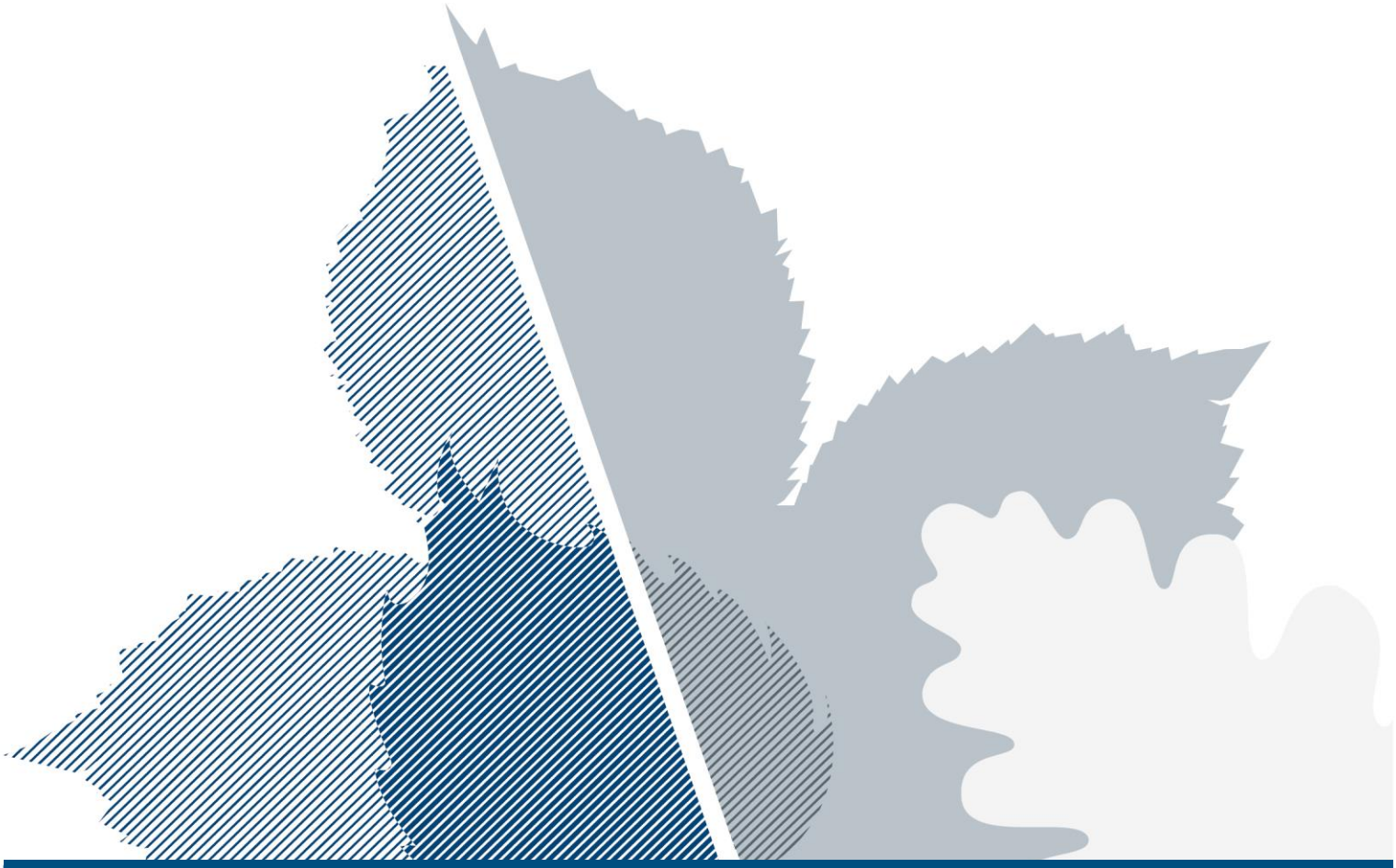
Bundeskriminalamt

BKA AUTUMN CONFERENCE HERBSTTAGUNG



Sicherheit in einer offenen und digitalen Gesellschaft

BKA Herbsttagung
21. – 22. November 2018

Kriminalitätsbekämpfung weiterdenken

Phänomene – Herausforderungen – Handlungsoptionen im Zeitalter von Big Data, Algorithmen und autonomen Systemen

Kurzfassung

Holger Münch
Präsident des Bundeskriminalamtes

KRIMINALITÄTSBEKÄMPFUNG WEITERDENKEN

PHÄNOMENE – HERAUSFORDERUNGEN – HANDLUNGSOPTIONEN IM ZEITALTER VON BIG DATA, ALGORITHMEN UND AUTONOMEN SYSTEMEN

Globalisierung und Digitalisierung haben uns vielfältige neue Möglichkeiten eröffnet. Sie haben die Welt aber auch unübersichtlicher werden lassen. Wo diese Unübersichtlichkeit zu Verunsicherung führt, entsteht schnell der Wunsch nach Abschottung. Wer sich hingegen sicher fühlt, ist auch in der Lage, offen für Neues, für Perspektiven, Chancen und Möglichkeiten zu sein. Sicherheit und das Vertrauen darin, dass die staatlichen Institutionen für Sicherheit sorgen, ist also eine Grundvoraussetzung, damit die offene Gesellschaft ihr Potential voll entfalten und Antworten auf die Herausforderungen unserer Zeit finden kann.

Die deutsche Polizei sorgt täglich für Sicherheit. Dennoch sieht auch sie sich großen Herausforderungen gegenüber. Denn Globalisierung und Digitalisierung verändern die Kriminalität und die Polizeiarbeit. Straftäter agieren längst über Landesgrenzen hinweg, sind international vernetzt und nutzen modernste Technik zur Begehung von Straftaten. Es gilt daher, die Polizei in Deutschland konsequent und schnell für das digitale Zeitalter fit zu machen. Das betrifft das „Dürfen“, also die notwendigen gesetzlichen Grundlagen, und das „Können“, die konkreten Fähigkeiten der Polizei in Bund und Ländern.

Zusammenarbeit neu denken - föderal geht nur digital

In der Herausforderung liegt dabei auch die Antwort: Föderal geht nur digital. Das BKA baut derzeit mit dem Programm Polizei 2020 eine digitale Plattform für die deutsche Polizei auf, die der gemeinsamen Datenhaltung, als eine Art „App-Store“, als Ort der digitalen operativen Zusammenarbeit und als Entwicklungsplattform dienen wird. Die Plattform wird administrativen Aufwand reduzieren, die Polizistinnen und Polizisten bei ihrer täglichen Arbeit unterstützen und völlig neue und zeitgemäße Formen der Zusammenarbeit ermöglichen.

Der Vorschlag des BKA, damit das Potential dieser Plattform voll ausschöpft werden kann, ist eine Zusammenarbeit, die nach dem Prinzip der Themenführerschaft funktioniert. Das heißt, dass einzelne Länder, Länderverbünde oder der Bund für ein bestimmtes Thema verantwortlich sind, die Entwicklungen vorantreiben und dann den anderen zur Verfügung stellen. Und zwar ohne detaillierte Abstimmungen. Der Einzelne wird gegenüber der föderalen Gemeinschaft so ergebnisverantwortlich.

Die Entwicklung und Bereitstellung von Fähigkeiten sollte sich an einem mehrstufigen Kompetenzmodell orientieren. Basiskompetenz sollte in der Fläche vorliegen, Fachkompetenz in spezialisierten Dienststellen. Im Bereich der Hochkompetenz, die naturgemäß nur bei einigen wenigen vorliegen kann, sollte eng zusammengearbeitet

werden, um Entwicklungen für die anderen Kompetenzebenen voranzutreiben und zur Verfügung zu stellen. Der immer noch weit verbreiteten Verwaltungsgrundsatz „§ 1 Jeder macht Seins“ wird so abgeschafft und eine ganz andere Form von föderaler Zusammenarbeit als bisher etabliert.

Erreicht wird so, dass jeder Polizist und jede Polizistin die notwendigen und rechtlich zulässigen Informationen in jeder Situation zur Verfügung hat – egal woher aus Deutschland oder Europa sie kommen. Es wird ferner sichergestellt werden, dass jede Ermittlerin und jeder Ermittler Zusammenhänge erkennen kann – egal wo ein Vorfall stattgefunden hat. Die Basis hierfür ist, dass die deutsche Polizei mit einheitlichen Werkzeugen und einheitlichen Systemen arbeitet, die einmal für alle entwickelt wurden.

Neue Abteilung des BKA zur Cybercrimebekämpfung

Neben der Modernisierung der Zusammenarbeit muss aber auch, was die ganz konkrete Kriminalitätsbekämpfung angeht, eine stetige Entwicklung stattfinden. Das gilt auch und insbesondere für die Gefahren aus dem Cyberraum.

Das BKA gehört, was Ermittlungen im Cyberraum angeht, zu den Besten der Welt. Anlass zur Selbstzufriedenheit ist das jedoch nicht. Im Gegenteil: Das BKA will sich noch besser aufstellen und für die Zukunft rüsten.

Daher wird das BKA eine neue Abteilung zur Bekämpfung von Cybercrime einrichten. In dieser Abteilung sollen „digitale Ermittlungen“ geführt, neue Tools- und Methoden entwickelt, aber auch Serviceleistungen für die Landespolizeien angeboten werden. Mit der neuen Cybercrimeabteilung will das BKA sich dabei nicht nur stärker in der Strafverfolgung engagieren, sondern bereitet sich auch darauf vor, Verantwortung bei der Gefahrenabwehr zu übernehmen.

Gefahrenabwehr im Cyberraum – Aufgabe für Polizei in Land und Bund!

Cyberangriffe bergen ein erhebliches Schadenspotential. Sie können die Wirtschaft, Leib und Leben von Menschen und auch den Staat selbst gefährden. Die Beeinträchtigungen des Gesundheitssektors in Großbritannien durch Wannacry, Angriffe auf Spitzentechnologien deutscher Unternehmen oder der Angriff auf staatliche Institutionen zeigen: Cyberangriffe sind längst real. Und sie werden künftig eher zu- als abnehmen.

Eine ganzheitliche Gefahrenabwehr scheitert jedoch immer wieder an bestehenden rechtlichen Lücken – genau genommen an einer fehlenden Zuständigkeit des Bundes.

Hierzu ein Beispiel: Der britischen Polizei gelang vor nicht langer Zeit der Takedown, also die Abschaltung eines Botnetzes. Sie teilte dem BKA mit, dass geplant sei, die infizierten Geräte zu bereinigen. Da nur die Länderkennung der betroffenen IP-Adressen für Deutschland ermittelbar war, nicht jedoch die genaue geographische Lage, hätten alle Bundesländer zustimmen müssen, sich an der Bereinigung zu beteiligen. Doch es gab nicht in allen Bundesländern die rechtlichen Voraussetzungen für eine solche Bereinigung. Sie

wurde deshalb nicht durchgeführt. Wenn betroffene Geräte, die Teil eines Botnetzes sind, nicht umfassend bereinigt werden, besteht jedoch die Gefahr, dass sie jederzeit wieder reaktiviert werden und mit ihnen DDoS-Angriffe auf Privatpersonen, Unternehmen oder Kritische Infrastrukturen gestartet werden.

Das Beispiel zeigt: Man kann einer globalen, digital vernetzen Gefahr aus dem Cyberraum nicht mit lokalen Maßnahmen der Gefahrenabwehr begegnen. Neben den auf den Landespolizeigesetzen basierenden Zuständigkeiten der Länder sollte daher auch der Bund Gefahrenabwehrbefugnisse haben.

Etwaige präventive Zuständigkeiten des BKA könnten sich dabei am Erfolgsmodell Präventivbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus und an den schon bestehenden Strafverfolgungskompetenzen des BKA im Bereich Cybercrime orientieren. Sie könnten also eingerichtet werden für den Fall, dass eine Bundeseinrichtung oder Kritische Infrastrukturen betroffen sind, eine länderübergreifende Gefahr besteht oder wenn die Zuständigkeit einer Landespolizei nicht erkennbar ist bzw. ein Land das BKA um Übernahme des Falls ersucht.

Die bestehenden Befugnisse in den Landespolizeigesetzen würden so sinnvoll ergänzt und bestehende Lücken geschlossen.

Die allermeisten Gefahren aus dem Cyberraum könnten dann durch polizeiliche Maßnahmen abgewehrt werden. Dabei könnte der Großteil möglichen präventivpolizeilichen Handelns im Inland umgesetzt werden, und zwar auch, wenn der Cyberangriff aus dem Ausland kommt. Gleichzeitig könnte aber auch, wenn Maßnahmen im Inland nicht ausreichen, auf die bestehenden Kontakte und bewährten Wege der internationalen polizeilichen Zusammenarbeit zurückgreifen und so auch gegebenenfalls notwendige Maßnahmen im Ausland angestoßen werden.

Was übrig bliebe, wären Gefahren aus einigen wenigen, nicht kooperationsbereiten Staaten. Gegen deren erklärten Willen auf deren Hoheitsgebiet Maßnahmen zu treffen, ist wahrlich keine polizeiliche Aufgabe, aber auch der absolute Ausnahmefall. Die aktuellen Diskussionen zum Thema Gefahrenabwehrbefugnisse sollten daher nicht zu sehr auf Maßnahmen der Cyber Network Intervention – den sogenannten „Hack-Back“ fokussiert werden. Es ist zwar wichtig und richtig, sich mit dem „Hack-Back“ auseinanderzusetzen, um auch für den Ausnahmefall vorbereitet zu sein; genauso wichtig ist es aber, die vielen anderen Szenarien im Auge zu haben, die die polizeiliche Gefahrenabwehr betreffen, und die hier bestehenden gesetzlichen Lücken zu schließen.

Vertrauen und Verantwortung

Die Bürgerinnen und Bürger müssen darauf vertrauen können, dass der Staat und die staatlichen Institutionen für ihre Sicherheit sorgen. Sie müssen darauf vertrauen können, dass der Rechtsstaat funktioniert, Straftaten verfolgt und die Regeln des Zusammenlebens in unserer offenen Gesellschaft eingehalten werden. Und sie müssen darauf vertrauen

können, dass die Polizei angemessen ausgestattet und in der Lage ist, ihre Aufgaben in einer sich dynamisch verändernden Umwelt zukunftsfähig zu erledigen.

Das alles zu gewährleisten ist eine große Verantwortung. Doch die deutsche Polizei ist bereit und in der Lage, diese Verantwortung zu tragen!