Digitalisierung - Was sind die größten Herausforderungen für die Sicherheitsbehörden?

02.04.2021

Aufbruch zur kriminalpolizeilichen Ausbildung und Fortbildungsinitiativen noch in diesem Jahr

Die derzeitige Phase der Digitalisierung wird von vielen als Beginn der vierten industriellen Revolution bezeichnet. Nach der Mechanisierung mittels Wasser- und Dampfkraft durch die Erfindung der Dampfmaschine, der Massenfertigung mit Hilfe von Fließbändern und elektrischer Energie, der Erfindung des Computers sowie der Nutzung von IT und Elektronik stehen wir möglicherweise gerade am Beginn einer Zeit, die neben der Ausweitung der Plattformökonmie und dem Internet der Dinge dadurch geprägt sein könnte, dass Softwareprodukte in breitem Umfang menschliche Entscheidungen erleichtern, beeinflussen oder ersetzen könnten. „Machine Learning“ und „Künstliche Intelligenz“ wird insoweit von den einen als Heilsbringer, von den anderen als bedrohliches Szenario erkannt. Dass derartige Entwicklungen neben dem Arbeitsmarkt ganze Gesellschaften und mithin auch Kriminalität und Kriminalitätsbekämpfung beeinflussen werden, erklärt sich von selbst.

Ich habe in den vergangenen Wochen viele Gespräche zu Themen rund um die Digitalisierung geführt. Alle Gesprächspartner kann man mehr oder weniger als „Spezialisten“ beschreiben. Darunter waren Abgeordnete, Kolleginnen und Kollegen aus Ministerien, Bundes- und Landesbehörden, Lehrstuhlinhaber sowie ein Mitglied der Bundesregierung. Inhaltlich ging es um die rechtliche Ausgestaltung der Bestandsdatenauskunft - und deren besondere Bedeutung im Zusammenhang mit dem Gesetz gegen Rechtsextremismus und Hasskriminalität oder um die Frage, ob und inwieweit den Behörden ein sog. Hackback („Gegenangriffe“ auf eine Cyberattacke, um diese zu beenden) erlaubt sein sollte und wenn ja, welche Behörde(n) dafür zuständig sein sollte(n).

Es ging um einen Gesetzesentwurf, der es im Ausland sitzenden Banden technisch unmöglich machen soll, bei Angerufenen die Rufnummern 110 oder 112 erscheinen zu lassen. Es ging um Analysten, die bei Recherchen zu einer Information Abfragen in völlig unterschiedlich aufgebauten Datenbanken vornehmen müssen. Ich sprach über neu ausgestaltete Prozesse, die das Bundeskriminalamt mit den Kriminalpolizeien der Länder abgestimmt hat, um Ermittlungen nach Meldungen („Kinderpornografie“) des NCMEC (National Center for Missing & Exploited Children) möglichst effizient durchführen zu können. In dem Zusammenhang drehte es sich auch um erforderliche Ermittlungen in offenen Quellen, sog. OSINT-Recherchen (Open Source Intelligence).

Ich sprach mit Finanzermittlern über Kryptowährungen. Investigative Journalisten berichteten mir von Ihren Recherchen in Zusammenhang mit dem erfolgreichen Hacken der französischen Gendarmerie von EncroCHAT-Handys, also besonders verschlüsselten Handys, die vorwiegend von der Organisierten Kriminalität genutzt wurden. Und nicht zuletzt spielten Softwarelösungen aus dem Segment der sog. Künstlichen Intelligenz eine Rolle, mit deren Hilfe Massendaten im Bereich der „Kinderpornografie“ besser und schneller ausgewertet werden können sowie technische Möglichkeiten, Material, auf dem sexualisierte Gewalt an Kindern zu sehen ist, komplett künstlich herzustellen, um damit Täternetzwerke zu infiltrieren.

Wer sich mit einzelnen der vorgenannten Themen befasst, stellt schnell fest, dass ich nicht mehr über exotische Fragestellungen schreibe, mit denen sich nur ganz wenige, hochspezialisierte Dienststellen der Kriminalpolizei befassen müssen. Nein! Viele dieser Themenkomplexe gehören längst zum kriminalpolizeilichen Handwerkszeug vieler Kripo-Dienststellen oder werden in Kürze dazukommen. Unabdingbare Voraussetzung ist allerdings, dass die Qualifikation der Kolleginnen und Kollegen in den betroffenen Dienststellen mit dem Werkzeugkasten Schritt hält. Genau das ist leider in den meisten Bundesländern längst nicht mehr der Fall. Es entsteht eine menschliche Wissens- und Fähigkeitslücke, die man ohne Übertreibung als die größte Achillesferse der Sicherheitsbehörden einstufen muss. Sie ist noch beträchtlich größer als der zahlenmäßige Personalmangel, mit dem wir in den Ländern ohnehin schon zu kämpfen haben. Politisch ist das vielerorts leider noch nicht angekommen. Die Dimension des täglich anwachsenden Wissensrückstands wird von Politik und Öffentlichkeit ähnlich unterschätzt wie das Ausmaß Organisierter Kriminalität, dass in jüngster Vergangenheit durch den gehackten EncroCHAT oder die Sicherstellung von 16 Tonnen Kokain im Hamburger Hafen etwas deutlicher wurde. Dabei müsste man nur aufmerksamer sein und sich an die Veröffentlichung der Bedrohungsanalyse zur schweren und organisierten Kriminalität von EUROPOL vom 9. März 2017 erinnern. Sie trug den Titel „CRIME IN THE AGE OF TECHNOLOGY“ (KRIMINALITÄT IM ZEITALTER DER TECHNOLOGIE) und enthielt u.a. folgende Kernaussagen, an die ich an dieser Stelle erinnern möchte:

- Gegen mehr als 5.000 internationale Gruppen der Organisierten Kriminalität (OCGs) mit mehr als 180 Nationalitäten wird derzeit in der EU ermittelt.
- Die Zahl der Gruppen der Organisierten Kriminalität, die in mehr als eine kriminelle Aktivität verwickelt sind (polykriminell), hat in den letzten Jahren stark zugenommen (45 % im Vergleich zu 33 % im Jahr 2013).
- Bei fast allen Arten der Organisierten Kriminalität setzen Kriminelle die Technologie immer geschickter und effektiver ein und passen sie an. Dies ist heute vielleicht die größte Herausforderung für die Strafverfolgungsbehörden auf der ganzen Welt - auch in der EU.
- Cryptoware (Ransomware, die Verschlüsselung nutzt) hat sich zur führenden Malware in Bezug auf Bedrohung und Auswirkungen entwickelt. Sie verschlüsselt benutzergenerierte Dateien des Opfers und verweigert ihm den Zugriff - es sei denn, das Opfer zahlt eine Gebühr, um seine Dateien entschlüsseln zu lassen.

- Dokumentenbetrug hat sich als eine der wichtigsten kriminellen Aktivitäten im Zusammenhang mit der Migrationskrise herausgestellt.
- Dokumentenbetrug, Geldwäsche und der Online-Handel mit illegalen Waren und Dienstleistungen sind die Motoren der Organisierten Kriminalität.

Diese Erkenntnisse sind über vier Jahre alt. Wenig überraschend haben die Gruppierungen der Organisierten Kriminalität in der Pandemie zusätzliche und neue Marktchancen für sich erkannt. So schreibt EUROPOL am 12. November 2020 auf seiner Homepage: „*Kriminelle haben ihre Techniken schnell angepasst, um unsere Ängste rund um die COVID-19-Pandemie auszunutzen. Ihr Hauptziel ist der Profit mit allen Mitteln.“*

Das Hauptziel der deutschen und europäischen Kriminalpolitik muss es sein, mit allen Mitteln dazu beizutragen, dass es die klügsten und besten Köpfe mit diesen Verbrecherbanden aufnehmen. Hierzu benötigen wir noch in diesem Jahr spezialisierte Studiengänge in allen Bundesländern, die den direkten Weg in die Kriminalpolizei ermöglichen. Wir benötigen einen deutlichen Aufbruch zur kriminalfachlichen Spezialfortbildung unter Nutzung der schon bestehenden Fortbildungskooperationen, neue berufsbegleitende Masterstudiengänge, Personalentwicklungskonzepte mit attraktiven Stellen für Fachkarrieren bei Beamten und Tarifbeschäftigten sowie Sonderzulagen oder/und Verbeamtung bei Tarifbeschäftigten und Möglichkeiten des Quereinstiegs für vorqualifizierte Bewerber. Das wäre eine echte Exzellenzinitiative, die von der Innenministerkonferenz ausgehen müsste, vor der sich die Organisierte Kriminalität ernsthaft fürchten sollte.

Bleiben Sie gesund,

Ihr Sebastian Fiedler