Neue Angriffsflächen

Polizeiliche Strategien für das digitale Zeitalter

HOLGER MÜNCH

Geboren 1961 in Bremen, 2009 bis 2011 Polizeipräsident von Bremen, 2011 bis 2014 Staatsrat beim Senator für Inneres und Sport der Freien Hansestadt Bremen, seit 2014 Präsident des Bundeskriminalamtes (BKA).

Die Kriminalität hat sich in den vergangenen Jahren und Jahrzehnten grundlegend verändert. Nationale Grenzen haben an Bedeutung verloren. Dadurch sind Straftäter mobiler geworden. Sie sind international vernetzt und agieren immer häufiger über Landesgrenzen hinweg. Durch die weltweit zunehmende digitale Vernetzung sind darüber hinaus neue Angriffsflächen und Möglichkeiten krimineller Taten entstanden, die Straftäter für ihre Zwecke zu nutzen wissen. Um Kriminalität weiterhin wirksam bekämpfen zu können, muss die Polizei mit dieser Dynamik Schritt halten. Das stellt sie in den Strukturen, wie sie bislang organisiert ist, zunehmend vor Probleme. Deshalb bedarf es neuer Ansätze polizeilicher Zusammenarbeit!

Eine der größten Herausforderungen für die Strafverfolgungsbehörden in Deutschland und weltweit ist nach wie vor der islamistische Terrorismus. Die Bedrohungslage wird unter anderem angesichts des Ausmaßes und der Dynamik des islamistischen Personenpotenzials deutlich: Wir zählen

derzeit mehr als 750 islamistische „Gefährder“ – Personen, von denen wir aufgrund verschiedener Erkenntnisse annehmen müssen, dass sie einen Anschlag ausführen oder sich an einem Anschlag beteiligen werden. Diese Zahl hat sich in den vergangenen fünf Jahren mehr als verfünffacht. Darüber hinaus sind über 970 Personen aus Deutschland nach Syrien und in den Irak ausgereist, um dort aufseiten des sogenannten Islamischen Staates (IS) oder anderer terroristischer Gruppierungen zu kämpfen oder sie in sonstiger Weise zu unterstützen.

Trotz der militärischen Zurückdrängung des IS in diesen Gebieten zeichnet sich bislang noch keine verstärkte Rückreisetendenz dieser Personen nach Deutschland ab. Man muss jedoch davon ausgehen, dass durch den gemeinsamen Aufenthalt Tausender Dschihadisten aus aller Welt in den Kampfgebieten im Nahen Osten internationale dschihadistische Netzwerke entstanden sind, die die Sicherheitsbehörden weltweit auf lange Sicht vor erhebliche Herausforderungen stellen werden. Über diverse Chaträume und Foren im Internet und speziell in den Sozialen Medien hat der IS darüber hinaus eine Art „virtuelles Kalifat“ geschaffen, das seine Anhänger untereinander vernetzt, radikalisiert und anschlagsbereite Personen bis zur Tatbegehung unterstützt und begleitet.

Deutschland und Europa stehen nach wie vor im Zielspektrum terroristischer Gruppierungen. Mit islamistisch motivierten Gewalttaten muss weiterhin gerechnet werden – sowohl mit mehr oder minder spontan begangenen Taten unter Nutzung von Alltagsgegenständen, wie Messern, Äxten und Fahrzeugen, als auch mit gezielten und koordinierten Anschlägen wie in Paris im November 2015 oder in Brüssel im März 2016, geplant und begangen von internationalen Netzwerken aus „homegrown terrorists“, „Dschihad-Rückkehrern“ und vom IS zu diesem Zweck entsandten Dschihadisten aus dem Nahen Osten.

KRIMINALITÄT IM CYBERRAUM

In anderen Kriminalitätsbereichen spielen international organisierte Täternetzwerke ebenfalls eine Rolle: Im Bereich der Organisierten Kriminalität (OK) weisen rund achtzig Prozent der Ermittlungsverfahren Bezüge zum Ausland auf. Wir haben weiterhin mit klassischen OK-Gruppierungen wie Rockern oder der Mafia zu tun. Darüber hinaus stellen wir ebenfalls bei Delikten wie Ladendiebstählen oder Wohnungseinbrüchen, die häufig als Klein- und Massenkriminalität wahrgenommen werden, zunehmend organisierte Strukturen fest, so zum Beispiel reisende Tätergruppierungen, überwiegend aus Osteuropa, die sich für einen bestimmten Zeitraum in Deutschland aufhalten, im Akkord Einbrüche begehen und sich schließlich mit der Beute wieder ins Ausland absetzen.

Gruppierungen der OK sind in sämtlichen Bereichen aktiv, in denen Profite zu erzielen sind – von Menschen-, Waffen- und Drogenhandel über Betrugsmaschen am Telefon bis hin zur Wirtschaftskriminalität. Die Aufdeckung ihrer hochkonspirativen Geschäftsmodelle erfordert intensive polizeiliche Ermittlungen, die ausschließlich durch eine Bündelung der Ressourcen und Kompetenzen aus Bund und Ländern sowie eine enge Abstimmung aller Akteure auf nationaler und internationaler Ebene erfolgreich zu bewältigen sind.

Ein weiteres Phänomen, das die Strafverfolgungsbehörden zunehmend beschäftigt, ist die Kriminalität im Cyberraum – Straftaten, die im beziehungsweise mittels des Internet begangen werden. Straftäter nutzen modernste digitale Technologien, eignen sich das Know-how entweder selbst an oder geben Straftaten in Auftrag. Dadurch verlagern sich klassische Deliktsbereiche zunehmend ins Internet; zudem entstehen neue Kriminalitätsphänomene. Straftaten reichen vom Diebstahl von Kreditkartendaten durch „Phishing“ oder digitale Erpressung mittels „Ransomware“ über Kinderpornographie im Internet bis hin zu Spionage, Sabotage und Angriffen auf Kritische Infrastrukturen. Wie weitreichend die Folgen von Cyberangriffen sein können, hat im vergangenen Jahr die „WannaCry“-Attacke verdeutlicht, von der Computersysteme in rund 150 Staaten betroffen waren und die in Großbritannien beispielsweise zahlreiche Krankenhäuser lahmlegte.

Für die polizeiliche Ermittlungsarbeit bedeutet die zunehmende Digitalisierung von Kriminalität, dass Spuren und Beweise häufiger im digitalen Raum anfallen und dort auch gesichert werden müssen.

GEMEINSAMES „DATENHAUS“

Derartigen internationalen und digitalen Kriminalitätsphänomenen kann die Polizei nicht in alleiniger Zuständigkeit eines einzelnen Staates oder eines einzelnen Bundeslandes begegnen. Auch die Strafverfolgungsbehörden in Deutschland und Europa müssen sich vernetzen und Strukturen schaffen, innerhalb derer sie effektiv und effizient zusammenarbeiten können.

Das betrifft zum einen den polizeilichen Informationsaustausch: Das Zusammenführen und Verarbeiten von Informationen ist die Grundlage jeglicher polizeilicher Ermittlungsarbeit. Deshalb muss gewährleistet sein, dass Daten zu Tätern, Taten und Tatmitteln an der richtigen Stelle und zum richtigen Zeitpunkt abrufbar sind – bundesweit wie auch in Europa.

In Deutschland ist dieser Datenaustausch bislang mit einigen bürokratischen und technischen Hürden und daher mit Qualitäts- und Effizienzeinbußen behaftet, die in Zeiten dynamischer Kriminalitätsentwicklung und mobiler Straftäter nicht länger hinnehmbar sind. Die deutsche Polizei schafft sich mit dem „Programm 2020“ daher nun ein neues Informationssystem, das auf Basis moderner Technologien und technischer Strukturen einen deutlich

schnelleren und effizienteren Datenaustausch ermöglicht: Statt verschiedenster unterschiedlicher Datentöpfe, die für neue Kriminalitätsphänomene jeweils neu geschaffen werden, sowie neunzehn unterschiedlicher Teilnehmersysteme der Polizeien im Bund und in den Ländern werden wir künftig ein gemeinsames „Datenhaus“ haben, in dem Daten in kürzester Zeit miteinander geteilt werden können; durch das Setzen eines „Häkchens“, anstatt sie wie bislang aufwendig und langwierig von einem System in ein anderes transferieren zu müssen. Genauso einfach können Berechtigungen zur Dateneinsicht auch widerrufen werden – das neue System ermöglicht somit neben allen anderen Vorteilen auch einen wesentlich effektiveren Datenschutz!

ZUGRIFF AUF MILLIONEN FAHNDUNGSDATEN

Auch auf europäischer Ebene geht es voran: In unserem zentralen europäischen Fahndungssystem, dem Schengener Informationssystem (SIS), können Polizeibeamte aus dreißig Staaten auf derzeit rund 77 Millionen Fahndungsdaten zugreifen. Anders als im deutschen Fahndungssystem können im SIS allerdings Fingerabdrücke bislang nicht automatisiert abgefragt werden. Das bedeutet: Wenn ein Straftäter Alias-Personalien nutzt oder unterschiedliche Schreibweisen eines Namens bestehen, werden im System keine Treffer erzielt. Diese Fälle sind nicht selten: Bei einem Abgleich des SIS mit dem deutschen Fingerabdruckbestand trat zutage, dass sich bei mehr als der Hälfte der Personen, die in beiden Systemen gespeichert sind, die hinterlegten Personalien unterscheiden – das heißt, bei einer üblichen Personenüberprüfung und erkennungsdienstlichen Behandlung hätte die Fahndung im SIS nicht festgestellt werden können! Daher hat sich das Bundeskriminalamt stets dafür eingesetzt, dass auch im Schengener Informationssystem die Voraussetzungen für eine automatisierte Recherche biometrischer Daten geschaffen werden, sprich für eine Verknüpfung des SIS mit einem Automatischen Fingerabdruck-Identifizierungssystem (AFIS). Im März dieses Jahres ging eine solche Komponente nun in den Pilotbetrieb.

Die Polizei benötigt darüber hinaus eine gemeinsam getragene Technikoffensive: Für Kriminalität, die mittels technischer Neuheiten begangen wird, müssen entsprechende Abwehrmaßnahmen erforscht und entwickelt werden. Genauso müssen wir die Digitalisierung nutzen, um unsere Ermittlungsarbeit auf gemeinsamen technischen Plattformen zu organisieren und damit effizienter zu machen.

Hierzu ein Beispiel: 2017 ist es gelungen, mit „crimenetwork.biz“ die größte deutschsprachige *Underground-Economy*-Plattform, auf der zum Beispiel Betäubungsmittel, Waffen, Hacker-Tools und Falschgeld gehandelt wurden, auszuheben. Gemeinsam mit zehn Landeskriminalämtern hat das BKA über vier Monate hinweg erfolgreich die Administratoren und „Power-User“

dieser Plattform identifiziert. Dieser gemeinsame Ansatz hat sich bewährt, war allerdings mit großem Aufwand für die Ermittler aus den verschiedenen Bundesländern verbunden, die dafür vier Monate lang in Wiesbaden tätig sein mussten. Solche gemeinsamen Ermittlungsverfahren, die künftig eher die Norm als die Ausnahme sein werden, müssen effizienter und flexibler zu organisieren sein! Im BKA haben wir deshalb ein Tool entwickelt und im vergangenen Jahr in den Pilotbetrieb gebracht, mit dem Auswerter und Forensiker nun parallel wie untereinander mit dem gleichen Datenbestand arbeiten können. Der Weg zu einer bundesweiten Lösung ist zwar noch weit, aber möglich. Angesichts der Dynamik der Technikentwicklung sowie begrenzter Ressourcen können wir diese Herausforderungen nur gemeinsam bewältigen und finanzieren.

FÖDERALISMUS IM EINHEITLICHEN GEFAHRENRAUM

Damit eine so enge Zusammenarbeit gelingt, brauchen wir, auch für die operative Arbeit, bundesweit einheitliche Standards und einen einheitlichen Rechtsrahmen.

Ein Beispiel hierfür ist der Umgang mit islamistischen Gefährdern in Deutschland. Bislang wurden die Risikoeinschätzung von Gefährdern und die Entscheidung über adäquate Maßnahmen der Gefahrenabwehr in den Ländern vorgenommen – ohne gemeinsame Abstimmungsmechanismen. Mit dem Instrument „Radar-iTE“ hat das BKA im vergangenen Jahr bundesweit ein einheitliches Verfahren eingeführt, mit dem Personen des militant-salafistischen Spektrums aufgrund festgelegter Kriterien hinsichtlich ihres Risikopotenzials bewertet und in eine dreistufige Skala eingeordnet werden. Zudem sind das Ergebnis dieser Bewertung und die Abstimmung entsprechender Maßnahmen seit dem vergangenen Jahr Gegenstand von Sitzungen im Gemeinsamen Terrorismus-Abwehrzentrum, so wie es bei Gefährdungssachverhalten schon seit Langem der Fall ist.

Nun sollte grundsätzlich gewährleistet sein, dass Personen, von denen ein hohes Risiko ausgeht, entsprechenden polizeilichen Maßnahmen wie einer Telekommunikationsüberwachung unterzogen werden können, und zwar unabhängig davon, in welchem Bundesland sie leben. Derzeit ist dies allerdings nicht der Fall, da in einigen Bundesländern die nötigen Rechtsgrundlagen fehlen. Das muss sich ändern! Deutschland ist ein einheitlicher Gefahrenraum, in dem die Bürgerinnen und Bürger einen berechtigten Anspruch auf gleiche Schutzstandards haben. Sicherheit darf nicht vom Wohnort abhängig sein! Daher ist es zu begrüßen, dass die Innenministerkonferenz beschlossen hat, an einem neuen Musterpolizeigesetz zu arbeiten, mit dem die wesentlichen polizeilichen Befugnisse vereinheitlicht werden.

Schließlich muss Polizei im Zeitalter digitaler Kriminalität digital auch so ermitteln dürfen, wie sie es analog schon lange darf! Das erfordert beispielsweise eine funktionierende Speicherung von Standort- und Verbindungsdaten sowie verbindliche Regelungen zur Quellen-Telekommunikationsüberwachung, um auch verschlüsselte Kommunikation von Straftätern, beispielsweise über Messenger- und internetbasierte Kommunikationsdienste wie WhatsApp oder Skype, auswerten zu können. In der vergangenen Legislaturperiode hat sich in dieser Hinsicht viel getan. Es ist zu hoffen, dass auch die neue Regierung diesem Leitsatz weiter folgt.

Eine Polizei, die in starren föderalen Strukturen denkt und handelt, ist nicht mehr zeitgemäß. Das heißt nicht, dass wir den Föderalismus abschaffen wollen! Im Gegenteil: Der Bezug zum Lokalen und der direkte Kontakt mit den Bürgerinnen und Bürgern sind für die polizeiliche Arbeit unabdingbar. Diese Stärken der föderalen Struktur gilt es zu bewahren. Wir müssen sie aber mit den Stärken zentraler Organisationen verbinden: einheitlichen rechtlichen Grundlagen und Standards und einem konzertierten Vorgehen bei der Entwicklung neuer, gemeinsamer Systeme. Als Zentralstelle der deutschen Polizei wird sich das Bundeskriminalamt auch weiterhin engagiert in diese notwendigen Veränderungsprozesse einbringen.