Ralf Michelfelder
Präsident Landeskriminalamt Baden-Württemberg a. D.
07.06.2021

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)863 D

Einleitung

Nachstehende Ausführungen entstanden anlässlich der

Anhörung des Innenausschusses des Deutschen Bundestags zum Antrag der Abgeordneten Benjamin Strasser u.a. und der Fraktion der FDP „Smart Police – Digitalisierung der deutschen Polizei anschieben“, BT-Drucksache 19/27172.

Die dargestellten Rahmenbedingungen und Handlungsfelder sollen lediglich exemplarisch die aktuelle Situation widerspiegeln, ohne Anspruch auf Vollständigkeit.

1. Kriminalität im Wandel

Erscheinungsformen von Kriminalität stehen immer im gesellschaftlichen Kontext, der die Rahmenbedingungen zur Straftatenbegehung bildet. Das gilt sowohl für die Art der Begehung einer Straftat als auch für Erscheinungsformen von Kriminalität. Um es vereinfacht zu sagen: Es gibt keine Postkutschenüberfälle mehr, weil es keine Postkutschen mehr gibt. Gegenläufig verhält es sich mit der Digitalisierung unserer Gesellschaft. Polizei und Gesellschaft werden mit neuen Begehungsweisen traditioneller Kriminalität, aber auch mit völlig neuen Kriminalitätsformen konfrontiert. Steigende Angriffe auf IT-Systeme korrelieren mit deren Verbreitung. Das Internet of Things (IoT), die Internetanbindung von Maschinen und Anlagen im gewerblichen und privaten Bereich, wird zunehmend weitere neue Angriffsmöglichkeiten eröffnen. Die jüngsten Ransomware Attacken auf die US Colonial Pipeline und den größten Fleischproduzenten in Südamerika haben beispielhaft vor Augen geführt, welche erheblichen Auswirkungen solche Angriffe nicht nur für das betroffene Unternehmen, aber auch in der Gesellschaft haben können.

Das Risiko, Opfer einer Straftat zu werden, beginnt heute mit dem Einschalten des PC Zuhause oder der Inbetriebnahme des Smartphones. Die Verbindung mit dem Internet ist gleichbedeutend mit dem Risiko eines bösartigen Angriffs. Zu den tradierten Parametern Opfer einer Straftat zu werden, wie Alter, soziales Umfeld, Wohngebiet etc. ist der Internetanschluss hinzugekommen. Deutlich zeigt sich dies in der Langzeitentwicklung der Kriminalität in Deutschland. Während die Straftaten insgesamt seit Jahren zurückgehen, steigt die Begehung von Straftaten mittels IT-Systemen und über das Internet rapide an, beispielsweise in Baden-Württemberg mit Steigerungsraten von jährlich über 20 Prozent in den vergangenen Jahren.[1]

[1] Sicherheitsbericht 2020 des Landes Baden-Württemberg; https://im.baden-wuerttemberg.de/fileadmin/redaktion/m-im/intern/dateien/publikationen/20210219_Sicherheitsbericht_Baden_Wuerttemberg_2020.pdf

2. Gesellschaft im Wandel

Auch unsere Sozialstruktur ist einem stetigen Wandel unterworfen. Aktuell nimmt in Deutschland die Internationalisierung der Gesellschaft zu, bis hin zu Subkulturen mit Bildung eigener Werte und Normen und dem sich Entziehen staatlicher Kontrolle. Die gesellschaftliche und wirtschaftliche Internationalisierung fördert die Bildung staatenübergreifender krimineller Netzwerke. Erfolgreiche, effiziente Polizeiarbeit muss daher reibungslos länder- und staatenübergreifend sein.

Technologischer Fortschritt hält Einzug in alle Lebensbereiche. Smarthome, Smartphone, digitale Kommunikation und Automatisierung sind alltägliche Begleiter geworden. Zirka 97,3 Prozent der 14- bis 19-jährigen Personen in Deutschland besitzen im Jahr 2020 ein Smartphone. In der Altersgruppe der 20- bis 29-Jährigen sind es 98,1 Prozent, bei den 30- bis 39-Jährigen 97,8 Prozent. Der Anteil der Smartphone-Besitzer bei den über 70-Jährigen beläuft sich immerhin noch auf 52,1 Prozent.[2] Ein Smartphone ist mehr als ein Telefon. Es ist ein Computer mit allen Office Funktionen, ein Foto mit hochauflösender Optik, eine Bank in der Hosentasche, ein Liebesbriefkasten und natürlich ein Telefon. Speichervolumen von 512 GB bis hin zu 1 TB erlauben es einem, sein ganzes Leben in der Hand oder Hosentasche zu tragen. Angesichts dieser Entwicklungen verwundert es nicht, wenn das Smartphone das einzige Internet-Gerät im Haushalt sein kann und für den Einzelnen unverzichtbar wird.

Parallel hierzu zeigt sich eine weltweite Entwicklung in der bürgerorientierten Polizeiarbeit, in welcher der Bürger zunehmend vom bloßen Konsumenten zum aktiven Teilnehmendem tendiert. Viele hochwertige Recherchetools sind online verfügbar und von jedermann nutzbar. Hohe Popularität erlangte beispielsweise bellingcat.com mit dem auf eigenen Recherchen gestützten Nachweis des Abschusses der Passagiermaschine MH-17 in der Ostukraine. Besonders interessant hierbei ist, dass sich die „Ermittler“ von bellingcat.com online staatenübergreifend vernetzten. Jede(r) bringt in dieser „internationalen Ermittlungsgruppe“ seine Kompetenz ein. So ist sich bellingcat.com sicher, den Nachweis zu führen, dass der Beschuldigte im Berliner Mordprozess z. N. des georgischen Asylbewerbers Z.K. tatsächlich eine andere Identität besitzt als die, mit der gegen ihn aktuell verhandelt wird – mit Bezügen zu staatlichen russischen Stellen.[3] Polizeiarbeit gerät in eine zunehmend kritische Wahrnehmung und Kontrolle, in der sowohl die Art des Einschreitens als auch das Ergebnis nachgeprüft und nachprüfbar werden.

Sinkende Hemmschwellen zur Gewaltanwendung gegenüber Einsatz- und Rettungskräften, Mobilisierung großer Menschenmengen zu Protestveranstaltungen, Auswirkungen ausländischer Ereignisse auf das Demonstrationsgeschehen in Deutschland, Großveranstaltungen etc. erfordern vielfach länderübergreifende Unterstützungseinsätze der Sicherheitsbehörden der Länder und des Bundes. Gleichermaßen kooperieren die Polizeien entweder auf regelmäßiger Basis (z. B. Gemeinsame Ermittlungsgruppen Rauschgift oder Schleuser) oder in anlassbezogenen Ermittlungsgruppen. Um reisende Täter

[2] https://de.statista.com/statistik/daten/studie/459963/umfrage/anteil-der-smartphone-nutzer-in-deutschland-nach-altersgruppe/
[3] https://www.bellingcat.com/news/2021/03/19/berlin-assassination-new-evidence-on-suspected-fsb-hitman-passed-to-german-investigators/

erfolgreiche ermitteln zu können, müssen Tatzusammenhänge und Erkenntnisse in einzelnen Bundesländern zeitnah und umfassend zusammengefasst und der Sachbearbeitung zugänglich gemacht werden.

3. Auswirkungen auf den polizeilichen Alltag

Die gesellschaftliche Durchdringung der Digitalisierung hat mittlerweile alle Lebens- und Arbeitsbereiche erreicht. Für die Polizei ergibt sich dementsprechend die Herausforderung, mit dieser Entwicklung Schritt zu halten, um auch zukünftig weiterhin erfolgreich Gefahren abwehren und Straftaten verfolgen zu können. Dabei bestimmt nicht die Polizei das Tempo der Transformation, sondern muss selbst diesem folgen.

Erfolgreiche Polizeiarbeit heute und noch mehr in der Zukunft hängt wesentlich von der IT-Kompetenz und IT-Ausstattung der Polizei ab. Es muss also in erster Linie darum gehen, die Polizeibediensteten in der Digitalisierung zu befähigen. Dazu zählt sowohl die Kenntnis über die IT-basierten Ermittlungsmöglichkeiten, aber gleichermaßen auch die Sensibilität, an einem polizeilichen Sachverhalt das Potenzial für digitale Ermittlungsschritte zu erkennen. Digitale Spuren dominieren die polizeiliche Arbeit. Es gibt heute keinen Tatort mehr, an dem nicht digitale Spuren anfallen. Zur herkömmlichen haptischen, analogen Tatortarbeit ist die digitale hinzugekommen. Beispiele:

- Kamen früher Schraubendreher oder Brecheisen zum Einsatz, um eine Haus- oder Autotür zu öffnen, so kann dies heute über die Überwindung IT-basierter Schließsysteme erfolgt sein.
- Es gibt keine Durchsuchung, bei der nicht auch digitale Spurenträger zur Auswertung anfallen. Sei es ein Handy, ein USB-Stick, eine mobile Festplatte, ein Laptop oder ein PC. Oder alles zusammen.
- Automobile sind längst mit der viel diskutierten „Blackbox“ ausgestattet. Viele Steuergeräte speichern für Ermittlungen relevante Informationen.
- Behördliche und private Kamera, Handyvideos etc. liefern wichtige Hinweise zur Täteridentifizierung. Das bayrische Landeskriminalamt hat im Jahr 2020 insgesamt 649 Tatverdächtige über ein digitales Gesichtserkennungsprogramm identifiziert. 2013 identifizierte das bayrische Landeskriminalamt im gesamten Jahr lediglich 45 Tatverdächtige über Gesichtserkennung. [4]
- Teilautonome Videoüberwachungssysteme wie in Mannheim[5] können tatkritische Situationen erkennen und das Bild erst dann zur Verifizierung freischalten. Dies entlastet den Beobachter und stärkt den Datenschutz.
- Angesichts von Millionen ge- oder verfälschter Ausweisdokumente in der EU kann künstliche Intelligenz dazu beitragen, Fälschungsmerkmale sicher zu erkennen und darauf basierende teilautomatisierte Gutachten erstellen.

[4] Schwäbisches Tagblatt, 05.06.2021, Verbrechen auf der Spur.
[5] https://www.mannheimer-morgen.de/themen-schwerpunkte_dossier,-videoueberwachung-in-mannheim-_dossierid,118.html

Zwangsläufig noch deutlicher wird der Bedarf bei der Bekämpfung der größtenteils ausschließlich digitalen Cyberkriminalität. Um hier erfolgreich ermitteln zu können, bedarf es Experten ihres Fachs, die neben der eigentlichen Ermittlungsarbeit auch einen hohen Fortbildungsbedarf haben, um mit den Tätern Schritt halten zu können.

Alle vorstehend genannten Beispiele haben gemein, dass bei der Sicherung digitaler Spuren Unmengen an Daten anfallen, die der Aufbereitung und Auswertung bedürfen. Durchsuchungsmaßnahmen mit der Sicherung von Datenträgern im Gigabyte-Umfang sind längst üblich und werden mittlerweile von Terrabyte-Festplatten, SD-Karten und USB-Sticks verdrängt. In einem Ermittlungsverfahren des Landeskriminalamts Baden-Württemberg wurde eine Datenmenge von 1,2 Petabyte gesichert. 1 Petabyte an Text bedeutet ausgedruckt einen DIN-A4 Papierstapel mit 50.000 km Höhe. Händisches durchblättern ist hier nicht mehr drin. Ein deutscher Autohersteller hat für die Forschungsbereich autonomes Verfahren einen Datenspeicher von über 240 Petabyte verfügbar. Das entspricht einer 80 qm Wohnung mit 3 Meter Raumhöhe, vollgestopft mit CDs. Parallel zur Vergrößerung des Speichervolumens von Datenträgern werden immer mehr Daten in der Cloud abgelegt. Für die Sicherheitsbehörden ergeben sich hierdurch Herausforderungen, die bereits bei der Sicherung und Übertragung der Daten beginnen, mit deren Aufbereitung fortschreiten, bis hin zu deren Auswertung.

Bei länderübergreifenden Ermittlungsverfahren müssen ggf. diese Datenmengen in gemeinsamen Systemen zusammengeführt und erneut auf Übereinstimmungen und ergänzende Informationen analysiert werden. Zuvor bedarf es oftmals erheblicher Anstrengungen für deren Aufbereitung.

Smart Cities[6] können im Verbund mit der Polizei zu einem sicheren Leben beitragen und die Aufgabenerledigung der Polizei effizienter gestalten, wenn die Systeme miteinander kommunizieren können.

4. Polizei 2020

In ihrer Herbstkonferenz am 30.11.2016 hatten die Innenminister und Senatoren von Bund und Ländern in Saarbrücken die Schaffung einer gemeinsamen, modernen und einheitlichen Informationsarchitektur der Polizei beschlossen. Ziel ist, dass alle relevanten Informationen in einem fachlichen, technischen und organisatorischen Gesamtsystem für die Polizeien in Bund und Ländern nutzbar sind. Künftig soll beispielsweise jeder Polizeibeamte jederzeit und überall über die für ihn relevanten Informationen verfügen können. Polizeiliche IT-Angebote, die Bund und Länder betreffen, sollen nur einmal entwickelt und allen Nutzern in Bund und Ländern zur Verfügung gestellt werden. Dies verbunden mit technischen Lösungen zur Stärkung des Datenschutzes. Das auf diesem Beschluss fußende Bund-Länder Projekt trägt den Titel Polizei 2020 und steht unter der Leitung des Bundesministeriums des Innern.

[6] https://www.bmi.bund.de/DE/themen/bauen-wohnen/stadt-wohnen/stadtentwicklung/smart-cities/smart-cities-node.html

Wesentlicher Bestandteil der vorstehend genannten Grundsätze von Polizei 2020 ist die Philosophie, dass neue Anwendungen von einem oder mehreren entwickelt, aber allen zur Verfügung gestellt werden. Aktuell trägt diese Idee beispielsweise in der in Baden-Württemberg initiierten Entwicklung eines umfassenden Asservatenmanagementsystems Früchte, ebenso in einem bundesweit einheitlichen polizeilichen Fallbearbeitungssystems (eFBS), das vom Bund und dem Landeskriminalamt Baden-Württemberg als Vertreter der Länder umgesetzt wird. Das bayrische Landeskriminalamt hat die Federführung in der Beschaffung einer neuen Auswerte- und Analysesoftware für die Polizei.

Auf weitere Ausführungen hierzu verzichte ich, angesichts der vorgesehenen Anhörung von Experten zum strategisches Controlling Polizei 2020.

5. Handlungsbedarf – Digitalisierung anschieben

Weiteren Handlungsbedarf im Sinne des Antrags sehe ich in

- Entwicklungsprozesse beschleunigen
  Der vorstehend aufgeführte Ansatz von Polizei 2020 ist richtig und muss weiterverfolgt werden. Allerdings sind die derzeitigen Zeitläufe von der Bedarfsfestlegung bis zur Realisierung von oftmals fünf und mehr Jahren völlig inakzeptabel. Dabei verschlingen nicht Fragen der polizeitaktischen oder technischen Ausgestaltung, sondern das Vergabeverfahren einen Großteil der Zeit, oftmals über zwei Jahre. Bei IT-Anwendungen für die Polizei handelt es sich um Angelegenheiten der nationalen Sicherheit. Es müssen hier dringend Wege gefunden werden, um IT-Beschaffungen zu beschleunigen. Polizeiliche IT-Anwendungen sind Angelegenheiten der nationalen Sicherheit und bedürfen einer entsprechenden Priorisierung.

  Dazu gehört meines Erachtens auch das Bekenntnis, vorrangig Software von der Stange zu beschaffen, statt zeit- und kostenintensiver Maßschneiderei.

- Datenflut beherrschbar machen – Künstliche Intelligenz nutzen
  Die Polizei muss IT-Entwicklungen und deren Auswirkungen auf die polizeiliche Arbeit frühzeitig mit ihren Partnern, insbesondere den Staatsanwaltschaften abstimmen. Die exponentielle Zunahme an Daten birgt das Risiko einer für alle Beteiligten unverhältnismäßigen und unzumutbaren Auswertedauer. Niemand wäre in der analogen Welt beispielsweise auf die Idee gekommen, in einem Wirtschaftsstrafverfahren neben Umzugskartons voll mit Leitzordnern der Buchhaltung auch noch die Fotoalben des Chefs sicherzustellen und auszuwerten. Genau das aber passiert in der digitalen Welt. Es braucht daher Absprachen zwischen Staatsanwaltschaft, Ermittler und forensischer IT zum Umfang der Datenaufbereitung.

  Insbesondere bei Routineaufgaben kann künstliche Intelligenz wesentlich dazu beitragen, schnellere und personalschonende Ergebnisse zu erzielen. Diese Potenziale sind breiter nutzbar zu machen.

- Grundwissen und Expertenwissen vermitteln
  Erfolgreiche polizeiliche Digitalisierung beginnt an der polizeilichen Basis vor Ort. Was dort nicht festgestellt und gesichert wird kann auch nicht ausgewertet und weiterverarbeitet werden. Daher muss als Basiswissen gleichermaßen die Kenntnis zu den IT-Anwendungen vorhanden sein, als auch die Sensibilität für die Präsenz digitaler Spuren. Die polizeilichen Lehrpläne müssen entsprechend angepasst werden. Digitalisierung ist nicht nur eine Frage der technischen Ausstattung, sondern insbesondere auch ein Transformationsprozess für die Anwender.

  Über das Basiswissen hinaus muss IT-forensisches Expertenwissen verstärkt vermittelt werden. Spezielle Studiengänge für Cyberkriminalisten können polizeiintern, aber auch in Kooperation mit Externen angeboten werden. Für effiziente Datenanalyse braucht es in diesem Aufgabenfeld routinierte Spezialisten. Analysespitzen können über In-House Kooperation mit Fachfirmen abgedeckt werden. Externe Analyse und Auswertung sollte angesichts sensibler Daten vermieden werden.

- Die Rahmenbedingungen für performante Anwendungen schaffen
  Die Digitalisierung gewinnt dann Akzeptanz, wenn sich spürbare Vorteile für den Ermittler an der Basis zeigen. IT-Anwendungen müssen vor Ort schnell und zuverlässig zur Verfügung stehen mit einem akzeptablen Antwort-Zeitverhalten.

- Verlässliche Budgets für IT-Forensik
  Parallel zur exponentiellen Fortentwicklung der IT in Wirtschaft und Gesellschaft bedarf es einer ständigen Adaption der polizeilichen forensischen Anwendungen sowie der Speicherkapazitäten. Dies kann am sichersten über eigenständige Budgets realisiert werden.

- Zeitgemäße Ausstattung
  Die digitale Ausstattung muss Zentralstellen und Vor-Ort Dienststellen gleichermaßen umfassen. Wenn Bürgerinnen und Bürger primär ihr Smartphone in nahezu allen Lebensbereichen nutzen, muss die Polizei Möglichkeiten schaffen, darauf vorhandene Beweise (Fotos, Mails etc.) vor Ort forensisch zu sichern.

Gez.

Ralf Michelfelder