht. Aber das Netz wirkt eben auf die meisten Menschen wie ein Raum, in dem Straftaten nicht verfolgt werden. Auch in diesem Zusammenhang ein Beispiel: Die Bundeswehr hat bereits 2015 – neuere Zahlen gibt es kaum – bekannt gegeben, dass sie zu diesem Zeitpunkt 71 Millionen Angriffe über das Internet auf ihre kritische Infrastruktur registriert hat. Hätte die Bundeswehr nur 10 % davon angezeigt, wären das mehr gewesen als alle Delikte der Kriminalstatistik in

Deutschland zusammengefasst. Die Wahrscheinlichkeit, dass Straftaten verfolgt werden, ist im Netz exorbitant niedriger als im physischen Raum, sodass es einem strafverfolgungsfreien Raum gleicht. Und das führt zum Gefühl eines rechtsfreien Raums. Dieses Problem zu lösen, ist eine Jahrhundertaufgabe.

Was schlagen Sie vor, um das Problem in den Griff zu bekommen?

Einer Studie zufolge war im Jahr 2017 lediglich 1 % der Polizeiangehörigen in Deutschland für Polizeiarbeit im Internet zuständig. Das ist viel zu wenig, wenn man bedenkt, dass die Menschen heute mehr Zeit im Internet verbringen als im Straßenverkehr, dass also die Kriminalität im digitalen Raum viel größer ist als im physischen Raum! Wir brauchen dringend einen Plan, welche Rolle die Polizei künftig im grenzenlosen Internet spielen soll. Ein Anfang könnte bereits darin liegen, die aufgrund des Rückgangs der Kriminalstatistiken freigesetzten Personalressourcen ins Netz zu verlagern.

Nationales, also „begrenzt“ Strafrecht wirkt angesichts der Globalität des Internets ziemlich unzeitgemäß.

Das ist es auch. Angenommen, ein deutschsprachiger Australier begeht bei Twitter eine Volksverhetzung. Daraufhin beleidigt ein deutschsprachiger Kanadier den Australier übel. Der Server, über den die strafrechtlich relevanten Äußerungen geschehen, steht zum Beispiel in Irland. Ein deutscher Polizeiaccount registriert dies und sieht sich durch das Legalitätsprinzip zum Handeln gezwungen. Nur welches Strafrecht soll da überhaupt gelten?

Antworten Sie.

Wir wissen nicht, wie nationale Polizeigesetze, die ja eine örtlich fixierbare Zuständigkeit erfordern, angesichts der globalen Vernetzung im digitalen Raum funktionieren sollen. Es gibt keine wahrnehmbaren und fixierbaren Grenzen im Internet, übrigens auch keine sprachlichen. Auch hierfür noch ein Beispiel: Viele Sexualstraftäter missbrauchen über das Internet Kinder, die gar nicht ihre Sprache sprechen. Das ist mit automatisierten Übersetzungsprogrammen überhaupt kein Problem. Bald wird wahrscheinlich jedes gesprochene und geschriebene Wort automatisch in die jeweilige Landessprache übersetzt.

Wie ließe sich dem beikommen?

Es ist vermutlich utopisch, aber meiner Ansicht nach brauchen wir ein globales Minimalstrafrecht. Vermutlich wird es zunächst ein digitales Strafrecht für den deutschsprachigen Raum und dann für Europa geben. Aber im Grundsatz kann das nur global funktionieren. Denn es geht ja noch über das Internet hinaus.

Was meinen Sie?

Es gab schon den ersten Kriminalfall im Weltraum. 2019 hat die US-Astronautin Anne McClain auf das Bankkonto ihrer Ex-Partnerin zugegriffen. Aus dem All in der Weltraumstation ISS und vom Netzwerk der US-Raumfahrtbehörde NASA aus! Welches Strafrecht soll denn im Weltall oder auf dem Mars, wenn von dort über das Internet kriminelle Handlungen begangen werden, gelten? Ich denke, die Antwort kann nur in einem gemeinsamen, globalen Strafrecht und einer gemeinsamen Polizeiarbeit liegen.

Vielen Dank für das Gespräch.



Dr. Thomas-Gabriel Rüdiger, geboren in Gera, hat ein Studium zum Diplomverwaltungswirt an der Fachhochschule der Polizei in Brandenburg abgeschlossen, einen Master of Arts in Kriminologie an der Universität Hamburg erworben und an der juristischen Fakultät der Universität Potsdam über Cybergrooming (onlinebasierte Anbahnung des sexuellen Missbrauchs von Kindern) promoviert. Bis 2012 arbeitete er im brandenburgischen Innenministerium, danach bis 2016 an der Fachhochschule der Polizei des Landes Brandenburg und seither als Akademischer Rat am Institut für Polizeiwissenschaft der Hochschule der Polizei des Landes Brandenburg. Seine Forschungsschwerpunkte sind Cyberkriminologie und digitale Polizeiarbeit.

Dr. Thomas-Gabriel Rüdiger

Cyberkriminologe am Institut für Polizeiwissenschaft
an der Hochschule der Polizei des Landes Brandenburg



„Mir geht es um Digital Natives versus digital-naiv.“



Dr. Roman Povalej, „Cybercrime-Professor“ an der Polizeiakademie Niedersachsen, über Defizite vieler Polizeianwärter schon beim digitalen Basiswissen, Kompetenzvermittlung unter Zeitmangel und die Wirtschaft als Partner in der Polizeiausbildung

PwC/Strategy&: Herr Povalej, Sie sind Cybercrime-Experte bei der Polizei. Davon gibt es nicht so viele. Sehen Sie sich als Exoten?

Dr. Roman Povalej: Ja und nein. Einerseits gibt es mittlerweile etliche Cybercrime-Experten bei der Polizei. Als „Cybercrime-Professor“ an der Polizeiakademie Niedersachsen bin ich aber sicherlich ein Exot, weil es bundesweit nur wenige solcher Professuren bei der Polizei gibt.

Gemessen an der Relevanz des digitalen Raums für Kriminelle und an der Anzahl der Straftaten im Netz ist die Polizei dort zu wenig präsent. Braucht die Polizei mehr Cybercrime-Experten mit Ihren Kompetenzen – Experten, die allerdings auch ermitteln?

Unbedingt. Und da die digitalen Ressourcen in den eigenen Reihen nicht ausreichen, treibt die Polizei das Thema auch mit externer Unterstützung voran. Ich selbst bin Quereinsteiger bei der Polizei, bin vor fünf Jahren aus der Privatwirtschaft zur Polizei gekommen.

Und wie hat der Wechsel funktioniert?

Gut. Zwar habe ich die „Polizei-DNA“ immer noch nicht so verinnerlicht, wie es bei Kolleginnen und Kollegen der Fall ist, die ihre berufliche Laufbahn bei der Polizei begonnen haben. Dafür schaue ich viele Fragestellungen unbefangener vom klassischen Polizeihandwerk, das heißt vor allem aus der IT-Perspektive, an. Die Kombination beider Fähigkeiten bringt neue Ermittlungsansätze, um Kriminellen im digitalen Raum besser auf die Spur zu kommen. Dafür sensibilisiere ich an der Polizeiakademie immer wieder.

Um welche Cybercrime-Themen geht es in Ihren Seminaren?

Zunächst sehr viel um Basisinformationen. Zum Beispiel darum, was digitale Spuren sind, wo man sie findet und wie man sie sichert. Nur wenn Polizistinnen und Polizisten von Beginn an richtig handeln, kommen Sie an digitale Informationen heran.

Wo beginnt „von Beginn an“?

Angenommen, polizeiliche Ermittler klingeln für eine unangemeldete Hausdurchsuchung bei einer verdächtigen Person, die dann öffnet: Die Polizisten müssen sofort dafür sorgen, dass laufende elektronische Geräte wie Laptops oder Smartphones nicht in den Energiesparmodus schalten. Würde dies passieren, lägen die Geräte in der Regel unter einem Passwortschutz und die Polizei käme zunächst nicht – oder niemals – an mögliche Beweisdaten heran.

”

Wir haben viel zu wenig Zeit für die digitale Qualifizierung.

Nach tiefer Cybercrime-Expertise klingt das aber nicht.

Es wirkt vielleicht banal, wenn man sich vorstellt, dass ein Polizist am Schreibtisch des Verdächtigen steht und solange die Maus bewegt, bis jemand von der Datenverarbeitungsgruppe da ist, um die Geräte auszulesen. Aber im digitalen Raum sind scheinbar banale Tätigkeiten für die Ermittlungsarbeit genauso relevant wie im physischen Raum. Davon gibt es sehr viele – und für jedes Detail, an das Polizisten zu denken haben, müssen sie unter anderem technologische Hintergründe und Zusammenhänge kennen. Und dort wird es dann kompliziert. Angesichts dessen haben wir viel zu wenig Zeit für die digitale Qualifizierung. Zumal wir bei der Polizei häufig auch bei der Vermittlung von Digitalkompetenz noch ganz am Anfang stehen.

Warum sind Sie eigentlich in die Polizeiausbildung gegangen? In der Privatwirtschaft würden Sie doch bestimmt mehr Geld verdienen.

Bereits während meines Physikstudiums hat mich die angewandte Informatik dermaßen begeistert, dass ich nach meinem Studium zunächst als EDV-Berater und IT-Entwickler gearbeitet habe. Dann ging ich für die Promotion zurück an die Universität. Während meiner Tätigkeit in der Wirtschaft fiel mir die Ausschreibung der Polizeiakademie Niedersachsen auf, die einen IT- und Cybercrime-Spezialisten suchte. Das war vor fünf Jahren die erste Professur für diesen Fachbereich in Niedersachsen. Die wollte ich unbedingt haben.

Sollten in der Polizeiaus- und -fortbildung mehr Quereinsteiger wie Sie oder sogar externe Referenten arbeiten?

Ich fände das gut, weil die Polizei ihre Defizite in Sachen Digitalkompetenz dann schneller wettmachen könnte. Ein paar mehr Quereinsteiger als mich gibt es ja bereits.

”

Ich fände Praktika, Hospitationen und andere Fortbildungsformate außerhalb des Polizeiapparates horizonterweiternd für Polizistinnen und Polizisten.

Welche Rolle spielen Praktika bei der Polizeiausbildung, um digitale Kompetenzen zu verbessern? Und können diese auch in der Wirtschaft stattfinden?

Praktika gibt es vor allem in Polizeibehörden. Ich fände Praktika, Hospitationen und andere Fortbildungsformate außerhalb des Polizeiapparates horizonterweiternd für Polizistinnen und Polizisten. Die Polizei Niedersachsen hat bereits eine Reihe von sehr gut qualifizierten Ermittlerinnen und Ermittlern im Deliktfeld Cybercrime – aber es sollten dringend noch mehr sein.

Sie lernen an der Polizeiakademie sehr viele junge Leute kennen. Wie viele von ihnen wollen Cyberprofis werden?

Sagen wir so: Primär wollen sie Polizistinnen und Polizisten werden. Und wir sensibilisieren sie dafür, dass IT-Kenntnisse und der bewusste Umgang mit Technologie für ihre Arbeit immer wichtiger werden. Cybercrime müsste bei der Rekrutierung und Ausbildung viel stärker in den Fokus rücken.

Und geht das voran?

Langsam geht es da voran. Für das aktuelle Curriculum an der Polizeiakademie Niedersachsen wurde zum Beispiel die Stundenzahl für das Themengebiet „Digitale Spuren und Cybercrime“ erhöht. Das reicht aber noch nicht. Allerdings ist die Zahl der Lehrveranstaltungsstunden im Studium endlich. Die juristischen, sozialwissenschaftlichen, einsatztaktischen und organisatorischen Inhalte bleiben ja ebenfalls wichtig. Hinzu kommt eine grundsätzliche Problematik im bewussten Umgang mit neuen Technologien.

Welche?

Mir geht es um Digital Natives versus digital-naiv. Die meisten Polizeianwärter haben sich noch nie tiefer mit neuen Technologien befasst, weil die Endgeräte heutzutage sehr einfach funktionieren. Kein Nutzer muss sich noch mit der Funktionsweise auseinandersetzen. Das ist schlecht, weil deshalb eine große Naivität darüber herrscht, was hinter den Technologien steckt und wer sie wie missbrauchen kann.

Fängt das nicht schon damit an, dass die meisten Polizistinnen und Polizisten ihre privaten Smartphones im Dienst bei sich tragen und damit ebenfalls digitale Spuren hinterlassen, die Tatspuren verändern oder überdecken können?

Das ist den Kolleginnen und Kollegen häufig gar nicht bewusst. Wir müssen unseren Polizeiangehörigen viel mehr über den sicheren Umgang mit Informationssystemen, über die Funktionsweise und den Einfluss von sozialen Medien sowie über gerichtlich verwertbare digitale Ermittlungsstrategien vermitteln.

Ist die Aus- und Weiterbildung für mehr Digitalkompetenz vor allem ein Thema für jüngere Polizeiangehörige – oder auch für ältere?

Ganz klar auch für die älteren Kolleginnen und Kollegen. Wenn ein Polizist heute 50 Jahre alt ist, hat er schließlich noch mindestens zehn Dienstjahre vor sich. Und der technologische Wandel verläuft ja rasant. Viele ältere Polizeiangehörige, die eine gewisse IT-Affinität haben, beherrschen digitale Themen übrigens besser als ihre jüngeren Kolleginnen und Kollegen. Wir sollten die „Alten“ nicht unterschätzen.

”

Wenn die Polizei klug digitalisiert, kann sie dadurch menschliche Ressourcen für die Kriminalitätsbekämpfung im digitalen Raum gewinnen.

Viele Arbeitnehmer in der Privatwirtschaft fürchten, dass die Digitalisierung über kurz oder lang Arbeitsplätze kosten wird. Wie sehen Sie diese Sorge mit Blick auf die Polizei?

Ich erwarte das Gegenteil: nämlich, dass die Digitalisierung neue Stellen bei der Polizei bringen wird. Denn die Kriminalität im digitalen Raum nimmt bei einer vermutlich hohen Dunkelziffer zu! Es wird ja nur ein Bruchteil der tatsächlichen und vermuteten Rechtsverstöße angezeigt. Wenn die Polizei ihre Strukturen und Methoden klug digitalisiert, kann sie dadurch menschliche Ressourcen für die Kriminalitätsbekämpfung im digitalen Raum gewinnen. Dafür müssen wir aber erst einmal deutlich mehr Technologie einsetzen und gleichzeitig die digitale Kompetenz auf- bzw. ausbauen.



Dann stiege auch die Zahl der IT-Experten bei der Polizei. Sehen Sie die Gefahr, dass viele von diesen Experten dann von der Privatwirtschaft abgeworben würden?

Selbstverständlich, wir haben ja einen freien Arbeitsmarkt. Gute Digitalexperten werden sich noch lange aussuchen können, für wen sie arbeiten. Die Polizei muss deshalb sehr darauf achten, ein attraktiver Arbeitgeber zu sein. Wechsel von Polizisten in die Privatwirtschaft sind allerdings auch eine Chance für eine bessere Kriminalitätsprävention und einen intensiveren Wissenstransfer in beide Richtungen.

Wissenstransfer ist auch das Ziel von bundesländer-übergreifender Polizeiarbeit. Wie funktioniert sie aus Ihrer Sicht?

Ich nehme ein großes Interesse wahr, gemeinsam etwas zu bewegen. Da läuft das Programm „Polizei 2020“. Außerdem gibt es beispielsweise eine Sicherheitskooperation der Landeskriminalämter von Nordrhein-Westfalen, Niedersachsen, Baden-Württemberg, Sachsen, Hessen und Rheinland-Pfalz sowie des deutschen Digitalverbands Bitkom. Über eine gemeinsame Plattform von Polizei und Digitalwirtschaft tauschen sie Wissen und technische Kompetenzen aus und verfolgen einen ganzheitlichen Ansatz zur Prävention und Bekämpfung von Cyberkriminalität. Es gibt noch mehr solcher Initiativen und es müssen noch viel mehr werden.

Vielen Dank für das Gespräch.



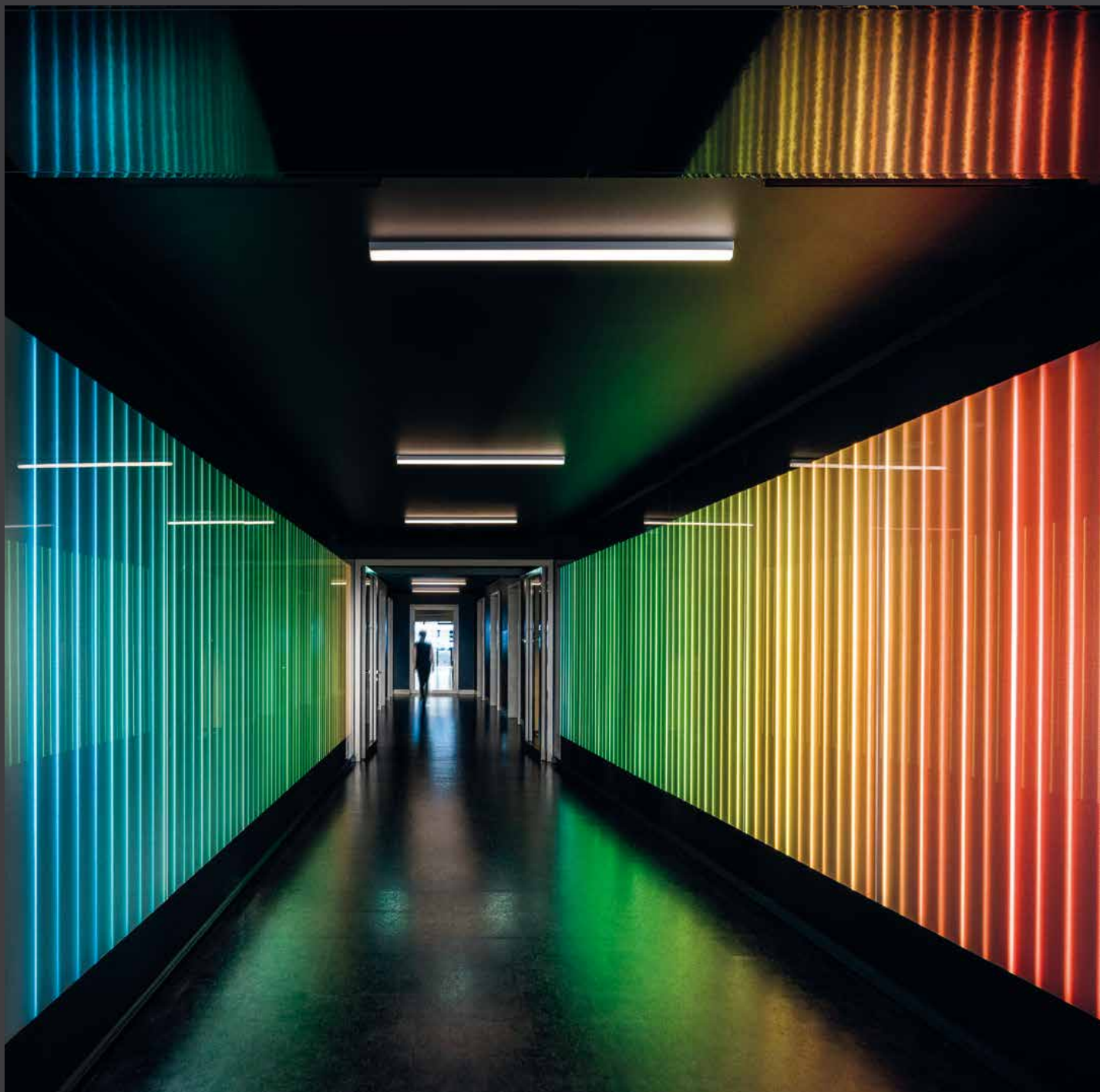
Dr. Roman Povalej, geboren am 22. Februar 1972 in Mosbach (Baden), studierte Physik in Heidelberg. Danach arbeitete er als EDV-Berater und Anwendungsentwickler in der Privatwirtschaft, ehe er am Karlsruher Institut für Technologie (KIT) zum Thema Skill-Meta-Frameworks und Wissensinformationssysteme in KMU promovierte. Im Jahr 2015 nahm er den Ruf als Professor für Informations- und Kommunikationstechnik und Cybercrime an der Polizeiakademie Niedersachsen an. Dr. Roman Povalej ist neben seinen Dozenten- und Forschungsaufgaben in mehreren Gremien aktiv und seit 2016 ständiges Mitglied der Expertengruppe Cybercrime an der Polizeihochschule Rheinland-Pfalz.

Dr. Roman Povalej

Professor für Informations- und Kommunikationstechnik und Cybercrime an der Polizeiakademie Niedersachsen



D Thought Leadership by PwC/Strategy&



Wenn es um sensible und komplexe Fragestellungen in Bereichen der öffentlichen Sicherheit geht, gibt PwC seit vielen Jahren nachhaltig wirksame Antworten. Wir stehen für „Strategy through Execution“ und bieten fundierte Beratung mit Umsetzungskompetenz für Entscheider der öffentlichen Hand. Zusammen mit unserer Inhouse-Strategieberatung PwC Strategy& und unserer Cybersecurity-Beratung liefern wir wegweisende Antworten für die Herausforderungen der Digitalisierung.

Hier bekommen Sie einen schnellen Überblick über unser Beratungsspektrum mit Schwerpunkt auf öffentlicher Sicherheit. Unsere Kunden sind Sicherheitsbehörden auf allen Verwaltungsebenen. Mit unserem globalen PwC Defense and Security Network verfügen wir über Einblicke in Modernisierungsvorhaben weltweit.

Wir möchten dazu beitragen, dass Sie Ihre Herausforderungen mit modernen, effizienten und messbar erfolgreichen Lösungen meistern. Sind Sie interessiert an Referenzprojekten? Dann kontaktieren Sie uns bitte. Wir freuen uns auf Sie!

Das Beratungsspektrum von PwC/Strategy& für verlässlich hohe innere Sicherheit:

- Digitalisierung zeitgemäß umsetzen und von den Nutzerinnen und Nutzern her denken
- Strategieprojekte entwickeln und moderieren
- Digitalisierungs- und IT-Projekte zuverlässig planen und deren Steuerung unterstützen
- Organisationen und Prozesse analysieren und verbessern
- Verwaltungsdigitalisierung unterstützen und evaluieren
- Personalbedarfe ermitteln und zeitgemäßes Ressourcenmanagement aufsetzen
- Kompetenzmodelle für das digitale Zeitalter entwickeln und in der Aus-, Fort- und Weiterbildung umsetzen
- Kulturwandel in Behörden ermöglichen
- effektives Finanzcontrolling etablieren
- Vergaben rechtssicher begleiten
- Cybersicherheit prüfen und erhöhen
- Datenschutz und IT-Sicherheit evaluieren und sichern
- mit moderner Technologie Betrugsfälle verhindern und aufdecken





Ihre Ansprechpartner

3 von 12.000 klugen Köpfen

Ihre Ansprechpartner für den Bereich Public Sector bei PwC/Strategy& und diese Veröffentlichung sind:



Prof. Dr. Rainer Bernnat

Senior Partner und Industry Leader Public Sector,
PwC/Strategy& Deutschland

Prof. Dr. Bernnat verfügt über mehr als 28 Jahre Beratungserfahrung. Er leitet für PwC/Strategy& den Bereich Öffentlicher Sektor mit über 1.100 Mitarbeiterinnen und Mitarbeitern. Seine Tätigkeitsschwerpunkte liegen im gesamten Spektrum der strategischen Neuausrichtung und technologiegetriebenen Transformationsprogramme öffentlicher Institutionen.

Das Autorenteam



Dr. Wolfgang Zink

Partner Public Sector Consulting, PwC Deutschland

Dr. Wolfgang Zink hat mehr als 20 Jahre Beratungserfahrung im deutschen und internationalen öffentlichen Sektor. Er hat an der französischen Verwaltungshochschule Ecole Nationale d'Administration (ENA) studiert und in Freiburg zu E-Government promoviert. Seine Beratungsschwerpunkte umfassen die gesamte Bandbreite von der Strategieentwicklung über die Reorganisation bis hin zum (IT-)Projektmanagement für öffentliche Klienten, darunter große Sicherheitsbehörden des Bundes und der Länder.



Kerstin Zimmermann

Manager Public Sector Consulting, PwC Deutschland

Kerstin Zimmermann ist seit mehr als zwölf Jahren im öffentlichen Sektor tätig. Sie hat an der Universität der Bundeswehr in Hamburg Betriebswirtschaftslehre studiert. Nach ihrer Laufbahn als Marineoffizier und Tätigkeiten bei anderen Beratungsunternehmen unterstützt sie für PwC/Strategy& Klienten aus der äußeren und inneren Sicherheit bei wichtigen Modernisierungsaufgaben.



Über uns

PwC/Strategy& versteht es als seine Aufgabe, wichtige gesellschaftliche Herausforderungen zu meistern und dadurch gesellschaftliches Vertrauen aufzubauen. Mehr als 250.000 Mitarbeiterinnen und Mitarbeiter in 158 Ländern tragen dazu bei: mit hochwertigen, branchenspezifischen Dienstleistungen in den Bereichen Wirtschaftsprüfung, Steuer-, Rechts- und Unternehmensberatung. Allein in Deutschland widmet sich diesen Aufgaben ein Team mit mehr als 12.000 klugen Köpfen. Ihr Altersdurchschnitt beträgt derzeit 36 Jahre; 45 Prozent unserer Beschäftigten sind Frauen.

Öffentliche Akzeptanz digitaler Technologien bei der deutschen Polizei

Herausgegeben von der PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft

Von Dr. Wolfgang Zink, Kerstin Zimmermann und Interviewer Mario Müller-Dofel

Dezember 2020, 64 Seiten, 15 Abbildungen, Softcover

Alle Rechte vorbehalten. Vervielfältigungen, Mikroverfilmung, die Einspeicherung und Verarbeitung in elektronischen Medien sind ohne Zustimmung des Herausgebers nicht gestattet.

Die Inhalte dieser Publikation sind zur Information unserer Mandanten bestimmt. Sie entsprechen dem Kenntnisstand der Autoren zum Zeitpunkt der Veröffentlichung. Für die Lösung einschlägiger Probleme greifen Sie bitte auf die in der Publikation angegebenen Quellen zurück oder wenden sich an die genannten Ansprechpartner. Meinungsbeiträge geben die Auffassung der einzelnen Autoren wieder. In den Grafiken kann es zu Rundungsdifferenzen kommen.

Bildnachweise

Seite 1 Getty Images/fhm, Seite 2 Getty Images/Westend61, Seite 10 Getty Images/Maremagnum, Seite 14 picture alliance/dpa/Michael Kappeler, Seite 16 picture alliance/Flashpic/Jens Krick, Seite 18 Getty Images/southerlycourse, Seite 26 Getty Images/Tashi-Delek, Seite 35 Getty Images/Virojt Changyenham, Seite 44 Getty Images/gorodenkoff, Seite 53 Getty Images/Laurence Dutton, Seite 56/57 picture alliance/Sven Simon/Malte Ossowski und Seite 58 PwC.

