Technologiegetriebene Polizeiausbildung im Umgang mit Digitalen Spuren

Wilfried Honekamp, Roman Povalej, Heiko Rittelmeier, Johannes Fähndrich, Silvio Berner und Dirk Labudde

Inhalt

W. Honekamp (✉)
Hochschule Stralsund, Stralsund, Deutschland
E-Mail: wilfried.honekamp@hochschule-stralsund.de

R. Povalej
Polizeiakademie Niedersachsen, Hann. Münden, Deutschland
E-Mail: roman.povalej@polizei.niedersachsen.de

H. Rittelmeier
Zentrale Stelle für Informationstechnik im Sicherheitsbereich, München, Deutschland
E-Mail: heiko@rittelmeier.de

J. Fähndrich

E-Mail: johannesfaehndrich@hfpol-bw.de

S. Berner
Hochschule der Sächsischen Polizei (FH), Rothenburg O.L., Deutschland
E-Mail: Silvio.Berner@polizei.sachsen.de

D. Labudde
Hochschule Mittweida, Mittweida, Deutschland
E-Mail: dirk.labudde@hs-mittweida.de

T.-G. Rüdiger, P. S. Bayerl (Hrsg.), *Handbuch Cyberkriminologie*,
https://doi.org/10.1007/978-3-658-35450-3_51-1

Zusammenfassung

Digitale Spuren müssen von gut ausgebildeten Polizistinnen und Polizisten erkannt, vor Veränderung geschützt sowie gesichert und ausgewertet werden. Sie sollten also wissen, in welchen Zusammenhängen welche Spuren entstehen, wie diese zu finden sind und wie diese beweiskräftig gesichert werden können. In diesem Kapitel wird anhand von Basiskompetenzen gezeigt, welcher Rahmen derzeit in den Bundesländern für eine entsprechende Lehre im Polizeistudium zur Verfügung steht. Anschließend wird die notwendige Anpassung der Lehre an den ständigen technischen Wandel beschrieben.

Schlüsselwörter

Crime Potential Cycle · Cyberkriminalität · Cyberkriminologie · Digitale Spuren · Technologiegetriebene Polizeiausbildung

1 Einleitung

Die Digitalisierung schreitet stetig voran und bringt dadurch auch immer neue Formen von Cyberkriminalität und Digitalen Spuren hervor. Cyberkriminalität kann aus verschiedenen Perspektiven betrachtet werden. Mögliche Sichtweisen sind die Perspektiven der Täter, der Opfer, der Bevölkerung und der ermittelnden Behörden. In diesem Kapitel soll die Perspektive der ermittelten Behörden in Bezug auf Digitale Spuren und der Zusammenhang zu Straftatbeständen und Tatbestandsmerkmalen genauer untersucht werden.

Digitale Spuren müssen von gut ausgebildeten Polizistinnen und Polizisten erkannt, vor Veränderungen geschützt sowie gesichert und ausgewertet werden. Sie sollten also wissen, in welchen Zusammenhängen welche Spuren entstehen, wie diese zu finden sind und wie sie beweiskräftig gesichert werden können. Anschließend müssen die Spuren so aufbereitet werden, dass sie vor Gericht als Beweismittel dienen können. Es ist also Aufgabe der Polizeiausbildung, entsprechende Kompetenzen zu vermitteln.

Die Geschichte in der Kriminalistik zeigt das Wechselspiel zwischen Kriminellen und ermittelnden Behörden deutlich. Beide Seiten dieser Interaktion beeinflussen sich gegenseitig und bewegen sich entlang einer Spirale. Die Interaktionen lassen sich in Anlehnung an das dritte Newtonsche Gesetz mit dem Konstrukt *actio et reactio* sehr gut beschreiben (Newton, 1739, S. 23). Das Wechselspiel basiert auf Technologien, die oft für andere Anwendungen kreiert und genutzt wurden. Beispiele hierfür wären die Fotografie, Drohnen und virtuelle Währungen. Die meisten Technologien besitzen ein sogenanntes *Dual Use Potential*, können also sowohl für nützliche als auch schädliche Zwecke eingesetzt werden (Brundage et al., 2018) und bestimmen nicht zuletzt die Interaktionen der Opfer und Täter. Technische Entwicklungen sind gerade im Bereich Cyberkriminalität Treiber dieser Interaktionen. Die Aus- und Fortbildung in den Ermittlungsbehörden sollte daher die Trends und

Neuentwicklungen von Technologien direkt aufgreifen und mögliches Gefährdungspotential und Risiken analysieren und bewerten. In diesem Kapitel widmen wir uns den folgenden beiden Fragen:

- Ist die Ausbildung der Polizeien der Länder gerade im Bereich Cybercrime zeitgemäß?
- Muss sich die Ausbildung in Zukunft am *Dual Use Potential* neuer Technologien ausrichten?

Grundlage für das in diesem Kapitel modellierte Vorgehen und die Abschätzung des neu zu definierenden *Crime Potentials* und des *Crime Potential Cycles* ist der *Gartner Hype Cycle* (Chen & Han, 2019) vermischt mit den Erfahrungen, wie technische Lösungen eine Entwicklung in S-Kurven durchlaufen (Brown, 1992).

2 Cybercrime und Perspektiven

Kriminalität ist ein hochkomplexes Gebilde unter Beteiligung verschiedener Akteure. In der Kriminologie werden oft die Perspektiven und die Interaktion von Tätern und Opfern in den Mittelpunkt gestellt. Kriminalität ist jedoch ein gesellschaftliches Phänomen und bedarf daher auch einer gesellschaftlichen und individuellen Einordnung. Diese kann durch eine Reduzierung auf das Mikro-Makro-Problem (Trültzsch, 2009) erfolgen. Im Phänomen Kriminalität treten die Akteure Täter, Opfer und die Gesellschaft als Beobachter auf. Kontrollparameter sind zum einen Norm- und Moralauffassungen, aber auch der Einsatz neuer Technologien zur Kriminalitätsbekämpfung und zur Begehung von Straftaten. Kontrollparameter und Akteure haben einen Einfluss auf die Struktur und Organisation (Begehungsweisen und Anzahl) von Kriminalität. Verschiebungen in der Organisation und Struktur wirken wiederum auf die Akteure zurück (Ludwig & Labudde, 2021).

In der Kriminologie sind Opfer Personen, die im Verlauf eines Verbrechens im weitesten Sinne oder eines eingetretenen Ereignisses geschädigt wurden, d. h. in ihren Rechten physisch, psychisch oder materiell verletzt wurden (siehe auch Feltes & Kerner, 2015 sowie Feltes, 2003). Auf der anderen Seite haben wir die Täter, die eine Straftat begehen. Das Strafgesetzbuch unterscheidet zwischen unmittelbarem Täter, mittelbarem Täter (§ 25 Absatz 1 StGB) und Mittäter (§ 25 Absatz 2 StGB). Das BKA (2015) beleuchtet in seiner Studie „Täter im Bereich Cybercrime“ Täter bzw. betrachtet täterspezifische Erkenntnisse in der Cyberkriminalität bzw. Cybercrime im engeren Sinne. Die Studie weist darauf hin, dass junge Täter häufig vorgefertigte Angriffswerkzeuge einsetzen (im Sinne von Testen), da sie nicht das erforderliche Wissen haben, um selbst welche zu entwickeln. Zudem können anhand der Tätertypologien unterschiedliche Präventionsmaßnahmen abgeleitet werden. Wie Abb. 1 verdeutlicht, stehen Täter und Opfer im Bereich Cybercrime durch die Technologie in einem engen Zusammenhang. Die Blickrichtung der Opfer und Täter auf diese Technologien ermöglicht einen Einstieg in das Gebiet der Cyberkriminologie.

Nach der Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20. Mai 2021 werden „Güter einschließlich Datenverarbeitungsprogramme

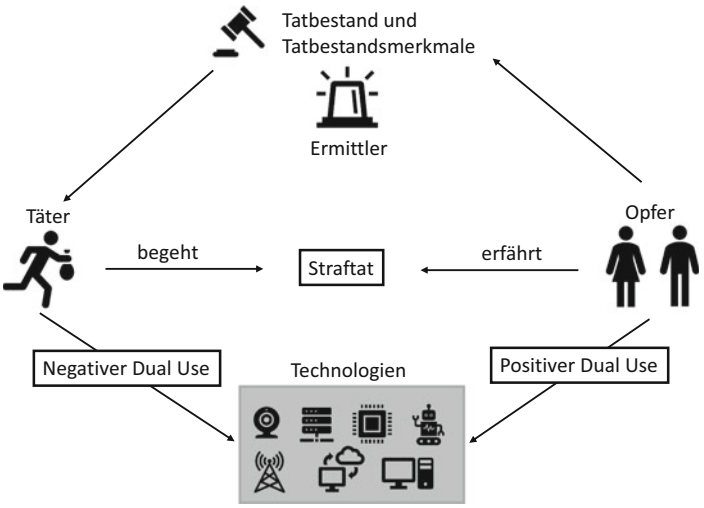

Abb. 1 Sichtweisen der Akteure auf Technologien und der Möglichkeit als Täter eine Straftat zu begehen bzw. als Opfer zu erfahren. Durch die juristische Bewertung von Tatbestandsmerkmalen und dem Straftatbestand auf der Basis von Beweisen aus analogen und digitalen Spuren wird ein Urteil gefällt

(Software) und Technologie, die sowohl für zivile als auch für militärische Zwecke verwendet werden können", als „Güter mit doppeltem Verwendungszweck" bezeichnet (EP & ER, 2021, L 206/6). Das Robert Koch Institut (RKI, 2013) versteht unter der Dual-Use-Problematik „die grundsätzliche Gefahr, dass Erkenntnisse der Lebenswissenschaften missbraucht und zum Schaden von Gesellschaft und Umwelt eingesetzt werden können". Allgemein wird in der Literatur unter *Dual Use* der doppelte Verwendungszweck verstanden, konkret wenn eine Verwendung als sozial nützlich und die Alternative als sozial schädlich zu verstehen ist.

Entsprechend können auch Konzepte, Modelle, Software, Technologien und Werkzeuge wie zum Beispiel Smartphones, *Internet of Things* oder Cloud-Lösungen für kriminelle Zwecke missbraucht werden. Für die Abschätzung eines *Crime Potentials* von neuen Technologien ist deshalb die Betrachtung und Bewertung des jeweiligen *Dual Use Potential* bzw. der *Dual Use Probability* innerhalb der Cyberkriminologie überaus wichtig. Unter dem negativen *Dual Use Potential* bzw. der *Dual Use Probability* verstehen wir im Kontext der Cyberkriminologie das Potential bzw. die Wahrscheinlichkeit des Missbrauchs einer Technologie für kriminelle Zwecke. In diesem Kapitel konzentrieren wir uns auf das Potential, da die Daten für die Ermittlung der Wahrscheinlichkeit bisher noch nicht erhoben wurden.

Ein einfaches Beispiel hierfür sind drahtlos nutzbare Zugangsberechtigungen, wie zum Beispiel die Keyless-Go-Systeme in Fahrzeugen. Für den Benutzer ergeben sich durch derartige Techniken erhebliche Komfortvorteile: der Kofferraum öffnet sich, wenn man von hinten an das Fahrzeug tritt; der Schlüssel muss nicht mehr in das Zündschloss gesteckt werden, sondern kann in der Hosentasche bleiben. Die

Berechtigung zum Öffnen des Fahrzeugs und Starten des Motors wird über den Austausch von kryptografisch gesicherten Datenpaketen auf Basis von Kurzstreckenfunktechniken geprüft. Ein wichtiger Sicherheitsaspekt ist also die direkte Nähe derartiger Schlüssel zum jeweiligen Fahrzeug.

Nach nicht allzu langer Zeit haben auch die Kriminellen das Potential dieser Technik erkannt. Musste man vorher noch versuchen, in den Besitz des Fahrzeugschlüssels zu kommen (oder alternativ teilweise erhebliche Beschädigungen an den Fahrzeugen in Kauf nehmen), so konnte man nach der Adaption der neuen Technologie Fahrzeuge unter Nutzung von Systemen zur Funkstreckenverlängerung unversehrt entwenden. In der praktischen Nutzung stehen jetzt Täter an der Hauswand in der Nähe des (im Haus befindlichen) Schlüssels und andere starten das Fahrzeug, das vor dem Haus außerhalb der eigentlichen Reichweite des Schlüssels abgestellt wurde. Die notwendigen Funksignale werden zwischen den beiden Tätern über eine andere Funktechnik übertragen und damit verlängert. Das einzige Problem der Täter ist, dass sie verhindern müssen, dass der Motor des Fahrzeugs bis zum Erreichen des Ziels neu gestartet werden muss. Um den Blickwinkel der ermittelnden Behörden im Umfeld der Cyberkriminologie einnehmen und den Einfluss neuer Technologien abschätzen zu können, muss ein Perspektivwechsel erfolgen. Dieser muss mit der Aus- und Fortbildung in den Polizeien der Länder beginnen.

3 Anforderungen an die Ausbildung im polizeilichen Umgang mit Digitalen Spuren

Honekamp (2018, S. 57) fordert zur „Bekämpfung von Cybercrime eine Grundqualifizierung des Personals in der Fläche“. Die Anforderungen an den Umgang mit Digitalen Spuren im Rahmen polizeilicher Ermittlungen werden bei Kunze (2018) beschrieben. Dieser bezieht sich auf einen Workshop an der Deutschen Hochschule der Polizei zu den Basiskompetenzen Cybercrime und Digitale Spuren, die aus Sicht von Fachpersonal aus den Bereichen „Wachdienst, IUK-Ermittlungsunterstützung, Ermittlungsdienst, Ausbildung/Fortbildung und Verkehrsunfallaufnahme“ (ebenda, S. 172) „unabhängig von der Verwendung [. . .] erforderlich sind“ (ebenda, S. 161). Cybercrime und Digitale Spuren stehen demnach „an einer Schwelle, Teile der klassischen Kriminalität und Spurenlage zu ersetzen, diese zu erweitern und eine gleichartige Bedeutung [. . .] zu erlangen“ (ebenda, S. 164). In diesem Beitrag soll auch diskutiert werden, ob diese Schwelle bereits überschritten ist. Kunze (2018, S. 168) weist darauf hin, dass der Status Quo bis auf wenige Ausnahmen eine Einheitsausbildung ist. Am Beispiel Nordrhein-Westfalen wird beschrieben, dass in 88 Präsenzlehreinheiten ganze 16 Kompetenzfelder ausgebildet werden, von denen Kriminalität im Bereich der Informations- und Kommunikationstechnologie nur eines darstellt. Der Schwerpunkt liegt dort auf dem analogen Spurenschutz.

In Niedersachsen soll es „eine polizeiliche Gesamtstrategie“ (ebenda, S. 178) zu den Basiskompetenzen geben. Hier wird wahrscheinlich auf das Aus- und Fortbildungskonzept Cybercrime verwiesen, das bei Herbst (2017) vorgestellt wird. Seit 2008 folgt die Polizei Niedersachsen einer neuen strategischen Ausrichtung, um dem

Gefahrenpotential aus dem Deliktsfeld Cybercrime und den damit einhergehenden polizeilichen Herausforderungen adäquat zu begegnen. Entsprechend wird den zentralen und dezentralen Fortbildungen im Deliktsfeld Cybercrime eine hohe Bedeutung beigemessen. Dieses Konzept wird regelmäßig fortgeschrieben und beinhaltet inzwischen eine fünfstufige, aufeinander aufbauende Struktur für die fünf Zielgruppen (1) Ersteinschreitende, (2) Sachbearbeitende Cybercrime im weiteren Sinne, (3) Sachbearbeitende Cybercrime im engeren Sinne, (4) IT-Spezialistinnen und -Spezialisten sowie (5) Sachbearbeitende DV-Gruppen (IT-Forensiker).

Die Hauptaufgabe der Ersteinschreitenden, d. h. der Polizisten bzw. Polizistinnen, die als erstes vor Ort am Tatort sind, ist die vorliegende Spurenlage vor Veränderungen zu schützen. Sollten aber Veränderungen vorgenommen werden müssen (Absperrung, Eigensicherung, Versorgung von Verletzten usw.), so sind diese im Nachgang zu dokumentieren. Dafür brauchen sie aber Kenntnisse, wo sich Spuren befinden könnten, um diese nicht unbewusst und versehentlich zu verändern oder gar zu vernichten. Die Aufgabe von Ermittelnden besteht darin, Täter nach einer Straftat zu überführen. Sie befragen Opfer, Zeugen sowie Beschuldigte und tragen Spuren sowie Beweismittel zusammen, die aufzunehmen, zu analysieren und zu bewerten sind. Fehler, die in diesem Kontext gemacht werden, sind später – wenn überhaupt – nur sehr schwer auszugleichen.

Unsere Hypothese ist, je mehr Kenntnisse die beiden Gruppen darüber haben, wo sich Digitale Spuren befinden könnten, desto besser können sie ihre Aufgaben erledigen. Teil davon ist zu wissen, welche Technologien für kriminelle Zwecke missbraucht werden können. Ziel dieses Kapitels ist, das *Dual Use Potential* bzw. den hier vorgestellte *Crime Potential Cycle* zu nutzen, um die Polizeiarbeit zu unterstützen. Das heißt, unser Ziel ist es, dass die neuen Erkenntnisse des *Crime Potential Cycle* schnellstmöglich ihre Anwendung in der Aus- und Fortbildung der Polizeien finden. Möglicherweise kann so gewährleistet werden, dass Ersteinschreitende und Ermittelnde frühzeitig dieses Wissen erlangen.

Grundsätzlich ist aus Sicht der Autoren eine Differenzierung von Cybercrime im ‚engeren' und ‚weiteren' Sinn nicht mehr zeitgemäß und sollte künftig entfallen. Gemäß der Definition aus dem „Bundeslagebild Cybercrime 2020" des BKA (2021, S. 42) handelt es sich bei *Cybercrime im weiteren Sinn* um „Straftaten, die unter Nutzung von Informationstechnik begangen werden (Tatmittel Internet)". Wie unzweckmäßig diese Unterscheidung ist, soll folgendes Beispiel zeigen: ein Mensch schickt einem anderen einen Brief und droht ihm, ihn umzubringen. Schreibt er den Brief mit der Hand, so handelt es sich um klassische Kriminalität. Schreibt er den Brief am Rechner und druckt ihn aus, so gehört die Tat zu ‚Cybercrime im weiteren Sinn'. Die Unterscheidung der Delikte – und in der Praxis auch teilweise der Zuständigkeit innerhalb der Polizei – findet also im Bereich Cybercrime anhand des Modus Operandi statt. Ob dieser zur Differenzierung geeignet ist, erscheint den Autoren stark zweifelhaft.

Die Unterscheidung zwischen ‚engerem' und ‚weiterem' Sinn diente bei ihrer Einführung ursprünglich dazu, neue Begehungsweisen im Hinblick auf neuartige Spuren und geänderte Ermittlungserfordernisse von herkömmlicher Kriminalität abzugrenzen und hatte ihren Sinn darin, die Aufmerksamkeit vor allem von Justiz

und Politik zu wecken, um auf die technologischen Entwicklungen durch geänderte Verfahrensregeln in den justiziellen Vorgängen, Gesetzesänderungen und Anpassungen innerhalb der Polizei reagieren zu können (z. B. durch gezielte Einstellung von Fachpersonal und Anpassung der Aus- und Fortbildung). Zwischenzeitlich ist jedoch die Technologie in all ihren Erscheinungsformen integraler Bestandteil des täglichen Lebens geworden und muss auch von allen Beteiligten an der Strafverfolgung umfänglich beherrscht werden. Es gibt in der Praxis so gut wie keine Delikte mehr, in denen Technologie überhaupt keine Rolle spielt. Damit muss auch fast zwangsläufig die Erwartungshaltung einhergehen, dass die Bearbeitung von Delikten mit einem derartig hohen Verbreitungsgrad nicht mehr auf Fachleute beschränkt sein kann, sondern dass Alltagskriminalität von jedem Polizisten kompetent aufgenommen und bearbeitet werden muss. Die Autoren gehen daher davon aus, dass der Umgang mit Technologien alltäglich ist und dass jede Person ihn beherrschen muss. Wenn quasi jede Straftat auch als ‚Cybercrime im weiteren Sinn' verstanden werden kann, dann ist der Begriff als Entscheidungskriterium für Zuständigkeiten und insgesamt als Ordnungsmerkmal obsolet geworden.

Kunze (2018, S. 169) blickt auch nach Europa und verweist auf einen „Best-Practice-Leitfaden für den Umgang mit Digitalen Spuren" (Williams, 2012), der in Großbritannien und Irland Anwendung findet, und auf die *European Cybercrime Education and Training Group*, mit der die Europäische Union den Mitgliedsstaaten Fortbildungen anbietet (ECTEG, 2021). Ein Verweis auf das internationale Ausbildungskooperationsprogramm *Nordic Computer Forensic Investigators* der Polizeihochschule Norwegens fehlt allerdings. Hier werden Fortbildungsprogramme und -kurse zum Umgang mit Digitalen Spuren angeboten. Partner sind neben Norwegen, Schweden, Finnland und Dänemark auch die Baltischen Staaten, Polen und Deutschland (Herbst, 2017; Honekamp, 2018; Jahren, 2020; Politihogskolen, 2021).

Als Ergebnis werden in Kunze (2018, S. 172) die folgenden im Workshop identifizierten Fähigkeiten und Kenntnisse der Basiskompetenzen „für die Ermittlung der Tätigkeiten zur Bekämpfung von Cybercrimedelikten und zum Umgang mit Digitalen Spuren" beschrieben:

- Sicherstellung von Hardware, flüchtigen Daten, Videos und Fahrzeugdaten
- Auswertung von Daten
- Recherche im Internet, speziell in Sozialen Netzwerken
- Auskunftsersuchen

Darüber hinaus wurden folgende spezifische Technologien identifiziert, bei denen der Umgang mit Digitalen Spuren bekannt sein müsste:

- Mobilfunkgeräte
- Telematik-/Telemetriesysteme
- Smart Home
- Cloud/Netzwerke

- Verschlüsselung
- Radio Frequency Identification

Als spezielle Delikte, auf die unter anderem auch in der Anzeigenaufnahme vorzubereiten ist, wurden genannt:

- Identitätsdiebstahl
- Call-ID-Spoofing
- Hacking/Phishing

Zeitansätze für die Ausbildung zu den einzelnen Aspekten wurden nicht erarbeitet bzw. empfohlen. Abschließend wird kritisiert, dass aus diesen identifizierten notwendigen Fähigkeiten in einigen Bundesländern keine Gesamtstrategie oder zumindest Fachstrategie abgeleitet wird. Positiv wird erwähnt, dass 2017 in Nordrhein-Westfalen fünf Modulbausteine zu Cybercrime und Digitalen Spuren in die Einführungsfortbildung aufgenommen wurden.

Als Schlussfolgerung wird gefordert, die dargestellten Basiskompetenzen in eine umfängliche Ausbildung zu überführen: „Die entsprechende Vermittlung sollte den erforderlichen Rahmen erhalten“ (Kunze, 2018, S. 178). In der Folge muss sich auch die polizeiliche Lehre mit den Technologien und ihren Auswirkungen auf die tägliche Arbeit in der Strafverfolgung auseinandersetzen und mit Anpassungen an den vermittelten Inhalten reagieren. Die Bedeutung der Technologie für das tägliche Leben aller Bürger (und damit einhergehend die Nutzung der Technologie für die Begehung von Straftaten) muss sich auch in der polizeilichen Lehre widerspiegeln. Die Auswertung der derzeitigen Zeitansätze für diese Inhalte legt einen deutlichen Nachbesserungsbedarf nahe. Im folgenden Abschnitt soll nun geprüft werden, inwieweit die Bundesländer diesen Rahmen in der Ausbildung geschaffen haben.

4 State of the Art der Ausbildung im Polizeistudium der Länder

Der Fokus liegt bei dieser Untersuchung auf dem ersten Einsatz vor Ort und auf der Anzeigenaufnahme, d. h. die weitere Ermittlungsarbeit wird nicht betrachtet. Dazu wird ausschließlich die Lehre in Pflichtfächern im Studium ausgewertet, da diese vergleichbar ist und nach erfolgreichem Abschluss zum Einsatz als Polizeibeamtin bzw. Polizeibeamter berechtigt. Da nicht in jeder Landespolizei eine Ausbildung im Mittleren Dienst angeboten wird, werden diese Anteile nicht betrachtet. Auch Wahlpflichtfächer wurden ausgenommen, da nicht garantiert werden kann, dass die aufnehmenden Beamten in den entsprechenden Sachverhalten ausgebildet wurden. Die Betrachtung beschränkt sich also auf die Studieninhalte, welche alle Studierenden durchlaufen müssen, um nach ihrem Abschluss als Polizeibeamtin bzw. Polizeibeamter eingesetzt zu werden. In einigen Bundesländern wird ein angepasstes Studium für Studierende mit Vordienstzeit angeboten. Dieses Aufstiegsstudium wird im Rahmen dieser Untersuchung genauso wenig betrachtet wie Studiengänge

für Kriminalistik oder deren Vertiefungen/Spezialisierungen bzw. Vertiefungen/Spezialisierungen in IT-Forensik oder Cybercrime. Ferner wurden aus Gründen der Vergleichbarkeit nur die Präsenzstunden bewertet. Eine Diskussion über den notwendigen Anteil von Selbststudium in einem wissenschaftlichen Studium soll hier vermieden werden. Darüber hinaus war nicht immer eine klare Trennung zwischen rechtlichen Grundlagen und deren Anwendung auf Digitale Spuren möglich. Hier wurde mit prozentualen Annahmen und Erfahrungswerten gearbeitet.

Zur Auswertung wurden die aktuell zugänglichen Modulhandbücher und Studienpläne aller 16 Bundesländer genutzt. Dabei fiel auf, dass nicht alle Hochschulen die Modulhandbücher bzw. Studienpläne transparent auf ihrer Webseite darstellen. Teilweise mussten die Unterlagen mit besonderem Nachdruck erfragt werden. Auch die Frage, inwieweit Wissenschaft Transparenz bedingt, soll hier nicht weiter diskutiert werden. In den Modulhandbüchern wurde nach den Begriffen „computer“, „iuk“, „internet“, „cyber“ und „digital“ gesucht, und es wurden die entsprechenden Module identifiziert und ausgewertet.

Als relevant für den ersten Einsatz vor Ort wurde dabei neben den oben beschriebenen Basisfähigkeiten der Punkt „Sicherstellung von Hardware, flüchtigen Daten, Videos und Fahrzeugdaten“ betrachtet, der bei Kunze (2018) noch durch die „Datenerhebung vor Ort“ („Fotografie, Fachleute/Admin vor Ort einbinden, Software mit sichern, Speicherfristen feststellen, Sicherungsmedien abstimmen“) und den „Fernzugriff“ („Möglichkeiten für Polizei und Täter kennen, Flugmodus, PIN/Entsperrcode erfragen“) konkretisiert wird. Die anhand dieser und der o. g. Kompetenzen in den Modulhandbüchern identifizierten Lehreinheiten (LE) von 45 Minuten werden in Tab. 1 dargestellt. Dabei werden für jedes Bundesland die Lehrveranstaltungen als Untergliederungen der Module genannt, in denen von einer Berücksichtigung der Inhalte ausgegangen werden kann.

Die Spannweite der Dauer, mit der die Basiskompetenzen nach Kunze (2018) in der Lehre im Polizeistudium berücksichtigt werden, reicht von 7 (Sachsen-Anhalt) bis 105 (Saarland) LE. Auf der einen Seite bedeutet dies, dass nicht auszuschließen ist, dass einige Polizistinnen und Polizisten, die nach dem jeweiligen Beamtenrecht der Bundesländer in geeigneter Weise ausgebildet sind, um in das Einstiegsamt eingewiesen werden zu können, nicht in der Lage sein können, einen Tatbestand im Zusammenhang mit Digitalen Spuren umfassend korrekt aufzunehmen. Auf der anderen Seite sind die Ausbildungs- und Einsatzkonzepte der Länder aber auch so unterschiedlich, dass hier nicht mit Sicherheit gesagt werden kann, dass diese Berufsanfänger auch gleich für diese Aufgabe eingesetzt werden. Vielmehr gibt es in diversen Ländern verpflichtende Fortbildungen im Anschluss an das Studium. Auch gibt es eine Spezialistenausbildung und Wahlangebote, die begünstigen, dass sich vornehmlich diese im Umgang mit Digitalen Spuren gut ausgebildeten Fachleute mit den o. g. Tatbeständen befassen. Im Rahmen dieser Untersuchung sei aber darauf hingewiesen, dass die Geschädigten keine Garantie bekommen, dass gerade diese Fachleute auch zur Verfügung stehen. Es ist also in einigen Bundesländern nicht ausgeschlossen, dass die aufnehmende Person doch nur über die Grundfertigkeiten aus dem Studium verfügt. Nach Erfahrung der Autoren ist es durchaus üblich, dass Berufsanfänger in der Fall- bzw. Anzeigenaufnahme eingesetzt werden.

Tab. 1 Darstellung der Inhalte und deren Umsetzung in LE in den Bundesländern

Bundesland	Lehrveranstaltungen	LE
Baden-Württemberg	• Informationstechnische Grundlagen polizeilichen Handelns und Entscheidens	48
Bayern	• Soziale Netzwerke/Cybercrime • Polizeiliches Einsatzverhalten • IT-Grundlagen	31
Berlin	• Informations- und Kommunikationstechnik	34
Brandenburg	• Cybercrime • Polizeiliche Standardsituationen II	21
Bremen	• Digitale Spuren und Datenschutz • Cybercrime • IT-Forensik • Datenschutzrecht	45
Hamburg	• Grundlagen der Informations- und Kommunikationstechnik • Cybercrime	88
Hessen	• Ermittlungsverfahren, Teilmodul 1 • Besondere Kriminalitätsphänomene und ihre eingriffsrechtliche Bewältigung • Informationstechnik	80
Mecklenburg-Vorpommern	• Cybercrime • Rechtsgrundlagen IV	70
Niedersachsen	• Digitale Spuren • IuK-Kriminalität • Grund- und Intensivkurs Cybercrime Ersteinschreiter • Training zum Grund- und Intensivkurs Cybercrime Ersteinschreiter	34
Nordrhein-Westfalen	• Anzeigenaufnahme und Erster Angriff der IuK-Kriminalität • Cybercrime • Straftaten in besonderen Kriminalitätsbereichen	15
Rheinland-Pfalz	• Computerkriminalität • Cybercrime und Digitale Ermittlungen • Die Bedeutung des Internet für polizeiliche Ermittlungen • Eingriffsrechtliche Grundlagen und Befugnisnormen im Rahmen von grenzüberschreitenden Maßnahmen auch im Kontext von Internetkriminalität • Grundlagen der Kriminalistik und Grundlagen der Körperverletzungs- und Tötungsdelikte • Grundlagen der Internetaufklärung • Grundlagen der technischen Funktionsweise des Internet • Kontrollen im öffentlichen Verkehrsraum • Verkehrsunfallaufnahme, Teil II • Prävention im Zusammenhang mit dem Internet • Ermittlungsmaßnahmen mit TK-Bezug	88
Saarland	• Seminar „Cybercrime“ • Praxiskunde	105
Sachsen	• Straftaten im Zusammenhang mit dem Internet • Kriminaltechnik	32
Sachsen-Anhalt	• Besondere Straftatbestände	7
		92

(Fortsetzung)

Tab. 1 (Fortsetzung)

Bundesland	Lehrveranstaltungen	LE
Schleswig-Holstein	• Straftaten gegen das Vermögen • Cybercrime • Todesermittlungen, Vermisstensachen und Kapitaldelikte • Ermittlungen bei Delikten gegen die sexuelle Selbstbestimmung • Aufnahme schwerer Unfälle • Schwere und Organisierte Kriminalität; Fälschungsdelikte • Grundlagen Cybercrime • Ersteinschreiter Cybercrime	
Thüringen	• Spezielle Deliktsbearbeitung, Teil 1 • Spezielle Kriminalistik, Teil 1	18

Die Auswertung hat weiter ergeben, dass die Herangehensweise an die Lehre in den Basiskompetenzen in den Bundesländern völlig unterschiedlich ist. Während es in einigen Bundesländern große Blöcke gibt (Saarland, Baden-Württemberg), sind die Lehrinhalte in anderen auf viele Lehrveranstaltungen aufgeteilt (Bremen, Rheinland-Pfalz, Schleswig-Holstein). Mit den Vor- und Nachteilen dieser verschiedenen Ansätze soll sich in diesem Kapitel nicht befasst werden.

Auch die Einordnung der Lehre zu den Basiskompetenzen ist in den Bundesländern unterschiedlich. Während die Lehre in Baden-Württemberg, Hamburg, Hessen und Niedersachsen durch Professoren (in der Regel im Bereich der Informatik bzw. verwandter Disziplinen) verantwortet wird, sehen alle anderen Bundesländer diese Lehre als fachpraktische Ausbildung und setzen dafür Fachleute aus der polizeilichen Berufspraxis ein. Auch die strategische Ausrichtung variiert. Während Berlin gerade ein Berufungsverfahren zum Schwerpunkt Cyber- und Informationssicherheit durchführt, wird in Sachsen die Professur für Informatik seit 2019 nicht nachbesetzt. Aus Sicht der Autoren dieses Beitrags, Professoren und erfahrene Fachleute aus der polizeilichen Berufspraxis, ist das Themengebiet Digitale Spuren eindeutig ein Fachgebiet, mit dem sich wissenschaftlich auseinandergesetzt werden muss. Es wird daher allen Bundesländern mit Nachdruck empfohlen, Professorinnen oder Professoren die Verantwortung für die entsprechende Lehre zu übertragen. Gerade der Umgang mit Digitalen Spuren ist ein Thema mit einem hohen wissenschaftlichen Anspruch, dem nach Meinung der Autoren durch den Einsatz von Ausbildungspersonal mit entsprechendem wissenschaftlichem Hintergrund begegnet werden müsste (Povalej et al., 2021; Povalej, 2019).

Aus den in Tab. 1 dargestellten Ergebnissen lassen sich anhand der Verteilung vier Klassen ableiten: Klasse 1 mit 100 oder mehr Lehreinheiten, Klasse 2 mit 69 bis weniger als 100, Klasse 3 mit 38 bis weniger als 69 und Klasse 4 mit unter 38 Lehreinheiten. Die Zuordnung der Bundesländer zu den Klassen ist in Tab. 2 dargestellt. Aus der Klassenerstellung lässt sich die Frage ableiten, ob die Dauer der Vermittlung der Lehrinhalte in den vier Klassen jeweils eine Vermittlung der Basiskompetenzen zulässt.

Ein Blick in die PKS (BMI, 2021) bzw. das Bundeslagebild Cybercrime (BKA, 2021) zeigt, dass trotz der Anstrengungen in einigen Bundesländern keine

Tab. 2 Klasseneinteilung der Bundesländer nach der Verteilung der LE im Gebiet Cybercrime

Klasse	Bundesländer
1	Saarland
2	Schleswig-Holstein, Hamburg, Rheinland-Pfalz, Hessen, Mecklenburg-Vorpommern
3	Baden-Württemberg, Bremen
4	Berlin, Niedersachsen, Sachsen, Bayern, Brandenburg, Thüringen, Nordrhein-Westfalen, Sachsen-Anhalt

wesentliche Verbesserung der Kriminalitätsbekämpfung im Bereich Cybercrime stattgefunden hat. Wie in den Studien ersichtlich, steigt die Anzahl der erfassten Fälle kontinuierlich, während sich die der aufgeklärten Fälle im Bereich von 31.000 bis ca. 35.000 bewegt. In der Folge sinkt die Aufklärungsquote bzw. stagniert bestenfalls. Es liegt also nahe, dass die Rahmenbedingungen für die Ausbildung nicht ausreichen, da sie mit den schnellen Entwicklungen auf dem Gebiet der Digitalen Spuren nicht adäquat mithalten können. Die Fähigkeiten und Fertigkeiten können nicht nur an vorhandenen Technologien und Techniken, welche für die Begehung und Aufklärung von Cyberstraftaten genutzt werden, ausgerichtet werden, sondern müssen ein anschließbares Wissen hervorbringen. Dieses Wissen muss sich neben den klassischen Methoden der Verbrechensaufklärung gerade an technologischen Trends orientieren. Somit rücken das Verständnis und die Abschätzung neuer Technologien in den Fokus der Ausbildung.

5 Das Wechselspiel zwischen Kriminellen und ermittelnden Behörden

Aus dem einleitend bereits beschriebenen Wechselspiel zwischen Kriminellen und ermittelnden Behörden ergibt sich die Frage, ob beispielsweise durch die Entdeckung der Daktyloskopie und den Eigenschaften, die diese mit sich brachte, eine verbesserte Strafverfolgung möglich war. Nachdem sich das Prinzip der Daktyloskopie etabliert hatte und auch nach und nach vor Gericht zugelassen wurde, fing auch die Polizei in verschiedenen Ländern an, sie in die Aufklärung ihrer Fälle mit einzubeziehen. 1880 veröffentlichte der schottische Arzt Henry Faulds einen Artikel, in dem er über Fingerabdrücke schrieb und entfachte damit eine Debatte, der sich auch Francis Galton anschloss. Diesem gelang es im Jahr 1888 dem Fingerabdruck eine tiefere Bedeutung zuzuschreiben (Evans, 1998, S. 120). Galton gilt als einer der Gründerväter des Fingerabdruckverfahrens, heute als Daktyloskopie bezeichnet und veröffentlichte damals auf Grundlage einer ausführlichen Studie seine Ausarbeitung zu dem Thema. Galton beschrieb darin die sogenannte Minutia-Eigenschaft des Fingerabdrucks.

Er untersuchte die Abdrücke, indem er sie in kleinere Bereiche unterteilte und stellte so ihre Individualität fest. Da dies bedeutete, dass jeder Mensch zu dieser Zeit einen eigenen und einmaligen Fingerabdruck besitzen müsse, beschäftigte Galton sich mit dem Problem, seine These entsprechend zu beweisen. Er konnte

mathematisch belegen, dass die Wahrscheinlichkeit zweier Personen mit demselben Fingerabdruck absolut gering war. Sie lag gerade einmal bei 1 zu 64 Milliarden. Aus dieser Information entstand die Idee, den Fingerabdruck auch als Beweismittel im Rahmen von Strafverfahren zu verwenden. Galton entwickelte dafür ein System der Personenerkennung (Koch, 2021, S. 3). In etwa zur selben Zeit begann der argentinische Kriminalist Ivan Vucetic seine Fingerabdrücke und die von straffällig gewordenen Personen zu sammeln. Dabei fiel ihm auf, dass kein Fingerabdruck dem anderen glich. Seine Methode, welche er anfangs als Iknofalangometrie bezeichnete, benannte er später um in Daktyloskopie. Im Jahre 1892 löste er aufgrund dieses Wissens den ersten Mordfall, welcher mithilfe der Daktyloskopie aufgeklärt wurde. Im Jahr 1888 schlug der Berliner Tierarzt Wilhelm Eber vor, die Methode der Daktyloskopie zum Zwecke der erkennungsdienstlichen Behandlung zu nutzen.

In Deutschland dauerte es allerdings noch einige Jahre, bis das Verfahren Fuß fassen konnte (Koch, 2021, S. 4). Inzwischen werden Fingerabdrücke digital gespeichert, um eine entsprechend belastbare Anzahl dieser zu erfassen und zeitnah auswerten zu können. Verglichen werden die Abdrücke heute von Programmen wie AFIS (Automatisiertes Fingerabdruckidentifizierungssystem). Zur Unterstützung der manuellen Tätigkeit der Sachverständigen wurde Anfang 1994 das AFIS in der deutschen Polizei eingeführt, welches es den Experten ermöglichte, Tatortspuren computergestützt mit bereits vorhandenen Fingerabdrücken von Straftätern zu vergleichen. Hierbei werden gesicherte Fingerabdrücke mit den in einer Datenbank gespeicherten verglichen. Die Speicherung der Daten erfolgt im Bundeskriminalamt und wird den Landeskriminalämtern für die Bearbeitung zur Verfügung gestellt. Mittlerweile umfasst die Kartei des BKA mehr als 2,5 Millionen Fingerabdrücke (Wigand, 2018).

Während man in der Geschichte der Daktyloskopie eine für die damalige Zeit eher typisch gemächliche Entwicklung sieht, haben sich die Umstände nicht zuletzt durch die Digitalisierung deutlich beschleunigt und die Frequenz der Einführung neuer Technologien erhöht. Mit dieser Beschleunigung müsste auch zwangsläufig eine schnellere Reaktion auf Seiten der Polizeiausbildung und der Weiterentwicklung der polizeilichen Methoden einhergehen. Die Auswertung der Modulhandbücher legt nahe, dass das nicht überall der Fall ist.

Es erscheint zudem notwendig zu sein, gezielt und proaktiv neue Technologien zu monitoren und auf ihre Auswirkungen auf die Kriminologie zu prüfen. Das Ziel muss sein, sozusagen schneller „neue Fingerabdrücke“ in Reaktion auf die von den Kriminellen gezeigte reale Techniknutzung und die hierdurch möglich gewordenen neuen Methoden zu finden und mit möglichst geringem Zeitverzug in die polizeiliche Lehre aufzunehmen. Eine Beschleunigung auf Seiten der jeweiligen Strafverfolgungsbehörden ist jedoch auf Basis der ausgewerteten Daten nicht durchgängig erkennbar.

Hinzu kommt, dass dabei die Begehungsweisen an die neue Technik angepasst werden, während das Grunddelikt unverändert weiter besteht. Bestellungen unter falschem Namen gab es beispielsweise schon zur Zeit von Katalogen, damals in der Regel unter Nutzung der Bestellscheine oder -postkarten. Später wechselten die Täter zum Fax und noch später zu Online-Bestellungen. Im Kern handelt es sich

aber immer um einen Warenkreditbetrug (sofern die Ware auf Rechnung verschickt wird), bei dem sich lediglich der Übermittlungsweg immer wieder an moderne Verfahren anpasst. Die Kriminalistik hat sich hier angepasst und heute ist *fraud detection* mittels Maschinellem Lernen Teil des Onlinehandels (Kou et al., 2004).

Das gilt auch in anderen Bereichen. Beispielsweise wurden vor 20 Jahren Überweisungsaufträge mit gefälschter Unterschrift bei den Banken eingeworfen, später kamen Ersatz-SIM-Karten für die mobile TAN zum Einsatz, die von den Tätern bestellt und diesen per Post zugeschickt wurden. Noch später wurde das Verfahren nach Einsatz der eSIM nochmal erheblich beschleunigt, da die Ersatz-eSIM online freigeschaltet und buchstäblich Sekunden später zum eigentlichen Zweck, der Ausführung einer betrügerischen Überweisung, genutzt werden konnte. Der Kern der Tat bleibt gleich. Was sich ändert sind Geschwindigkeit und Medium: von ein paar Tagen (eingeworfener Überweisungsauftrag), über 1–2 Tage (Bestellung einer Ersatz-SIM-Karte) bis zu wenigen Minuten (Nutzung von eSIM). Eine ähnliche Beschleunigung in der Anpassung der Lehrinhalte bei der Polizeiausbildung ist derzeit in kaum einem Bundesland zu erkennen. Allein für die Erkenntnis, dass es sich um keine neue Straftat handelt, sondern hinlänglich bekannte Mechanismen auf Basis neuer Wege zum Einsatz kommen, ist ein gewisses Maß an technischem Hintergrundwissen erforderlich, das in der Ausbildung vermittelt werden muss. Diese Beispiele zeigen, dass es auch in der analogen Welt den Wettlauf zwischen Ermittler und Kriminellen gibt bzw. gegeben hat. Im Phänomenbereich Cybercrime erhöht sich die Geschwindigkeit des Wettlaufs auf der Spirale immer weiter.

Auf der anderen Seite gibt es auch Technologien, die als positiver *Dual Use* die Verbrechensaufklärung revolutionieren, beispielsweise die Isotopenanalyse. Das chemische Verfahren lässt von Gewebeproben auf die Lebensweise und die geografische Herkunft einer Person schließen. Bei Opfern, deren Identität unbekannt ist, kann diese Methode aufschlussreiche Hinweise liefern. Zu den neuesten Entwicklungen im Bereich der Tatort-Erfassung gehört der 3D-Laserscan. Durch Referenzpunkte, die vor Ort platziert werden müssen, ist es möglich, eine dreidimensionale Darstellung des Tatortes anzufertigen. Diese Technik kann man auch bei betroffenen Körperstellen von Opfern einsetzen und so ein millimetergenaues, maßstabsgetreues 3D-Modell erstellen. Diese virtuellen Rekonstruktionen können unter Einbezug der dokumentierten Spuren und Befunde zur Klärung des Tathergangs führen. Die Möglichkeiten, heute ein Verbrechen aufzuklären, werden von den neuesten wissenschaftlichen und technischen Entwicklungen vorangetrieben. Frei nach Locard (1930) gilt: Jeder hinterlässt Spuren, die gefunden werden können, man muss sich eben nur auf die Suche danach machen.

Somit ist Technologie nicht nur das Verbindungsglied zwischen Opfern und Tätern, sondern ein wichtiger Baustein für die Verbesserung der Kriminalitätsbekämpfung. Die cyberkriminologische Perspektive der ermittelnden Behörden lässt sich somit ebenfalls durch die neuen Technologien in das Gesamtbild (Abb. 1) einführen und über die Ausbildung analysieren. Alle Beteiligten, Bürger und Opfer, Kriminelle und Ermittler nutzen neueste Technologien, jedoch mit anderen Vorzeichen behaftet. Allgemein kann die Technologie ein Treiber für die Begehung von (neuen) Straftaten sein und für deren Aufklärung. Aber es gibt kein Fach in der

polizeilichen Ausbildung, das systemisch, also unabhängig von der Lehrperson, im kurzen Zeitraum auf neue Erfordernisse reagiert.

6 Technologie als Treiber

Die Sichtweisen von Tätern, Opfern und Ermittlern, welche über die Entwicklung und die Verwendung neuer Technologien miteinander verbunden sind, lassen sich durch Ansätze des *Community-based Operations Research* (Johnson, 2012; Johnson & Smilowitz, 2012; Midgley et al., 2018) analysieren. In diesem Abschnitt soll die Sichtweise von Ermittelnden in den Mittelpunkt der Betrachtungen gerückt und der Einfluss neuer Technologien in der täglichen Fallarbeit betrachtet werden. Als Ergebnis lässt sich ein *Crime Potential Cycle* für den Bereich Cybercrime ableiten, welcher auf dem *Cyber Potential* der Technologien beruht.

Neue und auch bereits bekannte Technologien sind stetig auf deren *Dual Use Potential* anhand quantitativer und qualitativer Modelle und Methoden zu bewerten. In Anlehnung an das *Community-based Operations Research* benötigen wir mehrere analytische Methoden, um den *Dual Use Potential* zu erkennen. Darüber hinaus benötigen wir formelle und informelle Communities, in denen frühzeitig, idealerweise bevor eine Technologie erfolgreich missbraucht wird, Lösungen zum Schutz potentieller Opfer bereitgestellt werden. Dabei sind die Gruppen der Ermittler und (potentiellen) Opfer ebenso einzubeziehen, wie Experten aus verschiedenen Communities. Gemeinsam können diese Gruppen unter Berücksichtigung von technologischen Entwicklungen und deren Reifegraden Maßnahmen ableiten, um Handlungsempfehlungen zum Schutz vor kriminellen Angriffen abzuleiten, aber auch Straftaten schneller aufzuklären.

Eine Spezialisierung des in Johnson (2014) spezifizierten *Community-Based Operations Research* kann auf den hier vorgestellten Ansatz angewandt werden. Abb. 2 stellt einen Adaptionsvorschlag vor. Dabei ist jeder Schritt mit einem Beispiel hinterlegt worden. Links wird mit der Frage begonnen, wer die Beteiligten des Prozesses sind. Stakeholder sind hier beispielsweise die Nutzer der untersuchten Technologie, die auf beiden Seiten des *Dual Use* stehen. Dabei ist für diese Analyse die Gemeinschaft der Forensiker und IT-Spezialisten in den Strafverfolgungsbehörden zu nennen, da sie in dem Prozess eine grundlegende Rolle spielen.

Der nächste Schritt ist die Identifikation einer noch nicht bewerteten oder neu zu bewertenden Technologie und ihr Einsatz auf beiden Seiten des *Dual Use*, die es zu untersuchen gilt. Nach einer ersten Analyse, entsteht eine Bewertung bei der die Digitalen Spuren und ihre Bedeutung (Risiken, Nutzen und entstehende Kosten) beschrieben werden, beispielsweise durch ihren Einsatz in einem negativen *Dual Use*. Diese werden dann durch den hier beschriebenen Ansatz von Experten bewertet. Das so entstandene Wissen findet anschließend seine Anwendung in mit der Praxis entwickelten Lösungen. Hier entsteht eine Schleife, bei der das neu gewonnene Wissen wieder zurück in den Prozess fließen kann. Wünschenswert wäre, dass erzeugte Inhalte auf weiteres Vorgehen wie beispielsweise in der Prävention, in der Lehre und bei aktuellen Verfahren Einfluss nehmen. Eine Aussage über die letzte

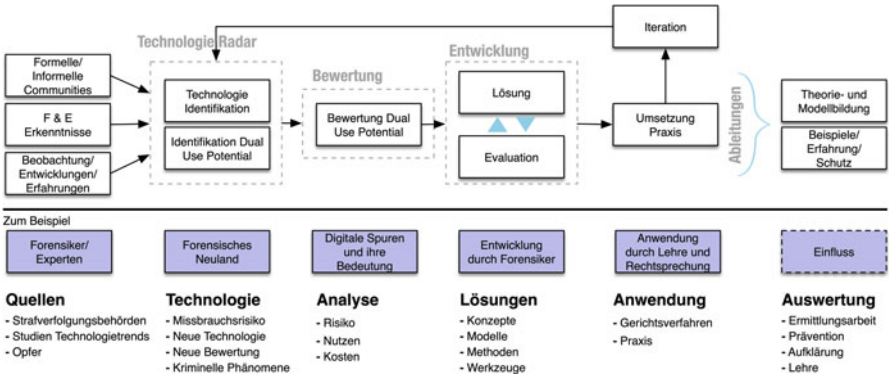

Abb. 2 Modell, um Dual Use Potential von Technologien zu identifizieren, zu bewerten, Lösungen für die Praxis zu entwickeln und Ableitungen vorzunehmen (in Anlehnung an das Framework Model-Driven Technologies: Community-Based Operations Research)

Phase – Einfluss auf die Gesellschaft (gestrichelt) – ist hier noch nicht möglich, da der Effekt des hier vorgestellten Ansatzes noch nicht untersucht ist. Für eine Analyse fehlen hier die Daten einer Evaluation. Ziel ist jedoch so einen strukturierten Austausch zwischen Praxis und relevanten Themen für die Lehre zu gewährleisten.

7 Analyse und Gefahrenabschätzung neuer Technologien mittels *Crime Potential Cycle*

Wir wollen nun die Modelle der Entwicklung und Akzeptanz von Technologie auf die Verwendung von Technologie im Zusammenhang mit Straftaten und damit in die Welt der Forensik übertragen. Dabei kann ein Überblick über solche Modelle beispielsweise bei Lee et al. (2003); Bagozzi (2007) oder Venkatesh und Bala (2008) gewonnen werden.

Vereinfacht betrachtet lassen sich bei den meisten etablierten Modellen die nachfolgend beschriebenen Phasen ableiten. Der Betrachtung zugrunde liegt der *Hype Cycle* von Gardner, der heute in der Informationstechnologie ein Quasi-Standard ist und in vielen weiteren Bereichen angewandt werden kann (O'Leary, 2008). Die hier vorgeschlagene Übertragung basiert auf der Beobachtung, dass die kriminologische Aufarbeitung der Digitalen Spuren gerade im Zusammenhang mit neuen Technologien immer etwas hinterherhinkt und es den Lehrenden schwer fällt zu entscheiden, welche Lehrinhalte für die Zukunft sinnvoll sind. Die forensischen Methoden entwickeln sich in einer ähnlichen Weise wie die Spuren an sich. Je mehr Technologie zum Einsatz kommt, desto höher ist nicht nur ihr negatives *Dual Use Potential*, also die Möglichkeit der Nutzung im Zusammenhang mit Straftaten, sondern auch die tatsächliche schädliche Nutzung. Sobald dies erkannt wird, setzen sich Ermittelnde mit der Technologie und den damit einhergehenden Digitalen Spuren im Rahmen ihrer Tätigkeit auseinander und definieren so den Start des *Crime Potential Cycles*.

Technischer Auslöser: Ab dem Zeitpunkt einer Erfindung oder einer Entdeckung gibt es einen Prozess der Innovation. Dabei wird die Idee, die hinter der Erfindung steht, auf eine Domäne angewandt. Dieser Prozess kann beispielsweise durch angewandte Forschung, Startups oder Forschungsabteilungen von Firmen geschehen. Vom Zeitpunkt der ersten Idee an werden meist Prototypen entwickelt, die dann durch eine weitere Verwertung zur Marktreife geführt werden. Dies bedeutet nicht nur die Entwicklung eines Produkts, sondern beispielsweise auch die Ausnutzung einer mit der Erfindung einhergehenden Schwachstelle durch einen Exploit. Für ein forensisches Artefakt ist dies die erste Analyse durch einen Experten der die Fakten so aufbereitet, dass eine digitale Spur identifiziert wird. Diese muss meist erst noch auf ihre Gerichtsfestigkeit überprüft werden (Povalej et al., 2021; Honekamp et al., 2020). Die Phase des Technischen Auslösers endet damit, dass eine Markteinführung stattfindet, die zu einer ersten Nutzung durch sogenannte *Early Adopters* führt.

Einführung: Nachdem die ersten Prototypen Anwendung finden, gibt es eine Phase der Einführung. Diese ist normalerweise durch eine Reifung der Prototypen zu einem Produkt geprägt. Bei einer Methode zur forensischen Analyse ist dies die Analyse von tatsächlichen Artefakten im Zusammenhang mit einer kriminellen Handlung und die erste Verwendung der so erzeugten Erkenntnisse vor Gericht. Dabei müssen meist Gutachter als Experten eingesetzt werden, um Richtern und Anwälten die Artefakte zu erklären.

Neuerungen: Nachdem sich nun eine Methode oder Technologie etabliert hat, wird diese in sogenannten S-Kurven weiterentwickelt (Brown, 1992). Dabei entstehen Neuerungen und Varianten der Methode oder Technologie, die wieder neu durch Experten analysiert werden müssen, um wieder gerichtsfest als digitaler Sachbeweis zu gelten. Hierzu wird der Zyklus insgesamt wieder durch die Phasen und seine Anwender abgebildet. Nach Brown (1992) gibt es hier nach den Innovatoren und der *Early Majority* die *Late Majority* und dann die *Laggers*. Für Digitale Spuren bedeutet dies, dass eine kleine Neuerung – beispielsweise eine Aktualisierung eines Dateisystems – dazu führen kann, dass eine digitale Spur verschwindet, eine neue entsteht oder eine Spur sich verändert. In all diesen Fällen gibt es jedoch wieder Zeitabschnitte, bis die Neuerung sich durchgesetzt hat. In dieser Zeit hat die von Brown genannte „Akzeptanz" noch nicht den ganzen Markt durchdrungen. In dieser Phase können die alten Digitalen Spuren noch zu Ermittlungserfolgen beitragen, es wird jedoch weiterer Forschungsaufwand benötigt, um die neuen Digitalen Spuren zugänglich zu machen.

Für eine Entscheidung, was gelehrt werden soll, kann hier abgeleitet werden, dass eine Technologie, die nicht mehr im Markt repräsentiert ist (also kaum noch Anwendung findet) auch nicht mehr Teil der Lehre sein sollte. Auf der anderen Seite kann Technologie, die nach Brown (1992) von der *Developing Technology* zur *Mature Technology* wechselt, aufgenommen werden, da sich diese in breiter Nutzung befindet. Während in den ersten beiden Phasen der Technologieentwicklung mehrere konkurrierende Technologien entwickelt werden können, gibt es nach Konsolidierung meist nur ein paar wenige, die sich durchsetzen. Ein gutes Beispiel dafür sind mobile Betriebssysteme, bei denen der Markt im Moment von zwei

Technologien dominiert wird (nach Alzubaidi, 2021 haben Android und IOS hier 99,3 % Anteil am Markt). Dies bedeutet für eine forensische Analyse, dass sich die Ermittlungserfolge negativ entwickeln und erst, wenn die Neuerungen stagnieren, die Forensik stabile Ergebnisse liefern kann. Dabei werden die Methoden jedoch zwangsläufig bekannt und ihre kriminelle Nutzung adaptiert sich, da eine Marktdurchdringung stattgefunden hat. Die Täter reagieren also auf die weiterentwickelten Methoden der Forensik (einfachstes Beispiel: nach Einführung der Analyse von Fingerabdrücken verwendeten die Täter zunehmend Handschuhe, um Fingerabdrücke zu vermeiden).

Durchdringung: Bei einer Marktdurchdringung bekommt die Methode oder die Technologie mehr Aufmerksamkeit und kommt mehr zu Einsatz. Beispielsweise gibt es mehr Verfahren die ein bestimmtes Artefakt verwenden, um Verurteilungen herbeizuführen. In der Folge wird von der negativen Dual-Use-Verwendung abgesehen oder es werden anti-forensische Maßnahmen ergriffen. Damit beginnt eine Abwärtsentwicklung der Aufklärungsquote, und meist werden hier schon alternative Technologien gesucht, die den Kreislauf von vorn anfangen lassen. Ein Beispiel hierfür sind die verwendeten Speichermedien: Festplatten waren am Anfang teuer und hatten wenig Speicherplatz. Mit der S-Kurven-artigen Entwicklung von HDD wurden die Kapazität und ihre Lese-/Schreibgeschwindigkeit immer besser. Auch wenn heute noch ab und zu HDD im Einsatz sind (beispielsweise in Servern), so sind diese doch von den meisten Geräten verschwunden und wurden durch eine neue Technologie (z. B. SSD) ersetzt. Die forensische Analyse einer HDD ist prinzipiell anders als die einer SSD, und damit muss in der Forensik der Digitalen Spuren hier der Cycle von vorne beginnen.

Auslauf: Die Endphase des Kreislaufs ist unterschiedlich zu den typischen Hype-Kurven. Sie entwickelt nicht den typischen *Slope of Enlightenment* und ein *Plateau of Productivity,* sondern verliert ihre Relevanz in kriminellen Auswertungen, da die Technologie keinen Einsatz mehr findet, Spuren ausreichend verwischt oder nur an Stellen entstehen, die eine Sicherung (zumindest derzeit) nicht zulassen. Ein Beispiel hierfür ist die Forensik von Schreibmaschinenbändern. Hier kann anhand der Abdrücke der Buchstaben etwas Geschriebenes einer konkreten Schreibmaschine zugeordnet werden. Da der Einsatz von Schreibmaschinen in Tatbeständen in den letzten Jahren zurückgegangen ist, werden diese Spuren nur noch selten in Verfahren verwendet. Damit geht auch der Ermittlungserfolg für diese Spuren zurück.

Die Abb. 3 stellt zwei Aspekte von Technologie in ihrem negativen *Dual Use* dar. Die dünne Linie spiegelt die kriminelle Nutzung wider (*Early Adopter*, Nutzen frühzeitig erkannt, sobald Durchdringung erfolgt springen *Early Adopter* ab, übrig bleiben „Unwissende“, die noch auf den Zug aufspringen wollen). Danach – sobald die Ermittlungserfolge hoch sind – sind es nur noch die „Pechvögel“, die diese Technologie nutzen. Hier fängt in den ersten Monaten nach dem technischen Auslöser die kriminelle Nutzung an. Beispiele dafür können Programmierfehler sein, für die ein Exploit entwickelt wird, oder einfach neue Technologien, wie ein Telefon, das dann für einen Betrug verwendet wird.

Nach den ersten Fällen, bei denen es zu Anzeigen kommt beginnt sich die Gemeinschaft der digitalen Forensik mit dem Phänomen zu beschäftigen. Die

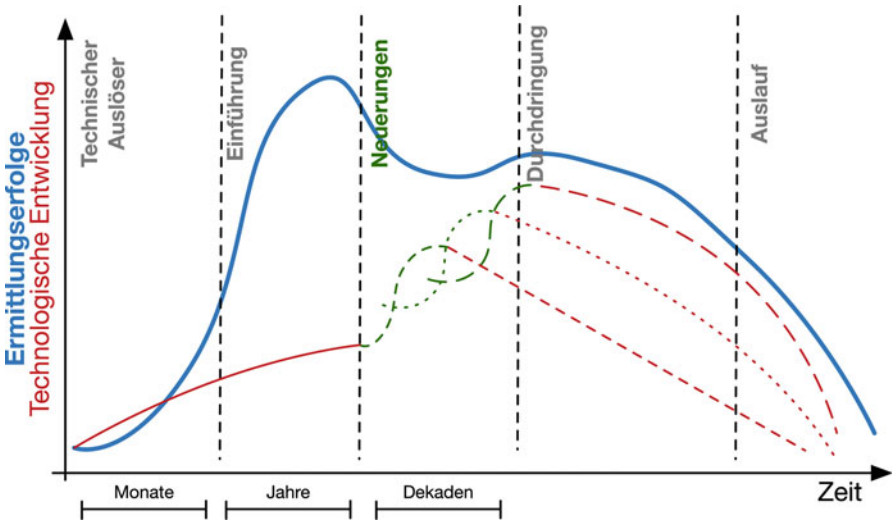

Abb. 3 Crime Potential Cycle – Zeitliche Abhängigkeit der Ermittlungserfolge in Korrelation mit der technologischen Entwicklung

Nutzung – wenn erfolgreich – nimmt zu und es kann Jahre dauern, bis für diese Technologie Neuerungen nötig werden. Nachdem eine Technologie eine gewisse Nutzung (Marktdurchdringung) erreicht hat, gibt es neue Versionen der alten Technologie (Telefon mit Wählscheibe zu Telefon mit Druckknöpfen) oder Neuerungen in der Technologie selbst (z. B. GSM zu 3G). Diese Neuerungen laufen meist in sogenannten S-Kurven (Brown, 1992). Es gibt am Anfang eine Startphase, die Technologie setzt sich durch und erreicht eine Sättigung. Dies sind die gestrichelten Kurven in der Abb. 3 im Bereich Neuerungen. Aber auch diese werden mit der Zeit durch eine andere Technologie abgelöst und verschwinden vom Markt, was dann in der Auslaufphase dargestellt wird.

Die zweite Kurve (fett) spiegelt den Ermittlungserfolg wider. Nach einem initialen verzögerten Start, werden forensische Methoden entwickelt, die den Ermittlungserfolg erhöhen. In der Phase der Neuerungen sind meist nicht genug Ressourcen vorhanden, um bei der Aktualisierung der forensischen Methoden mit der Entwicklung mitzuhalten. In der Durchdringungsphase bleiben Ermittlungserfolge, es ist jedoch durch öffentlich geführte Verfahren bekannt, wie hier die Technologie forensisch genutzt wird, und es werden Gegenmaßnahmen verwendet oder die Technologie wird immer weniger kriminell genutzt.

Beide Kurven stehen in Relation zur Lebenskurve (*Life Cycle*) der Technologie. Horizontal ist die Zeit der forensischen Relevanz der Technologie. Die Y-Achse stellt den Nutzen/Erfolg der jeweiligen Gruppe (Kriminelle vs. Ermittelnde) dar. Ob dieses Modell des Einflusses von technologischer Entwicklung, die Lehrinhalte der Curricula der polizeilichen Ausbildung und die Ermittlungserfolge so korrelieren oder ob hier eine Kausalität existiert, muss erst noch evaluiert werden. Die in Abb. 3

vorgestellten Zeitläufen des Modells müssen in den nächsten Jahren quantifiziert werden.

8 Crime Potential und Ausbildung der Ermittler

Aus den Rahmenbedingungen für die Vermittlung der Basiskompetenzen, den Statistiken zur Aufklärung von Cyberkriminalität und den jetzt vorhandenen kritischen Technologien sowie deren Auswirkung auf Cyberkriminalität kann ein *Investigation Knowledge Gap* abgeleitet werden. Je größer der Abstand zwischen der fachlichen Kompetenz der Ermittelnden und dem Schadpotential ist, desto weniger erfolgreich werden in der Regel Ermittlungen in dem Bereich sein. In fast allen Bundesländern wird im Studium nicht der zeitliche Rahmen für eine umfassende Vermittlung der Basiskompetenzen nach Kunze (2018) bereitgestellt. Die Abb. 4 soll diese Wissenslücke als schematische Darstellung an ausgewählten Beispielen verdeutlichen. Sie illustriert das Verhältnis von Lehrwissen (innere Kurve) zu den potentiellen Auswirkungen der Technologie (äußere Kurve), die man auch als „potentiellen Nutzen für Kriminelle" beschreiben kann. Die Fläche zwischen den Kurven stellt den *Investigation Knowledge Gap* dar.

Bei der Betrachtung muss beachtet werden, dass es im Hinblick auf die Strafverfolgung mehrere *Investigation Knowledge Gaps* gibt, die zwar kausal zusammenhängen, aber zur Lösung des Problems getrennt betrachtet werden müssen. Es kann eine Lücke zwischen der Technologienutzung durch die Täter und dem Erkennen des deliktischen Hintergrunds durch die Strafverfolgung erkannt werden. In dieser Zeitspanne wird dem negativen Teil des D*ual Use* kaum etwas durch Ermittelnde entgegengesetzt. Diese Lücke entsteht dadurch, dass Kriminelle erfahrungsgemäß neue Technologien schneller adaptieren und illegale Geschäftsmodelle entwickeln, die diese neue Technik nutzen, als dass die Ermittlungsbehörden ihre Ausbildung anpassen.

Unsere Erfahrung als Dozenten an Polizeihochschulen und Akademien zeigt, dass es dann einige Zeit dauern kann, bis das Wissen über „neue" Deliktsformen (bei denen es sich oft um altbekannte Delikte handelt, die lediglich auf neue Art begangen werden) im Rahmen von konkreten Strafverfahren auffällig wird. In diesem Moment ist oft noch nicht klar erkennbar, welches Täterhandeln hinter einem angezeigten Sachverhalt steht. Ab einem bestimmten Zeitpunkt kann die digitale Forensik zwar das deliktische Handeln einordnen, das bedeutet allerdings nur, dass man die Handlungen der Täter versteht, nicht aber, dass man die dadurch erzeugten Spuren inhaltlich auswerten oder auch überhaupt nur sichern könnte. An diesem Punkt beginnt die forensische Forschung damit, technische Lösungsansätze für die Sicherung und Bewertung der Daten zu entwickeln, um diese beweiskräftig ins Ermittlungsverfahren einbringen zu können.

Wenn diese Lücke überwunden ist, dann bleibt als nächste Herausforderung, die Inhalte aus dem Lernprozess an die gesamte Kette der Strafverfolgung zu vermitteln, also von den Ersteinschreitenden (diejenigen, die als erstes mit dem Fall zu tun haben), über die Sachbearbeitung (diejenigen, die den Sachverhalt bearbeiten und in

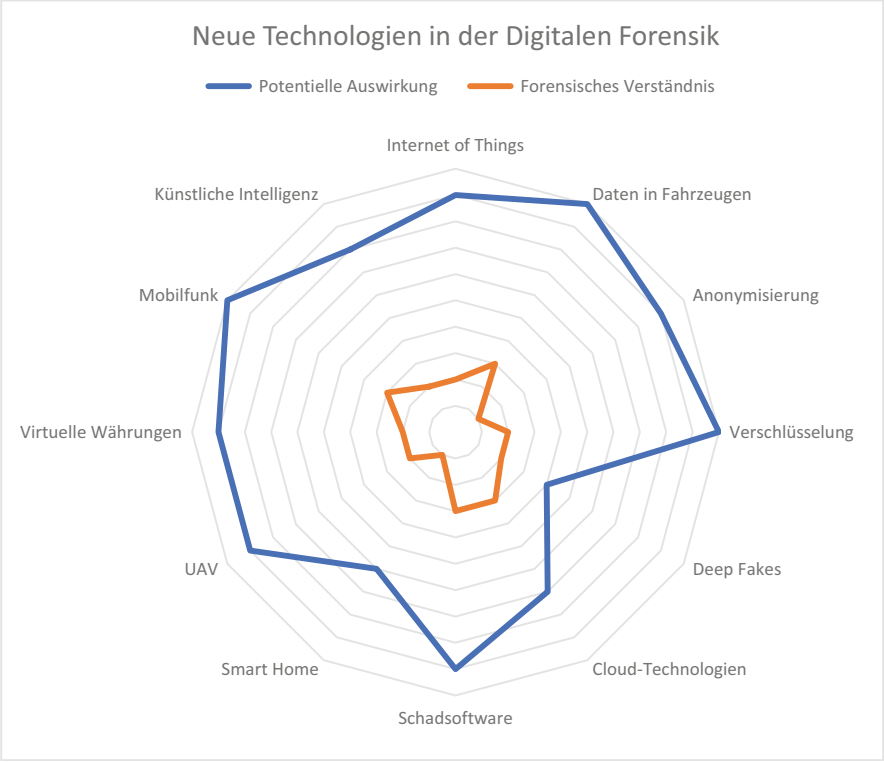

Abb. 4 Investigation Knowledge Gap – das Verhältnis von vermitteltem forensischem Verständnis in der Lehre zu den potentiellen Auswirkungen von ausgewählten Technologien

der Regel über ein tiefergehendes Hintergrundwissen verfügen) und die Führungskraft, die auf den Einsatz der neuen forensischen Methoden in konkreten Fällen hinwirken muss. Gerade hier ist es nach Meinung der Autoren zwingend erforderlich, Kompetenz und Forschung zum Thema „Cybercrime" auch in der Deutschen Hochschule der Polizei als festen Bestandteil des Studiums zu integrieren und entsprechende Forschung zu betreiben, um proaktiv auf aktuelle Entwicklungen reagieren zu können. Die Kette setzt sich auch außerhalb der Polizei weiter fort. Es ist zwingend erforderlich, dass Staatsanwaltschaft und Richter die Methoden kennen und verstehen, um sie juristisch bewerten zu können und sie dann geordnet in die gerichtliche Praxis einfließen zu lassen.

In einigen Fällen ergibt sich dann die nächste Lücke, nämlich immer dann, wenn man erkennt, dass es sich zwar um sozial inadäquates Verhalten handelt, dieses aber aufgrund einer Regelungslücke nicht strafbewehrt oder eine Strafverfolgung aufgrund anderer Umstände nicht möglich ist (z. B. weil die Täter aus dem Ausland agieren und der Sachverhalt dort nicht strafbar ist). Ab diesem Zeitpunkt gilt es, den politischen Entscheidungsträgern den Sachverhalt so zu erklären, dass diese daraus politische Handlungszwänge erkennen und regulatorisch reagieren können. Dies

kann beispielsweise auf Basis von Gesetzesänderungen erfolgen oder auch durch internationale Vereinbarungen, die eine Strafverfolgung im Ausland erleichtern oder überhaupt erst ermöglichen. Die Behebung dieser Lücken ist in jedem Stadium eine Herausforderung für sich und zwangsläufig immer mit zeitlichem Verzug verbunden. Wenn beispielsweise die Forensiker Methoden entwickelt haben, wie sie wertvolle Artefakte aus neuen Geräten extrahieren können (z. B. Positionsdaten mit korrelierenden Zeitstempeln aus Smartwatches), diese Fähigkeiten und deren potentielle Auswirkungen auf die Ermittlung aber nicht allen Gliedern der Kette bewusst sind, wird die Ermittlung insgesamt nicht optimal verlaufen.

Die genannte Smartwatch soll anhand eines fiktiven Falls als Beispiel dienen: ein Tatverdächtiger eines Tötungsdelikts wird in der Nacht festgenommen, er trägt eine Smartwatch. Wenn der Ersteinschreiter nicht weiß, dass dieses Gerät ein potentieller Spurenträger ist, werden im Extremfall Spuren unbrauchbar (durch zeitlichen Verzug oder durch Manipulation des Tatverdächtigen). Der Beamte wird ohne Kenntnis wahrscheinlich auch nicht nach derartigen Beweismitteln suchen. Ist das Wissen beim später involvierten kriminalpolizeilichen Sachbearbeiter nicht vorhanden, so wird dieser die Smartwatch wahrscheinlich nicht zur Untersuchung in die Forensik geben oder nur unzureichende Untersuchungsaufträge formulieren. Digitale Forensik ist heute in vielen Fällen nach praktischer Erfahrung der Autoren „Fließbandarbeit“, deren Bearbeitung aus Auslastungsgründen oft streng entlang des Auftrags erfolgt. Das bedingt, dass schon die Untersuchungsaufträge so formuliert werden müssen, dass der Forensiker den zugrundeliegenden Ermittlungssachverhalt versteht, die für ihn wichtigen Informationen erhält und aus diesen Informationen heraus zielführende Methoden ohne großen Aufwand festlegen kann.

Verstehen die Staatsanwaltschaft und das Gericht nicht, dass die Positionsdaten wichtige und vor allem valide Sachbeweise sein können, so finden diese weder den Weg in die Anklageschrift noch in die Urteilsbegründung. Daher muss bei allen Gliedern der Kette ein solides Verständnis für Anforderungen, Inhalte und Möglichkeiten aller anderen Beteiligten vorhanden sein, um ein optimales Ermittlungsergebnis zu garantieren. Besonders kritisch sind hierbei die Ersteinschreitenden, da bei diesen die Weichen gestellt werden und Fehler, die in diesem Stadium begangen werden, später oft nicht mehr zu beheben sind. Es handelt sich hierbei in der Regel um die Vollzugsbeamten, die auf Basis der obenstehenden Curricula ausgebildet wurden. Umso wichtiger wäre es, dass das Rüstzeug schon in der Ausbildung jeder Beamtin und jedem Beamten mitgegeben wird und zwar zeitnah mit dem Auftauchen neuer Begehungsweisen im Zusammenhang mit technischen Entwicklungen.

Daraus erwächst die Frage, wie die Ausbildung zum Umgang mit Digitalen Spuren bei der Polizei gestaltet werden sollte. Wie sehen die bei Kunze (2018) ermittelten Basiskompetenzen in Anbetracht des technischen Fortschritts aus und was bedeuten Sie für die zukünftige Ausbildung? Es wird darauf abgezielt, mit dem Fortschritt neuer Technologien mithalten zu können und durchgehend handlungssicher zu sein bzw. zu bleiben. Unsere Hypothese ist, dass die Entwicklung neuer Technologien und deren Zyklus-förmige Einführung direkten Einfluss auf kriminelle Handlungen und die sich daraus ergebenden Ermittlungstätigkeiten hat. Dabei greift der Begriff Entwicklungsarbeit alle Phasen der forensischen Arbeit auf: Sicherung,

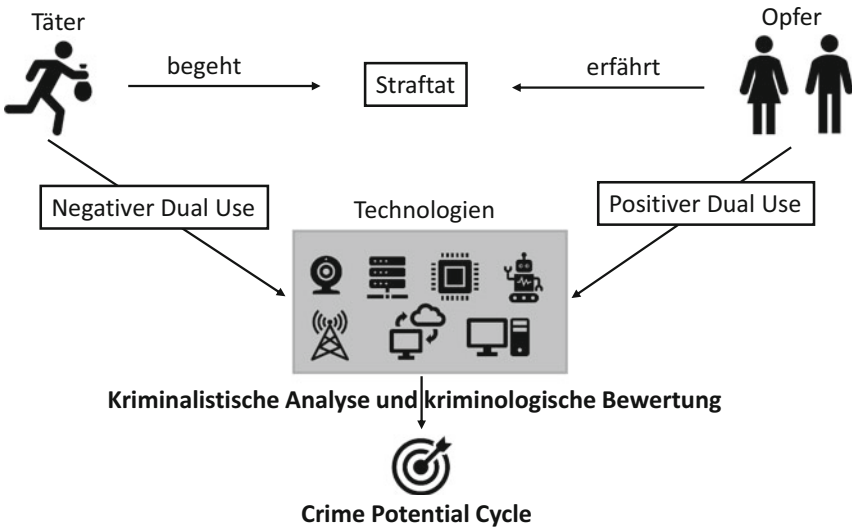

Abb. 5 Neue Ausbildungskonzepte – technologiebasierte Lehre im Bereich Cybercrime, ohne Anwendungen

Analyse und Präsentation. Der in Abb. 5 illustrierte *Crime Potential Cycle* stellt die Basis für das Technologieradar dar und kann als Bewertungsgrundlage dienen. Jedoch nicht nur die neuen Technologien können so beobachtet werden, sondern auch der Einfluss von Neuerungen lässt sich abschätzen. Die Phasen spiegeln den Lebenszyklus einer Technologie wider. Daraus ergibt sich eine neue Sichtweise und Perspektive auf neue Technologien.

9 Neue Sichtweisen auf Technologieentwicklungen und Ausbildung

Im Mittelpunkt der neuen Sichtweise auf Cyber-Straftaten steht nun das *Crime Potential* und deren dynamische Entwicklung, der *Crime Potential Cycle*, wobei sich das Potential auf unterschiedliche Technologien bezieht. Aus der Analyse der potentiellen Auswirkung neuer Technologien ergeben sich aktuelle Inhalte für die Aus- und Fortbildung (siehe Abb. 6). Dies kann als erste Einbeziehung des *Crime Potential* angesehen werden. Der *Crime Potential Cycle* bezieht sich auf die Anwendung in der Ermittlung und zeitlichen Verwendung bei Begehungsweisen.

Da die Menge an verwendeten Technologien eine breite Ausbildung nicht zwangsläufig zulässt, muss eine Auswahl der Lehrinhalte getroffen werden. Das hier vorgeschlagene *Crime Potential* soll bei dieser Auswahl als Grundlage dienen. Die Abb. 6 stellt alle cyberkriminologischen Perspektiven auf neue Technologien dar. Durch die konkrete Bestimmung des C*rime Potential* und der Einbeziehung des C*rime Potential Cycle* kann ein Rückschluss auf Begehungsweisen und stringente

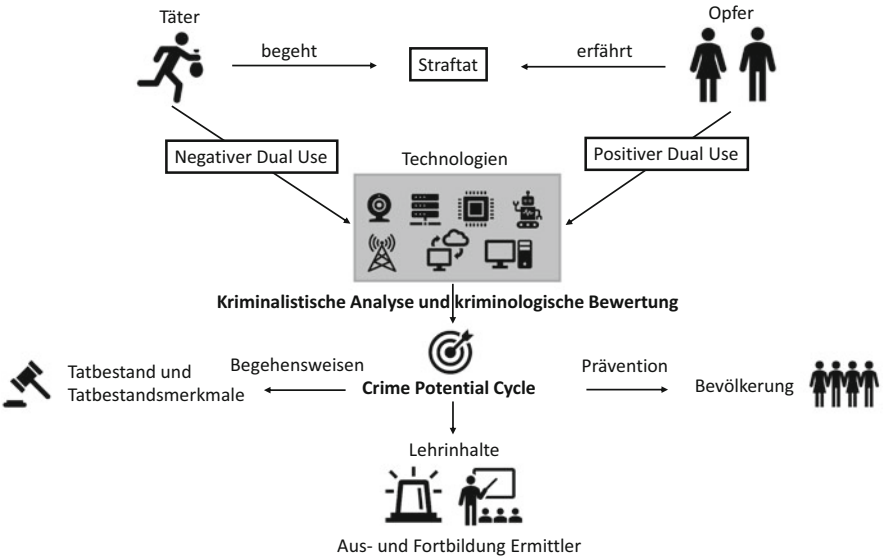

Abb. 6 Verwendung der Ausgabe des Crime Potential Cycle für die Aus- und Fortbildung der Ermittler, der Prävention oder direkt in Ermittlungsverfahren

Maßnahmen für die Prävention vorgeschlagen werden. Dieses Konzept vereinigt über die Technologie die Akteure Opfer, Täter, Ermittler und die beobachtende Bevölkerung.

Das vom BKA (2022) eingerichtete Technologieradar stellt einen ersten Versuch des Monitorings dar. Jedoch können weder alle Perspektiven abgebildet werden, noch kann die technologiegetriebene Ausbildung darauf begründet werden. Die Abb. 7 illustriert ein Modell für die Einbringung neuer Technologien mit einem beobachtbaren *Crime Potential*.

Dabei werden Sachverhalte, die als mögliche Inhalte für eine Ausbildung infrage kommen, von einem Expertenteam bewertet. Das Technologieradar setzte sich aus den Experten zusammen, die in aktuellen Fällen auf den negativen *Dual Use* einer Technologie treffen. Auch wenn diese Ermittler keine forensischen Experten sind, so können sie doch eine Technologie als Eingabe liefern, um diese von dem hier vorgestellten Prozess bewerten zu lassen. Der Prozess sieht vor, dass vorgeschlagene Technologien in einem *Hype Cycle* eingetragen werden. Dazu bewerten die Experten Risiko, Nutzung und Kosten der Technologie, das kriminelle Potential und die Relevanz für aktuelle oder zukünftige Ermittlungen. Damit soll eine auf Daten basierende Empfehlung geschaffen werden, die dann zur Verbesserung der Lehrinhalte beiträgt. Um entsprechende Lehrinhalte zu schaffen, wird eine forensische Lösung und Umsetzung wie in Abb. 2 dargestellt erarbeitet. Das bedeutet, dass hier die Technologien auf gerichtlich verwertbare Spuren untersucht werden, Werkzeuge zum Bearbeiten dieser Spuren beschafft oder erstellt werden und Schulungskonzepte erarbeitet werden. Damit kann dann die Lehre diese Erkenntnisse aufgreifen und ein

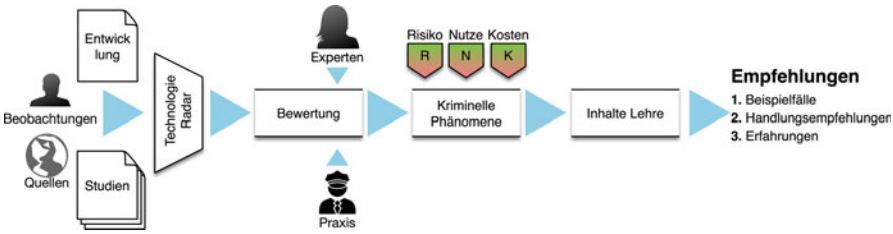

Abb. 7 Prozesses eines technologiegetriebenen Ausbildungskonzepts, bei dem Technologien für die Polizeiarbeit und deren kriminelle Anwendung bewertet werden

Wissen über den Umgang der Strafverfolgungsbehörden mit der neuen Technologie schaffen.

10 Schlussfolgerungen

Wir haben in diesem Kapitel nicht nur festgestellt, dass die Digitalisierung stetig voranschreitet und immer neue Formen von Cyberkriminalität und Digitalen Spuren hervorbringt, sondern auch, dass es nicht mehr sinnvoll ist, den Begriff „Cybercrime im weiteren Sinne" zu verwenden, da heute bei nahezu jeder Straftat auch Informationstechnik verwendet werden. Unsere Analyse der aktuellen Lehrinhalte zeigt, dass die derzeitige Ausbildung im Bezug auf Digitale Spuren in den meisten Bundesländern angepasst werden müsste. Aus der damit einhergehenden Änderung der Curricula ergibt sich die Frage nach einer Herangehensweise. Damit die Inhalte praxisrelevant bleiben und eine zeitnahe Aktualisierung in Zukunft möglich ist, sollte der hier vorgestellte Prozess zukünftig evaluiert werden.

Die Studierenden aller Polizeien müssen durch eine adäquate und zukunftsgerichtete Ausbildung auf ihre tägliche Polizeiarbeit in der immer mehr digitalisierten Welt bestmöglich vorbereitet werden. Die polizeilichen Themengebiete erstrecken sich dabei von Cybercrime, Gewaltkriminalität, Kinderpornografie, Körperverletzung, Organisierte Kriminalität, Raubdelikte, Wirtschaftskriminalität und viele mehr. Allen Themen ist gemein, dass immer mehr Digitalkompetenz benötigt wird. Neue Technologien spielen in diesen und allen Straftatsdelikten eine immer größere Rolle. Deshalb ist es unumgänglich, dass die Wissensvermittlung in der Ausbildung zum einen integriert interdisziplinär verläuft, aber auch technologiebetrieben, sodass grundsätzlich immer die neuesten Entwicklungen aus dem *Crime Potential Cycle* für die Lehre abgeleitet und zeitnah vermittelt werden. Unter dem negativen *Dual Use Potential* bzw. der *Dual Use Probability* verstehen wir im Kontext der Cyberkriminologie das Potential bzw. die Wahrscheinlichkeit des Missbrauchs einer Technologie für kriminelle Zwecke.

Eine umfassende und aktuelle Ausbildung in den Ländern und auch im Bund muss sich an den neuen Technologien ausrichten und sich an der Durchdringung der verschiedenen Perspektiven der jeweiligen Technologie messen lassen. Die Gesamtschau der Cyberkriminologie umfasst Opfer, Täter, Ermittlungsbehörden und die

beobachtende Bevölkerung. Die Ermittlungsbehörden können diese Gesamtschau durch die Einbeziehung neuer Technologien und Phänomene durch ein technologiegetriebenes Ausbildungskonzept unterstützen. Dieses Konzept basiert auf einem ständigen Monitoring und der Bewertung des *Crime Potential* und dem daraus entwickelten *Crime Potential Cycle*. Die Autoren sprechen sich für die Einrichtung einer Expertenkommission aus, die regelmäßig neue Technologien bewertet und Empfehlungen zur Anpassung der Lehre ausspricht.

Die Durchdringung der Gesellschaft und damit auch der Straftaten durch Informationstechnik muss nach Ansicht der Autoren nicht nur den Beamtinnen und Beamten im operativen Vollzug, sondern auch dem Führungspersonal vermittelt werden. Konkret bedeutet dies, dass entsprechende Kenntnisse im Masterstudiengang „Öffentliche Verwaltung – Polizeimanagement“ an der Deutschen Hochschule der Polizei in Hiltrup vermittelt werden sollten.

In einem nächsten Schritt könnten die Ausbildungsinhalte aller Bundesländer auf dem Gebiet der Digitalen Spuren umfassend gegenübergestellt werden, um auch die Fortbildung einzubeziehen. Bei Lehreinheiten, in denen Cyberkriminalität neben anderen Themen behandelt werden, könnten die Lehrenden zu den jeweiligen Stundenanteilen befragen werden, um ein genaues Bild des fachspezifischen Umfangs der Lehre zu erhalten. Anschließend kann aus den Erkenntnissen ein bundeseinheitliches polizeispezifisches Kompetenz-Framework Digitale Spuren entwickelt werden, das auf bewährten Kompetenzstrukturmodellen aufbaut (Schecker & Parchmann, 2006). Dieses müsste in das Aus- und Fortbildungskonzept des Bundes und der Länder eingeordnet werden.

Literatur

Alzubaidi, A. (2021). *Recent advances in android mobile malware detection: A systematic literature review*. IEEE Access.

Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems, 8*(4), 3.

BKA. (2015). Täter im Bereich Cybercrime – Eine Literaturanalyse. Bundeskriminalamt (BKA), Kriminalistisches Institut, Forschungs- und Beratungsstelle Cybercrime KI 16, Stand: 04.12.2015. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015TaeterImBereichCybercrime.html. Zugegriffen am 20.01.2022.

BKA. (2021). Bundeslagebild Cybercrime 2020. Bundeskriminalamt. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.pdf?__blob=publicationFile&v=4. Zugegriffen am 14.01.2022.

BKA. (2022). Technologien. https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/technologien_node.html. Zugegriffen am 31.01.2022.

BMI. (2021). Polizeiliche Kriminalstatistik 2020 – Ausgewählte Zahlen im Überblick. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/pks-2020.pdf?__blob=publicationFile&v=2. Zugegriffen am 30.01.2022.

Brown, R. (1992). „Managing the „S“ Curves of Innovation“. *Journal of Business & Industrial, Marketing 7*(3), 41–52.

Brundage, M. A., Clark, S., et al. (2018). The malicious use of artifcial intelligence: Forecasting, prevention, and mitigation. arXiv:1802.07228. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf. Zugegriffen am 31.01.2022.

Chen, X., & Han, T. (2019). Disruptive technology forecasting based on gartner hype cycle. In *2019 IEEE Technology & Engineering Management Conference (TEMSCON)*.

ECTEG. (2021). European Cybercrime Training and Education Group. https://www.ecteg.eu/. Zugegriffen am 30.12.2021.

EP & ER. (2021). Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20. Mai 2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck (Neufassung). https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021R0821&from=DE. Zugegriffen am 29.01.2022.

Evans, C. (1998). Daktyloskopie – Die Analyse von Fingerabdrücken. In *Die Leiche im Kreuzverhör*. Springer Basel AG.

Feltes, T. (2003). Täter und Tätertypen. Studienbrief in der Reihe „Kriminologie", VdP-Verlag, Hilden 1995, überarbeitet 2003. https://www.thomasfeltes.de/pdf/veroeffentlichungen/TaeterUndTaetertypen1995.pdf. Zugegriffen am 20.01.2022.

Feltes, T., & Kerner, H.-J. (2015). Kriminologie-Lexikon ONLINE. Kooperationsprodukt des Lehrstuhls für Kriminologie, Kriminalpolitik und Polizeiwissenschaft der Ruhr-Universität Bochum und des Instituts für Kriminologie der Universität Tübingen. http://www.krimlex.de/artikel.php?BUCHSTABE=O&KL_ID=130. Zugegriffen am 29.01.2022.

Herbst, M. (2017). Alter Wein in neuen Schläuchen? Neue Formen der Fortbildung im Deliktsfeld Cybercrime bei der Polizeiakademie Niedersachsen. In W. Honekamp & R. Povalej (Hrsg.), *Polizei-Informatik 2017*. Rediroma.

Honekamp, W. (2018). Cybercrime: Aktuelle Erscheinungsformen und deren Bekämpfung. In H. J. Lange, T. Model & M. Wendekamm (Hrsg.), *Zukunft der Polizei. Trends und Strategien*. Springer VS.

Honekamp, W., Povalej, R., Rittelmeier, H., & Labudde, D. (2020). Bekämpfung von Cybercrime durch die Polizei. In G. R. Wollinger & A. Schulze (Hrsg.), *Handbuch Cybersecurity für die öffentliche Verwaltung*. Kommunal- und Schul.

Jahren, J. H. (2020). *Is the quality assurance in Digital Forensic work in the Norwegian police adequate?* [Master's Thesis. Faculty of Information Technology and Electrical Engineering. Norwegian University of Science and Technology, Oslo].

Johnson, M. P. (2012). Community-based operations research: Introduction, theory, and applications. In M. Johnson (Hrsg.), *Community-based operations research* (International Series in Operations Research & Management Science, Bd. 167). Springer. https://doi.org/10.1007/978-1-4614-0806-2_1. Zugegriffen am 29.01.2022.

Johnson, M. P. (2014). Data, analytics and community-based organizations: Transforming data to decisions for community development. March 2014, Conference: Big Data Future. At: Ohio State University. https://www.researchgate.net/publication/263200235_Data_Analytics_and_Community-Based_Organizations_Transforming_Data_to_Decisions_for_Community_Development. Zugegriffen am 29.01.2022.

Johnson, M. P., & Smilowitz, K. (2012). Community-based operations research. In M. Johnson (Hrsg.), *Community-based operations research* (International Series in Operations Research & Management Science, Bd. 167). Springer. https://doi.org/10.1007/978-1-4614-0806-2_2. Zugegriffen am 29.01.2022.

Koch, C. (2021). *Die Fingerabdruckspur und ihre Historie. Daktyloskopie als erfolgreiche Methode der Strafverfolgung*. Grin.

Kou, Y., Lu, C.-T., Sirwongwattana, S., & Huang, Y.-P. (2004). Survey of fraud detection techniques. In *IEEE International Conference on Networking, Sensing and Control, 2004*, Bd. 2, S. 749–754. https://doi.org/10.1109/ICNSC.2004.1297040. Zugegriffen am 29.01.2022.

Kunze, D. (2018). Basiskompetenzen im Bereich Cybercrime und Digitale Spuren. In T. G. Rüdiger & P. Bayerl (Hrsg.), *Digitale Polizeiarbeit*. Springer VS.

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems, 12*(1), 50.

Locard, E. (1930). *Die Kriminaluntersuchung und ihre wissenschaftlichen Methoden* (S. 139). Kameradschaft. (frz. Originalausgabe 1920: Locard, E: *L'enquête criminelle et les méthodes scientifiques*).

Ludwig, A., & Labudde, D. (2021). Ansätze für die Dunkelfeldforschung: Möglichkeiten von Simulationen auf Grundlage der PKS. In W. Honekamp, R. Povalej, H. Rittelmeier, S. Berner, J. Fähndrich & D. Labudde (Hrsg.), *Polizei-Informatik 2021*. Rediroma.

Midgley, G., Johnson, M. P., & Chichirau, G. (2018). What is community operational research? *European Journal of Operational Research, 268*(3), 771–783. https://doi.org/10.1016/j.ejor.2017.08.014. Zugegriffen am: 29.01.2022.

Newton, I. (1739). *Philosophiae naturalis principia mathematica: Tomus Primus*. Holding library: Max Planck Institute for the History of Science, Library; Permanent URL (S 63). http://echo.mpiwg-berlin.mpg.de/MPIWG:7S5THXPK. Zugegriffen am 29.01.2022.

O'Leary, D. E. (2008). Gartner's hype cycle and information system research issues. *International Journal of Accounting Information Systems, 9*(4), 240–252.

Politihogskolen. (2021). Nordic Computer Forensic Investigators. https://www.politihogskolen.no/en/post-graduate/nordic-computer-forensic-investigators/. Zugegriffen am 30.12.2021.

Povalej, R. (2019). Digital Natives vs. Digital Naive – Sensibilisierung in der polizeilichen Ausbildung. In W. Honekamp & E. Kühne (Hrsg.), *Polizei-Informatik 2019*. Remscheid.

Povalej, R., Rittelmeier, H., Fähndrich, J., Berner, S., Honekamp, W., & Labudde, D. (2021). Die Enkel von Locard. *Informatik-Spektrum, 44*, 355–363.

RKI. (2013). Hausverfügung: Dual-Use-Potenzial in der Forschung. Robert Koch Institut (RKI) Stand: 25.03.2013. https://www.rki.de/DE/Content/Forsch/Dual-Use-Risiken/hausverfuegung.html. Zugegriffen am 29.01.2022.

Schecker, H., & Parchmann, I. (2006). Modellierung naturwissenschaftlicher Kompetenz. *Zeitschrift für Didaktik der Naturwissenschaften, 12*(1), 45–66.

Trültzsch, S. (2009). *Kontextualisierte Medieninhaltsanalyse*. VS Verlag für Sozialwissenschaften.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273–315.

Wigand, B. (2018). Fingerabdrücke. https://www.planet-wissen.de/gesellschaft/verbrechen/kriminalistik/fingerabdruecke-100.html. Zugegriffen am 12.01.2022.

Williams, J. (2012). *Good practice guide for digital evidence*. Association of Chief Police Officers. https://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf. Zugegriffen am 30.12.2021.

Prof. Dr. Wilfried Honekamp studierte Informatik an der Universität der Bundeswehr München sowie Defence Simulation and Modelling (MSc) am Royal Military College of Science in Shrivenham, Großbritannien und promovierte in den Gesundheitswissenschaften an der Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik (UMIT) in Hall in Tirol, Österreich. Er war viele Jahre lang Lehrbeauftragter für die Module Intelligente Systeme und Betriebssysteme sowie Intelligent Systems an der Hochschule Bremen und übernahm 2010 die Professur für Softwaretechnik und Programmierung an der Hochschule Zittau/Görlitz. Hier lehrte und forschte Prof. Honekamp zu Software Engineering und Medizinischer Informatik. Im November 2014 wechselte er auf die Professur für Angewandte Informatik an der Hochschule der Akademie der Polizei Hamburg. Seine Schwerpunkte in Lehre und Forschung bildeten u. a. Cybercrime, Forensische Informatik und IT-Sicherheit sowie IT-Systeme und -Verfahren der Polizei. Im Rahmen des Forschungsprojekts HITS-Moni wurde Prof. Honekamp im August 2018 zum Gastprofessor im Fachbereich Informatik der Universität Hamburg ernannt. Von Oktober 2018 bis Mitte 2020 war Prof. Honekamp Gastforscher an der Fakultät für Betriebswirtschaft der Universität Hamburg. Im Oktober 2020 übernahm er die Professur für Cloud-Computing und DevOps an der Hochschule Stralsund. Seit Juli 2021 ist er Dekan der Fakultät für Elektrotechnik und Informatik.

Dr. Roman Povalej ist seit 2015 Professor für Informations- und Kommunikationstechnik und Cybercrime an der Polizeiakademie Niedersachsen. Er ist neben seinen Dozenten- und

Forschungsaufgaben in mehreren Gremien aktiv. Zu seinen Themenschwerpunkten gehören die Polizei-Informatik, Geoinformatik, Cybercrime, Digitale Spuren und Massendaten sowie Künstliche Intelligenz, immer in der Anwendung im polizeilichen Kontext. Dabei legt er großen Wert auf die kontinuierliche Verbesserung und den nachhaltigen Wissenstransfer in die polizeiliche Praxis. In der Fortbildung ist er Ansprechpartner für Themen der IT-Spezialisten und Sachbearbeitende Cybercrime im weiteren Sinne sowie im engeren Sinne. Ein besonderes Anliegen ist Roman Povalej das Fördern, Stärken und Voranbringen der Polizei-Informatik. Deshalb engagiert er sich von Anfang an sehr stark für die Fachtagungsreihe Polizei-Informatik, die seit 2016 jährlich stattfindet.

Heiko Rittelmeier schloss das Studium zum gehobenen Polizeivollzugsdienst in Bayern an der Hochschule für Öffentliche Verwaltung – Fachbereich Polizei – als Diplom-Verwaltungswirt (FH) ab. Später studierte er nebenberuflich Digitale Forensik an der Hochschule Albstadt-Sigmaringen und beendete das Studium mit einem Abschluss als Master of Science. Es folgten umfangreiche Schulungstätigkeiten für verschiedene Behörden im digitalforensischen Kontext. Daneben konnte er Erfahrungen in der Beratung von mittelständischen Unternehmen sammeln und wird von unterschiedlichen Staatsanwaltschaften und privaten Firmen als Sachverständiger mit der Erstellung von Gutachten im Bereich „Digitale Forensik“ beauftragt. Im Bereich der Strafverfolgung leitete er zuletzt ein Cybercrime-Kommissariat mit angeschlossener Forensik, bevor er als Leiter des Referats „Digitale Forensik – Services“ zur ZITiS wechselte.

Prof. Dr. Johannes Fähndrich ist Fachgruppenleiter in der Fachgruppe Angewandte Informatik, Cybercrime und Digitale Spuren an der Hochschule für Polizei Baden-Württemberg. Er leitet den Studiengang K-IT für die Ausbildung von Polizisten mit Spezialisierung für digitale Spuren. Er ist dabei Forscher im Bereich Starke Künstliche Intelligenz, Verteilte Künstlicher Intelligenz, Maschinelles Lernen, Datenanalyse, Pragmatische künstliche Bedeutung, Automatische Heuristik & Abstraktion sowie symbolische und konnektionistische Repräsentation von Bedeutung. Johannes Fähndrich ist PC-Mitglied unter andrem bei der IJCAI und der AAMAS, wurde mehrfach international wissenschaftlich ausgezeichnet und bringt sich in der Gesellschaft für Informatik als Sprecher der Fachgruppe Computational Intelligence ein. Er studierte am KIT bis 2010 Informatik, arbeitete am FZI als Hilfswissenschaftler und nach seinem Abschluss bei Seeburger in der Forschungsabteilung. Danach schloss er 2018 seine Promotion an der TU-Berlin ab und vertiefte sein Wissen noch ein Jahr als Post-Doc am Distributed Artificial Intelligence Lab.

Silvio Berner studierte an der Technischen Universität Dresden im Magisterstudiengang Informatik und Wirtschafts- und Sozialgeschichte. Anschließend arbeitete er zunächst als Field Support Engineer, später als Berater für Informationssicherheit bei der Bundesdruckerei in Berlin. Im November 2013 wechselte er zur T-Systems MMS nach Dresden, wo er als Consultant für IT-Security and Data Privacy tätig war. Seine Schwerpunkte lagen hier in den Bereichen Cloud Security und im Aufbau von ISMS nach BSI IT-Grundschutz und ISO27001. Am 1. Oktober 2015 begann er einen Vorbereitungsdienst an der Hochschule der Sächsischen Polizei (FH) zum Kriminalkommissar, mit Schwerpunkt Computer- und Internetkriminalität. Nach seinem Abschluss 2016 war er im Cybercrime Competence Center des LKA Sachsen als Sachbearbeiter der Zentralen Ansprechstelle Cybercrime, sowie als Teilprojektleiter im Projekt IT-Forensik.2020 tätig. Seit Januar 2020 ist er als Dozent an der Hochschule der Sächsischen Polizei (FH) eingesetzt. Zugleich hat er die kommissarische Leitung des Studienbereich Polizeiliche Informatik und die Lehrgangsleitung Computer- und Internetkriminalitätsdienst inne.

Dirk Labudde ist seit 2009 Professor für Bioinformatik an der Hochschule Mittweida und gründete 2014 Deutschlands ersten Bachelorstudiengang „Allgemeine und Digitale Forensik“ zu welchem er ebenfalls 2014 zum Professor berufen wurde. Seit 2017 ist er außerdem Leiter des Lernlabors Cybersicherheit der Fraunhofer Academy. An der Hochschule Mittweida leitet er darüber hinaus die Forschungsgruppe FoSIL (Forensic Science Investigation Lab), welche sich mit den verschiedensten forensischen Fragestellungen beschäftigt. Der Kern liegt in der

Identifikation von aus forensischer- bzw. Sicherheitssicht relevanten, innovativen Technologien und deren Verbindung mit agilem Wissensmanagement zu Werkzeugen für die Forensische Praxis bzw. den Einsatz im interdisziplinären Management im Krisen- und Katastropheneinsatz. In diesem Zusammenhang ist Prof. Labudde auch als Gutachter vor Gericht, sowie als Berater für Polizeien und Staatsanwaltschaften tätig. Von 1988 bis 1997 studierte er zunächst Theoretische und Medizinische Physik an der Universität Rostock, am College Enschede (Niederlande) und an der Universität Kaiserslautern. Im Jahr 1993 erhielt er sein Diplom und 1997 promovierte er in Theoretischer Physik. In dieser Zeit arbeitete er außerdem als Dozent an der Medizinischen Fakultät in Neubrandenburg. Für seine herausragenden Tätigkeiten in Lehre und Forschung erhielt er 2014 u. a. den sächsischen Lehrpreis und wurde 2018 Fellow der IARIA.