Cybercrime aus Sicht der Aus- und Fortbildung der Polizei

Von Gerrit Domenghino LL.M., Münster

1 Einleitung: Das Böse schläft nie

„Die Zukunft ist schon da, nur noch nicht gleichmäßig verteilt“ soll der Science-Fiction-Autor William Gibson schon vor 20 Jahren in Bezug auf die Kluft zwischen denen, die moderne Technologien einsetzen und jenen, die der technischen Entwicklung hinterherhinken, gesagt haben. Diesen Ausspruch kann man heute auch auf die Cyberkriminalität übertragen, denn dort gibt es die Einen, die vielleicht ihr gesamtes Leben diesem Thema widmen, die vor dem Computer essen, trinken und schlafen. Sie stecken ihre ganze (kriminelle) Energie und Leidenschaft in das Ziel, die allgemeinen Risiken und aus ihrer Sicht Chancen der Digitalisierung für ihren (oftmals finanziellen) Vorteil zu nutzen. Und auf der anderen Seite sitzen die Mitarbeiter[2] von Unternehmen und Behörden, die die Cyberattacken verhindern oder verfolgen sollen.

„So wie sich unsere Gesellschaft rasant verändert, so schnell verändern sich Kriminalität und ihre Erscheinungsformen“[3] hat der damalige nordrhein-westfälische Innenminister Ralf Jäger im Zusammenhang mit der Vorstellung der Polizeilichen Kriminalstatistik (PKS) 2013 gesagt. Das vor gut einem Jahr zunächst in China aufgetretene und dann zur weltweiten Pandemie gewordene COVID-19-Virus hatte ein gewaltiges Momentum, um die Gesellschaft und folglich die Kriminalität und ihre Erscheinungsformen zu verändern. Die Regierungen vieler Länder reagierten mit unterschiedlichsten Direktiven auf die Bedrohungslage. Zu den im März 2020 von den Regierungen in Bund und Ländern beschlossenen Maßnahmen zur Eindämmung der COVID-19-Pandemie zählten Kontaktbeschränkungen und Ausgangssperren, die viele Unternehmen dazu veranlassten, Mitarbeiter möglichst von zu Hause aus arbeiten zu lassen, wo diese dann für berufliche Zwecke meist private Endgeräte nutzten. Von heute auf morgen wurden Esstische als Arbeitsplätze und das heimische Wohnzimmer für Videokonferenzen genutzt; oftmals mit Hard- und Software, die aus der Not heraus und ohne ausreichende Sicherheitsüberprüfung für gut und nutzbar befunden wurden. Die in großen Unternehmen und Behörden sonst üblichen institutionalisierten Schutzmechanismen zur Abschottung der IT gegen Gefahren von außen waren somit oft nicht mehr gegeben, stattdessen wurden Heimnetzwerke mit häufig fehlenden professionellen Virenschutzprogrammen oder Firewalls genutzt. Ein weiteres Risiko entstand dadurch, dass auf diesen Systemen häufig Software installiert ist, die grundlegende Sicherheitslücken aufweist. So konnte man sich beim Videokonferenz-Anbieter Zoom eine Zeit lang in fremde Konferenzen zu schalten, oder auch Software wie Cisco Web-ex, Microsoft Teams oder Google Hangouts verfügte nur über eine unzureichende Ende-zu-Ende-Datenverschlüsselung.[4] Nicht zuletzt wurden unter Zeitdruck vermehrt Möglichkeiten zum Fernzugriff auf die internen Netzwerke der Arbeitgeber geschaffen, wodurch es für die jeweiligen IT-Experten der Unternehmen und Behörden schwieriger wurde, unrechtmäßige Zugriffe zu identifizieren. Diese Veränderungen in der Nutzung von digitalen Angeboten und die daraus resultierende Gefahr impliziert einen wachsenden Bedarf im Bereich der Aus- und Fortbildung zur Bekämpfung der Cyberkriminalität.

2 Aktuelle Entwicklungen im Bereich Cybercrime

Angesichts der rasant steigenden Zahl von Cyberangriffen weltweit und in Deutschland sind die Sicherheitsbehörden mehr denn je gefordert, diesem Phänomen repressiv als auch präventiv entgegen zu treten. Die Polizeiliche Kriminalstatistik weist für das Jahr 2019 einen Trend mit einer Steigerung um 11,3% bei der Computerkriminalität aus, bei einem gleichzeitigen Rückgang der Aufklärungsquote um 15,2%.[5] Bereits 2017 hatte der Digitalverband Bitkom[6] vermeldet, dass jedes zweite Unternehmen in den vorangegangenen beiden Jahren Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden war, und dadurch ein Schaden von rund 55 Milliarden Euro pro Jahr entstanden war.[7] Trotz des immensen Schadens, der ein Vielfaches der beispielsweise für das Berichtsjahr 2018 bezifferten Gesamtschadenssumme von 7,3 Milliarden Euro aller in der PKS erfassten Straftaten ist,[8] schaltete nicht einmal jedes dritte betroffene Unternehmen staatliche Stellen ein; zum Teil aus Sorge vor Imageschäden.[9] Um den Cybergefahren begegnen und die Cyberkriminalität bekämpfen zu können, bedarf es eines Bündels an Maßnahmen – von der Aufklärung der Nutzer über die Präventionsarbeit bis hin zur Aus- und Fortbildung der Mitarbeiter in den verschiedenen Strafverfolgungsbehörden.

3 Cybercrime in der grundlegenden Ausbildung der Polizei

Die Gewerkschaft der Polizei in NRW forderte Anfang vergangenen Jahres eine Optimierung der Aus- und Fortbildung, um den aktuellen Entwicklungen im Bereich Cybercrime entgegen zu treten.[10] Eine Forderung, die nur unterstützt werden kann, denn zur erfolgreichen Bekämpfung bedarf es einer frühzeitigen Auseinandersetzung mit dem Phänomen in der Ausbildung der Mitarbeiter der Sicherheitsbehörden und eines ausreichenden Fortbildungsangebots, um das Wissen aufrecht und aktuell zu halten.

Auch außerhalb des (mehr oder weniger) geschlossenen Systems der Aus- und Fortbildung der Polizei kann eine Qualifizierung im Bereich Cybercrime wahrgenommen werden, beispielsweise an der Hochschule Wismar[11] oder der Hochschule Mittweida[12]. Die Studienangebote außerhalb der polizeilichen Aus- und Fortbildung haben zwar den Vorteil, dass sie keine so strikten Zugangsbarrieren haben und im Prinzip von Jedem oder Jeder studiert werden können, jedoch ist der Nutzen für ein berufliches Vorankommen im Polizeidienst nicht immer gegeben. Es bedarf hier stets der Einzelfallprüfung, ob ein solcher Studienabschluss für eine möglicherweise angestrebte Laufbahnbefähigung anerkannt wird.

3.1 Bachelor-Studium Polizeivollzugsdienst

Der Grundstein für die Bekämpfung der Cyberkriminalität wird in der Ausbildung der Polizeivollzugsbeamtinnen und -beamten (PVB) gelegt, die von Bundesland zu Bundesland unterschiedlich ist. In Nordrhein-Westfalen erfolgt der Einstieg in den Polizeidienst in den gehobenen Dienst über ein dreijähriges duales Studium. In diesem werden den angehenden Kommissaren an der Hochschule für Polizei und Verwaltung (HSPV), dem Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten der Polizei (LAFP) und den Kreispolizeibehörden in einem Dreischritt – Theorie lernen, durch Training vertiefen und in der Praxis anwenden – die nötigen Inhalte vermittelt. Im Modulhandbuch des Studiums ist das Thema Cybercrime nicht explizit vorgesehen, dennoch hat das Thema bereits seit mehreren Jahren Einzug in die Aus- und Fortbildung in NRW gehalten und ist entsprechend der allgemeinen Digitalisierung auch nicht mehr aus der Ausbildung wegzudenken. Aus diesem Grunde werden den Studierenden für die Tätigkeit im Wach- und Wechseldienst über zehn Lehrveranstaltungsstunden[13] (LVS) durch fachlich versierte Dozenten Basiskompetenzen im Zusammenhang mit Cybercrime vermittelt, zu denen u.a. die Besonderheiten bei der Anzeigenaufnahme, dem Ersten Angriff sowie der Anschlussinhaberfeststellung und der Ermittlung von IP-Adressen zählen.[14]

Etwas differenzierter hat sich beispielsweise die Hochschule für Polizei Baden-Württemberg (HfPolBW) der Cyberkriminalität angenommen,[15] bei der Cybercrime in der Ausbildung für den mittleren Polizeivollzugsdienst (mPVD) als eigenständiges Thema sowohl in den Lehrplänen für den mPVD, als auch im Lehrplan zur Vorausbildung des gehobenen Polizeivollzugsdienstes (gPVD) verortet ist. In der Ausbildung der mPVD wird das Thema „Computer- und Internetkriminalität, Cybercrime“ im Abschlusskurs des Moduls „Ausgewählte Erscheinungsformen der Kriminalität“ behandelt, in dem eine Lernanwendung „Ersteinschreiter Cybercrime – Grundlagenwissen für Ersteinschreiter“ enthalten ist. In der Vorausbildung zum gPVD wird den Teilnehmern in einem vierstündigen Seminar das erforderliche Grundlagenwissen eines „Polizeilichen Sachbearbeiters als Ersteinschreiter“ vermittelt. Primäres Ziel der Ausbildung ist die Vermittlung von Erst- und Sofortmaßnahmen, die vom Streifendienst im Rahmen des Ersteinschreitens gemeistert werden sollen. Dazu gehört der Sicherungsangriff bei Delikten, bei denen Informations- oder Kommunikationsmedien eingesetzt wurden, und die Einleitung aller unaufschiebbaren Maßnahmen, die zur Aufklärung der Straftat notwendig erscheinen. Des Weiteren werden den Anwärtern in den Rechtsfächern die wichtigsten Eingriffsnormen unter Berücksichtigung des Telekommunikationsgesetzes, des Telemediengesetzes, der Strafprozessordnung und des Strafgesetzbuches vermittelt. Darauf aufbauend liegt im Fach Kriminalistik der Fokus auf den Ermittlungsmöglichkeiten und dem Ersten Angriff, der den fachgerechten Abbau von PC-Anlagen oder die Sicherung von Smartphones beinhaltet. Schließlich

werden in dem Bereich „Information und Kommunikation“ eine weitere Sensibilisierung für das Thema angestrebt und Kenntnisse zum Umgang mit Informationsquellen wie Polizei-Online und Extrapol vermittelt. Der Schwerpunkt liegt hier jedoch auf dem Erlernen von speziellem Grundlagenwissen, um beispielsweise durch die Verfolgung von IP-Adressen und E-Mail-Header[16] und die Recherche im Intra-/und Internet Cyberkriminalität zu verfolgen und zu bekämpfen. Mittelfristig wird durch eine verstärkte Schwerpunktsetzung im Themenfeld Cybercrime in der Ausbildung des mPVD und des gPVD angestrebt, so dass die Absolventen die Qualifikation eines Sachbearbeiters der Ebene 2 vorweisen können, die derzeit erst noch in Fortbildungen vermittelt wird.

In Sachsen wird in der Ausbildung des gPVD an der Hochschule der Sächsischen Polizei neben den obligatorischen Pflichtmodulen ein Wahlpflichtmodul *„Cybercrime“* angeboten und dadurch eine intensivere Auseinandersetzung mit dem Kriminalitätsfeld ermöglicht. Die Studierenden vertiefen in dem Modul ihr zuvor im Studium erlangtes Grundwissen zum Themenkomplex „Straftaten im Zusammenhang mit dem Internet“ und erweitern ihre Kenntnisse über Phänomene sowie Modi Operandi im Bereich Cybercrime. Sie lernen, welche ermittlungsrelevanten Informationen im Bereich der Informations- und Kommunikationstechnik anfallen, und wie diese technisch erlangt beziehungsweise gesichert werden können. Des Weiteren bekommen sie einen Überblick über ermittlungstechnische Möglichkeiten im Bereich Cybercrime und erlernen grundlegende Techniken zu Ermittlungen im Internet und der Auswertung der Ergebnisse.[17] Dafür setzen sich die Studierenden in insgesamt 100 Stunden Kontakt- und Selbststudium u.a. mit Schadsoftware, Botnetzen, dem Aufbau und den Ermittlungen im „Darknet“ sowie Grundlagen der IT-Forensik, inklusive dem Kennenlernen der polizeilichen forensischen Sicherungs- und Auswertetools, auseinander. Sie erlangen Kenntnisse über den verdeckten Zugriff auf informationstechnische Systeme, Quellen-TKÜ, Server-TKÜ, mobile Funkaufklärung und IP-Tracking, einschließlich der Grundsätze der Vorbereitung und Durchführung entsprechender Maßnahmen. Abgerundet wird das Wahlpflichtmodul durch technische Aspekte der IuK-Tatortarbeit, z.B. Besonderheiten bei der Durchführung von Durchsuchungen, und können im Rahmen von Einsatzhospitationen Praxiserfahrung sammeln.

Dieser kleine Einblick in die Integration der Thematik Cybercrime in der Ausbildung der PVB zeigt, dass es einen unterschiedlichen Stand in den Ländern gibt. Hier könnte der „Blick über den Tellerrand“ gewinnbringend für alle Beteiligte sein, da die Herausforderung für die Sicherheitsbehörden ähnlich sind und eine Kooperation bei der Entwicklung von Ausbildungsinhalten Synergieeffekte ergeben könnte.

3.2 Bachelor-Studium Kriminalpolizei

Im Dezember 2009 erfolgte erstmals die Akkreditierung für den dualen Bachelor-Studiengang Kriminalvollzugsdienst des Fachbereiches Kriminalpolizei der Fachhochschule des Bundes für öffentliche Verwaltung,[18] über den ein Direkteinstieg als Kriminalkommissar beim Bundeskriminalamt (BKA) möglich wurde. Ergänzend zu den unter anderem kriminal- und rechtswissenschaftlichen Studieninhalten sind polizeispezifische Trainings wie Sprachausbildung, Einsatztraining und Dienstkunde vorgesehen. Obwohl es sich um einen kriminalwissenschaftlich ausgerichteten Studiengang handelt, erfolgt erst im vierten Semester in einem Modul die Auseinandersetzung mit der polizeilichen Informationserhebung und -verwendung und dem Phänomen Cybercrime. In einer insgesamt 240 LVS umfassenden Einheit sollen die Studierenden das Phänomen in kriminologischer und strafrechtlicher Hinsicht begreifen und dazu befähigt werden, (kriminal-)polizeiliche Informationsgewinnungs- und -verwendungsmaßnahmen sowie Ermittlungshandeln im Bereich Cybercrime zu gestalten. Dafür werden ihnen u.a. Grundlagenwissen zu den (informations-)technischen Gegebenheiten und Möglichkeiten sowie besondere verfassungsrechtlichen Anforderungen, insbesondere bei verdeckter Überwachung, als auch die einschlägigen Rechtsgrundlagen im Strafverfahrens- und Gefahrenabwehrrecht vermittelt. Dadurch sollen die Studierenden Cybercrime aus kriminologischer und strafrechtlicher Sicht begreifen. Nicht zuletzt geht es in dem Studium darum, polizeipraktische und taktische Aspekte sowie klassische und neuartige Maßnahmen und Methoden, sowohl der verdeckten technischen und personalen Überwachung als auch sonstiger Informationserhebung im Zusammenhang mit der Nutzung von Informations- und Kommunikationstechnik, zu erlenen.[19] Eine Besonderheit des Studiengangs ist es, dass Bewerber, die bereits über einen Bachelorabschluss verfügen, die Laufbahnausbildung auf 24 Monate verkürzen können. Bei erfolgreichem Abschluss können die Kriminalkommissare bei den Ermittlungen gegen organisierte Kriminelle oder den Terrorismus, dem Auswerten von Informationen und bei der Zusammenarbeit mit anderen Polizeibehörden weltweit eingesetzt werden.

Auch in Hessen wurde die Notwendigkeit einer Gewinnung von Fachkräften durch eine spezialisierte Ausbildung der angehenden Kollegen erkannt und neben dem 2006 an der Hessischen Hochschule für Polizei und Verwaltung eingeführten dualen Studium „Kriminalpolizei“, der den Direkteinstieg in die Kriminalpolizei ermöglicht, zum Wintersemester dieses Jahres erstmals die Vertiefungsrichtung „Cyberkriminalistik“ angeboten. Das Curriculum sieht vor, dass die Studierenden nicht nur die besondere Bedrohung durch Cyberkriminalität und ihre unterschiedlichen Erscheinungsformen verstehen, sondern auch die einschlägigen Normen des Strafgesetzbuches in Bezug auf Cyberkriminalität kennen und anwenden können. Auch die digitale Ermittlung, das Erfassen und forensische Auswerten von digitalen Spuren, OSINT-Ermittlungen[20] sowie die Erfassung und Auswertung von Standortdaten im Rahmen der Bearbeitung von Ermittlungsverfahren sollen den angehenden Kriminalkommissaren vermittelt werden.[21] Erstaunlicherweise war die Nachfrage für diesen Studiengang so gering, dass er entgegen der eigentlichen Planung nicht im Oktober 2020 starten konnte; zum Sommersemester 2021 wird der Studiengang

jedoch wieder angeboten werden.

3.3 Spezialisierung zum Cyberkriminalisten

Bei der Bekämpfung von Cyberkriminalität kann ein durchschnittlich geschulter PVB an die Grenzen seines informationstechnischen Wissens geraten. Regelmäßig erfordert die Bearbeitung der Fälle sowohl besonderes IT-Fachwissen als auch besondere technische Beweisführungsmethoden. Denn neben der Sicherung digitaler Spuren und der forensischen Untersuchung von IT-Systemen sollen die Mitarbeiter auch die Aufbereitung und möglicherweise Dekryptierung von gesicherten Daten vornehmen können. Infolge dieser Herausforderungen wurde auf Bundesebene und in einigen Ländern eine Sonderlaufbahn im gehobenen Dienst für Cyberkriminalisten geschaffen.

Um der Kriminalität im Bereich der Informations- und Kommunikationstechnik (IuK) effektiv und effizient zu begegnen, wurden im Herbst 2018 erstmals in einem Pilotprojekt sieben Cyber-Kriminalisten beim BKA eingestellt. Das BKA ist gewillt auch auf diesem Wege seinen Bedarf an Fachkräften zu decken und sucht zur Bekämpfung der Computer- und Internetkriminalität Absolventen mit einem Bachelor-Abschluss der Informatik, Physik, Mathematik oder vergleichbarer (informations-)technischer/naturwissenschaftlicher Fachrichtungen, die dann beispielsweise über Kenntnisse in den Bereichen praktischer Informatik, Scripting und Programmierung, Verschlüsselungstechnologien oder der Analyse und Abwehr von Netzwerkangriffen verfügen sollen.[22] In einer 20-monatigen Qualifizierungsmaßnahme werden die Teilnehmer in Theorie und Praxis für den gehobenen Kriminaldienst ausgebildet und durchlaufen dabei ein Einsatz- und Schießtraining, Schulungen im Bereich der Rechtswissenschaften, Kriminalwissenschaften, Dienstkunde und eine Sprachausbildung, begleitet von Praxiszeiten in den entsprechenden Fachabteilungen.[23] Das Aufgabenspektrum der Cyber-Kriminalisten umfasst in der späteren Verwendung die gesamte Bandbreite eigenständiger kriminalpolizeilicher Sachbearbeitung in den Fachabteilungen des BKA. Dazu zählen das Aufklären von Hackerangriffen, Betrugsdelikte im Internet und andere Computerstraftaten, forensische Ermittlung und Auswertung digitaler Spuren, Ermittlungen gegen organisierte Kriminelle oder Terroristen und Informationsauswertung und -analyse.[24] Eine vergleichbare Qualifizierungsmaßnahme gibt es in Baden-Württemberg, wo im April 2018 eine Sonderlaufbahn für den höheren Dienst der Cyberkriminalisten eingerichtet wurde, welche Beamten des gehobenen Dienstes der Cyberkriminalisten, die zusätzlich einen Masterabschluss in einer für den Bereich Cybercrime geeigneten Fachrichtung[25] erlangt haben, unter Erfüllung enger Voraussetzungen den Aufstieg in den höheren Polizeivollzugsdienst ermöglicht. Durch den Aufstieg können die Cyberkriminalisten in regionalen Polizeipräsidien als Referenten oder Leiter der Kriminalinspektion fungieren, im Landeskriminalamt die Leitung von Inspektionen im Bereich Cybercrime übernehmen oder an der HfPolBW als Dozent im Institutsbereich Cybercrime des Instituts für Fortbildung lehren.[26] Ergänzend zu den bisherigen Qualifizierungsmaßnahmen wird es ab dem Wintersemester 2020/2021 in der Ausbildung des gPVD einen Studienzug „IT-Ermittlungen/IT-Auswertungen“ geben, in welchem umfangreiche dv-technische Inhalte vermittelt werden, und der aufgrund der großen Nachfrage schon jetzt sicher zustande kommen wird. Auch in Sachsen wurde vor wenigen Jahren ein spezieller Ausbildungsgang geschaffen, der Absolventen mit einem Bachelor-Abschluss im IT-Bereich über einen zwölfmonatigen Vorbereitungsdienst den Einstieg im Bereich des Computer- und Internetkriminalitätsdienst des gehobenen PVD eröffnet.

4 Cybercrime in der Fortbildung der Polizei

Die Anforderungen an die Fortbildung der Mitarbeiter der Polizei ist sehr verschieden und abhängig von den Vorkenntnissen des Mitarbeiters und seinem Tätigkeitsbereich. In der Fläche sind Grundkenntnisse gefragt, während in den entsprechenden Abteilungen und Landeszentralen hoch spezialisierte Fachkräfte benötigt werden. Dies impliziert, dass es für den Kollegen auf der Straße ein anderes Angebot geben muss, als für den Cyberkriminalisten im Landeskriminalamt.

So vielseitig präsentieren sich auch die Angebote an Fortbildungen, die im Folgenden auszugsweise für einige Bundesländer einen kleinen Eindruck in das Engagement zur Bekämpfung des Cybercrimes geben soll.[27] In Hamburg wurden beispielsweise seit vergangenem Jahr zehn neue Fortbildungslehrgänge ins Leben gerufen, die zielgruppenspezifisch für die Schutzpolizei, Wasserschutzpolizei oder Kriminalpolizei angeboten werden. So werden die Mitarbeiter jährlich in rund 50 Lehrgängen unter anderem im Bereich Cybercrime, OSINT-Recherche und der Sicherung digitaler Spuren fortgebildet. In Bayern existiert seit 2014 ein umfassendes Aus- und Fortbildungskonzept im Bereich Cybercrime, für das federführend das Fortbildungsinstitut der Bayrischen Polizei (BPFI) zuständig ist, welches sich in engem fachlichem Austausch mit dem dortigen LKA befindet. Vom BPFI werden derzeit jährlich mehr als 30 Seminare angeboten, die durch vier Arbeitstagungen für die Leiter und spezialisierte Sachbearbeiter sowie ein E-Learning-Angebot und ein Infoportal ergänzt werden. Auch in Baden-Württemberg übernimmt das Institut für Fortbildung und hier speziell der Institutsbereich Cybercrime die Fortbildung, sowohl die der Spezialisten der regionalen Polizeipräsidien und des LKA, als auch die der Kollegen im Ermittlungsdienst der Schutz- und Kriminalpolizei, die zum Sachbearbeiter Cybercrime ausgebildet werden. Die Fortbildungsangebote können bei freien Kapazitäten auch von Kollegen aus

anderen Bundesländern oder Behörden, wie Zoll oder Finanzermittlern, kostenpflichtig besucht werden.

Erfreulich zu sehen ist die Tatsache, dass es länderübergreifende Maßnahmen gibt, die sich auch in der Fortbildung widerspiegelt. So wird beispielsweise im Rahmen einer Südschienenkooperation zwischen Baden-Württemberg, Rheinland-Pfalz, Hessen und dem Saarland, aber auch in der Sicherheitskooperation der Länder Brandenburg, Saschen-Anhalt, Berlin und den Freistaaten Sachsen und Thüringen im Bereich des Fortbildungsangebots kooperiert.

5 Fazit

Die zunehmende Digitalisierung wird sich auf die Kriminalitätsentwicklung im Bereich des Cybercrimes auswirken. Mit einer gewissen Spannung kann daher der Veröffentlichung der PKS für das Jahr 2020 entgegen geschaut werden, da die aufgrund der COVID-19-Pandemie gestiegene Nutzung digitaler Angebote erwarten lässt, dass es zu einem weiteren, möglicherweise sprunghaften Anstieg im Bereich der Computerkriminalität kommen wird. Hierbei ist nicht die Frage ob, sondern wie sehr der Einsatz privater digitaler, meist weniger geschützter Endgeräte im Homeoffice Kriminellen Tür und Tor geöffnet haben. Denn durch eine intensivere Nutzung des Internets und neue teilweise unerfahrene Nutzer, die erst aufgrund der besonderen Lage das Medium nicht nur zu Informationszwecken oder zum Zeitvertreib nutzen, sondern erstmals zum Onlineshopping, für Bankgeschäfte oder berufliche Zwecke, bietet kriminellen Akteuren mehr Möglichkeiten für ihre Aktivitäten.

Bei den Strafverfolgungsbehörden sollte sich das grundlegende Verständnis entwickeln, dass kein Mitarbeiter, vom Sachbearbeiter oder Kollegen im Streifendienst bis hin zur Führungskraft, um das Thema Cybercrime herumkommt, und die Kapazitäten zur Prävention und Aufklärung ausgebaut werden müssen. Das BKA hat im April 2020 mit der Einrichtung der Abteilung „Cybercrime“ beispielsweise einen wichtigen Schritt getan, um Kompetenzen zur Bekämpfung dieses Phänomens zu bündeln und eine erforderliche Spezialisierung der Mitarbeiter voranzutreiben.

Der Bedarf an (polizeilicher) Aus- und Fortbildung im Bereich der Ermittlungs-, Auswertungs- und Analysekompetenzen ist groß und wird weiter steigen. In einigen Bereichen sind bereits heute gute Grundlagen geschaffen, um die Mitarbeiter frühzeitig und nachhaltig zu schulen, und dadurch die digitalen Kompetenzen flächendeckend im Bereich des PVD zu stärken sowie Spezialisten zu qualifizieren. Bei einer strategischen Ausrichtung der Maßnahmen können als Ziele die Anpassung der Ausbildung der PVD und der Ausbau der spezifischen Fortbildungen festgezurrt werden. Hierfür dürften mit Hilfe von fachspezifischen E-Learning-Angeboten insbesondere bei der aktuellen Lage und der damit einhergehenden eingeschränkten Präsenzlehre Kapazitätsengpässe in der Aus- und Fortbildung kompensiert und durch die Kooperationen mit externen Hochschulen zumindest vorübergehend die benötigte Quantität und Qualität an Spezialisten für die Fortbildung gewonnen werden. So lässt sich konstatieren, dass sich auch hier aus der Krise eine Chance ergibt und die Aus- und Fortbildung in der Polizei eine Entwicklung nach vorn machen kann. Es bleibt spannend, diese Entwicklung zu beobachten und zu begleiten.

Anmerkungen

1. Gerrit Domenghino LL.M. ist Wissenschaftlicher Mitarbeiter im Fachgebiet III.[4] (Öffentliches Recht mit Schwerpunkt Polizeirecht) an der Deutschen Hochschule der Polizei in Münster.
2. Aus Gründen der besseren Lesbarkeit wird im Folgenden auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet und das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für jegliche Geschlechter.
3. Vgl. Manuskript der Rede von Innenminister Ralf Jäger am 10.3.2014 in Düsseldorf anlässlich der Vorstellung der Polizeilichen Kriminalstatistik 2013, S 6, online verfügbar unter: docplayer.org/30855976-Rede-von-innenminister-ralf-jaeger-am-10-maerz-in-duesseldorf-anlaesslich-der-vorstellung-der-polizeilichen-kriminalstatistik-2013.html
4. Kommune[21], IT-Sicherheit: Was Behörden beachten müssen, wenn sie Mitarbeiter ins Homeoffice schicken, 9/2020, S. 26f.
5. Vgl. PKS 2019. S. 183.
6. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
7. Vgl. Bitkom online, Pressebereicht vom 21.7.2017, online verfügbar unter: www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html.

8. Vgl. PKS 2018, S. 45.
9. Siehe Fn. 7.
10. Vgl. Förderungspapier der GdP NRW zur Bekämpfung Cybercrime, Januar 2019, online verfügbar unter: www.gdp.de/gdp/gdpnrw.nsf/id/DE_Computer-Profis-dauerhaft-an-die-Polizei-binden/$file/Bekaempfung_Cybercrime.pdf.
11. An der Hochschule Wismar kann im Fernstudium ein Bachelor-Abschluss im Bereich IT-Forensik erlangt werden. Des Weiteren bietet die Hochschule ebenfalls im Fernstudium ein Master-Studiengang „IT Sicherheit und Forensik“ an, der als berufsbegleitendes Studienangebot konzipiert ist und die Studierenden dazu befähigen soll Sicherheitsaspekte zu bewerten und technisch-organisatorische Maßnahmen gegen Cyber-Angriffe einzuleiten.
12. Die Hochschule Mittweida bietet einen konsekutiven viersemestrigen Master-Studiengang an. Durch die Auswahl von Qualifizierungslinien kann entweder der Schwerpunkt „Cybercrime“ oder „Cybersecurity“ gesetzt werden, um sich für eine später eigenständige Tätigkeit in hochspezialisierten Cybercrime oder IT-Forensik-Abteilungen in Ermittlungsbehörden, Bundesbehörden oder einem privatwirtschaftlichen Unternehmen zu qualifizieren.
13. Eine LVS entspricht 45 Minuten.
14. Die folgenden Informationen stammen aus der Beantwortung einer Anfrage an die HSPV NRW.
15. Die folgenden Informationen stammen aus der Beantwortung einer Anfrage an die Hochschule für Polizei Baden-Württemberg bzgl. der Aus- und Fortbildung im Bereich „Cybercrime“.
16. Bei dem E-Mail-Header handelt es sich um die Kopfzeile einer E-Mail, aus der Informationen zum Empfänger, Absender sowie der IP-Adresse des Absenders entnommen werden können, die sonst nicht sichtbar sind.
17. Zum Vorstehenden vgl. Modulhandbuch für den Studiengang „Bachelor of Arts (B.A.) - Polizeivoll-zugsdienst“ im 28. Studienjahrgang, S. 123 f., online verfügbar unter: www.polizei.sachsen.de/de/dokumente/PolFH/2020X09X14XMHBXX28XXStjg.pdf.
18. Die Geschichte des Bundeskriminalamtes, 2000-2009, online verfügbar unter: www.bka.de/DE/DasBKA/Historie/GeschichteDesBKA/geschichteDesBKA_node.html.
19. Zum vorstehenden vgl. Bundeskriminalamt, Modulhandbuch für den Bachelorstudiengang (B.A.), Kriminalvollzugsdienst im Bundeskriminalamt, S. 66ff., online verfügbar unter: www.bka.de/SharedDocs/Downloads/DE/KarriereBeruf/FHBWiesbaden/ModulhandbuchBachelorstudiengang.pdf.
20. Vgl. dazu auch Zwick, Die Kriminalpolizei, 3/2020, S. 34.
21. Vgl. HfPV Hessen, Modulbuch für den Studiengang Bachelor of Arts “Kriminalpolizei” Vertiefungsrichtung „Cyberkriminalistik“, S. 46ff., online verfügbar unter: www.hfpv.de/sites/default/files/public-type-files/01_Modulbuch_Cyberkriminalistik_v10_WZ_0.pdf.
22. Vgl. Bundeskriminalamt, Flyer Cyber-Kriminalist/-in im gehobenen Kriminaldienst des BKA, online verfügbar unter: www.polizei.de/SharedDocs/Downloads/DE/KarriereBeruf/FlyerCyberKriminalist/180223FlyerCyberKriminalist.html.
23. Ebd.
24. Die Geschichte des Bundeskriminalamtes, 2010-2019, online verfügbar unter: www.bka.de/DE/DasBKA/Historie/GeschichteDesBKA/geschichteDesBKA_node.html.
25. Z.B. Masterstudiengang „Digitale Forensik“ an der Hochschule Albstadt-Sigmaringen.
26. Vgl. Internetpräsenz der Polizei Baden-Württemberg, online verfügbar unter: sonderlaufbahnen.polizei-bw.de/cyberkriminalist-in/.
27. Die folgenden Informationen stammen aus der Beantwortung von Anfrage an die entsprechenden Behörden bzgl. der Aus- und Fortbildung im Bereich „Cybercrime“.