Dirk Labudde
Michael Spranger *Hrsg.*

Forensik in der digitalen Welt

Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt

Springer Spektrum

Forensik in der digitalen Welt

Dirk Labudde · Michael Spranger
(Hrsg.)

Forensik in der digitalen Welt

Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt

Springer Spektrum

Herausgeber

Dirk Labudde
University of Applied Sciences Mittweida
Mittweida, Deutschland

Michael Spranger
University of Applied Sciences Mittweida
Mittweida, Deutschland

ISBN 978-3-662-53800-5 ISBN 978-3-662-53801-2 (eBook)
DOI 10.1007/978-3-662-53801-2
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Spektrum

Planung: Sarah Koch

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer Spektrum ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer-Verlag GmbH Germany
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Im allgemeinen halte man aber an dem Satze fest, daß Egoismus, Faulheit und Eitelkeit die einzigen Triebfedern im Menschen sind, auf die man sich stets und unbedingt verlassen kann.
Dr. jur. Hanns Gross (1847–1915)

Geleitwort

Die Erfahrungen der vergangenen Jahre bei der Bekämpfung des Kriminalitätsphänomens Cybercrime haben gezeigt, dass der zeitgemäßen Forschung und Entwicklung, der Lehre und praxisbezogenen Anwendung sowie der Aus- und Fortbildung im Bereich der polizeilichen Informationssicherheit auf hohem Niveau auch in Zukunft eine herausragende Bedeutung zukommt. Moderne Technologien stellen Ermittlungsbehörden und Gesetzgeber vor immer neue Herausforderungen. Dieselben Technologien, die Straftäter bei der Begehung von Straftaten nutzen, müssen Behörden zur Verfügung stehen und von diesen beherrscht werden können, um auf Augenhöhe Kriminalität zu bekämpfen. Die Cyberkriminalität dabei als singuläres Problem neben anderen Kriminalitätsformen zu betrachten, ist nicht zielführend. Es bedarf vielmehr einer ganzheitlichen Betrachtung, welche die Cyberkriminalität als eingebettetes Phänomen der realen Welt begreift. Die richtungsweisende Entwicklung neuer Methoden zur Kriminalitätsbekämpfung kann deshalb nur in enger Zusammenarbeit von Forschungsinstitutionen und Ermittlungsbehörden erfolgreich sein.

Dresden, Juli 2016

Klaus Fleischmann
Generalstaatsanwalt
Freistaat Sachsen

Geleitwort

Viele der klassischen Kriminalitätsfelder verlagern sich teilweise oder auch ganz ins Internet, viele Straftaten werden mit dem „Tatmittel Internet“ begangen. Straftäter aller Couleur nutzen zur Begehung ihrer Taten die neuesten technischen Möglichkeiten, die weltweite elektronische Vernetzung sowie verschiedenste Mittel und Methoden der Anti-Forensik – das alles länderübergreifend und arbeitsteilig. In diesen Deliktfeldern ist eine kontinuierlich steigende Kriminalitätsentwicklung zu bilanzieren, ganz zu schweigen von der sehr hohen Dunkelziffer. Dem gegenüber stehen die Mitarbeiterinnen und Mitarbeiter der Strafverfolgungsbehörden, die u. a. mit den Mitteln und Methoden der Computerforensik Beweise sichern und bewerten, kausale Zusammenhänge zwischen Tätern und Straftat erkennen und schlussendlich solche Straftaten aufklären müssen. Eine der großen Herausforderungen ist bereits die reine Quantität der zu bearbeitenden Fälle und somit der beschlagnahmten Asservate, ganz abgesehen von der zunehmenden Heterogenität der im Zusammenhang stehenden Datenformate. Cloud-Forensik, Netzwerk-Forensik und Forensik der sozialen Netzwerke sind weitere große, bis dato in ihrem Umfang noch gar nicht absehbare und zusätzliche Baustellen. Mit den bisherigen Mitteln, aber insbesondere auch den bisher genutzten Methoden der klassischen Datenträgerforensik, ist dem nicht zu begegnen, neue Mittel und Methoden – manchmal auch außerhalb der klassischen Denkweise – sind gefragt. Und hier setzt dieses Buch an: Die Autoren, alle aus der Wissenschaft stammend, haben durch ihre tägliche Zusammenarbeit mit verschiedensten Strafverfolgungsbehörden eine „kriminalpolizeiliche Denkweise“ entwickeln können, die sie in ihre originäre Forschungsarbeit auf dem Gebiet der Forensik einfließen lassen. „Bücher über Datenträgerforensik gibt es genügend.“ – könnte man meinen. Dass dies nicht stimmt, beweist dieses Buch und macht neugierig auf eine wissenschaftlich untersetzte kriminalpolizeiliche Denkweise im Bereich der modernen Forensik.

Berlin, September 2016

Ronald Schulze
Geschäftsführer IT-Expertenkreis
Bund Deutscher Kriminalbeamter (BDK)

Vorwort

Wir leben in einer Welt, deren Technologien geprägt sind vom schnellen Wandel und kurzen Lebenszyklen. Eine Innovation jagt die nächste und heute gelerntes ist morgen bereits veraltet. Genau dieser Umstand spielt Straftätern in die Hände. Sie nutzen kurzfristig neue Technologien zum Planen, Verabreden und Begehen von Straftaten. Dabei sind sie den Strafverfolgungsbehörden immer einen Schritt voraus. Auf der anderen Seite bieten eben diese Technologien dem Forensiker neue Quellen und Methoden der Informationsgewinnung sowie neue Möglichkeiten Hintergründe aufzuklären und Zusammenhänge aufzudecken. Der steigende Grad der Digitalisierung zwingt Ermittlungsbehörden umzudenken, Wege zu finden, in der virtuellen und realen Welt zu ermitteln. Da die virtuelle Welt, der Cyberspace, nicht losgelöst von der realen Welt existiert, ist es notwendig, die Informationen aus den Daten beider Welten zu verbinden, um ein vollständiges Bild einer Straftat zu erhalten. Die einschlägige Fachliteratur beschäftigt sich aber zumeist mit Fragen der Auswertung klassischer oder digitaler Spuren. Diese Lücke soll mit dem vorliegenden Buch geschlossen werden.

Für wen ist dieses Buch

Es soll Ermittlungspersonen zeigen, welche Möglichkeiten der digitalen und digitalisierten Untersuchung von Straftaten aktuell existieren, welche Tendenzen sich in der Forschung abzeichnen und welchen rechtlichen Fragestellungen mit den aktuellen Entwicklungen einhergehen. Es ist ein Buch für forensische Praktiker, die ihren Blick nach vorn richten müssen, um vor allem Fälle mit hoher gesellschaftlicher Brisanz schnell und mit allen technologisch zur Verfügung stehenden Mitteln untersuchen zu können. Auf der anderen Seite bietet es einen breiten Einstieg in Themenkomplexe der digitalen und computergestützten Forensik für Wissenschaftler, die bei der Weiterentwicklung dieser hochkomplexen Thematiken mitwirken wollen.

Über die Herausgeber

Die Herausgeber und ein Teil der Autoren beschäftigen sich als Leiter bzw. forschende Mitglieder der Arbeitsgruppe FoSIL (Forensic Sciences Investigation Lab) an der Hochschule Mittweida, aus der Sicht der Informationstechnologien und der digitalen Forensik, mit aktuellen Themen aus der sicherheitsrelevanten Forschung. Der Schwerpunkt liegt

dabei auf 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 beim interdisziplinären Management im Krisen- und Katastropheneinsatz. Einzellösungen werden darüber hinaus und im Sinne eines Resilienz-Engineering-Ansatzes zu einer Basis für eine grundlegende, technische Infrastruktur für prozessbasiertes-und IKT-gestütztes Wissensmanagement zur Krisenprävention und -bewältigung weiterentwickelt. Getrieben von aktuellen Forschungsergebnissen werden im Studiengang „Allgemeine und digitale Forensik“ Methodenkompetenzen in der forensischen Fallarbeit vermittelt. Das Studium ist angelehnt und in seinen Ausprägungen orientiert am Locard'schen Prinzip. Absolventen sind in der Lage in der Wirtschaft und in Strafverfolgungsbehörden als Experten die Entwicklung innovativer Technologien zur Kriminalitätsbekämpfung voranzutreiben.

Aufbau des Buches

Nach einer Einführung in die Welt der modernen Forensik und der daraus resultierenden Verbindung zwischen virtueller und realer Welt in Kap. 1 richten wir in den Kap. 2–4 unseren Blick in Richtung der Anwendbarkeit moderner Technologien zur Untersuchung klassischer Spuren und der Rekonstruktion von Tatorten und Tatabläufen. Anschließend betrachten wir in den Kap. 5–8 das weite Feld der digitalen Spuren von ihrer Sicherung bis hin zur inhaltlichen Analyse ausgewählter Spurenarten. Das Zusammenführen von digitalen und digitalisierten Spuren steigert die Heterogenität des Untersuchungsmaterials und damit die Komplexität der Auswertung enorm. Kap. 9 zeigt aktuelle mathematische Ansätze zum Umgang mit dieser Problematik. Den Abschluss bildet Kap. 10, eine Darstellung der Herausforderungen und aktuellen rechtlichen Lage im Spannungsfeld der Forensik im digitalen Zeitalter.

Mittweida, *Dirk Labudde*
Juli 2016 *Michael Spranger*

Danksagung

An dieser Stelle möchten wir uns ganz herzlich bei allen Autoren und Autorinnen bedanken, die durch ihre unermüdliche Forschungsarbeit die Forensik vorangetrieben und mit ihrem Engagement die inhaltliche Ausgestaltung dieses Buches unterstützt haben.

Weiterhin gilt unser besonderer Dank der Staatsanwaltschaft Chemnitz für die Bereitstellung von forensischem Untersuchungsmaterial zum Zweck der forensischen Forschung sowie dem Bund Deutscher Kriminalbeamter (BDK) für die Unterstützung beim Aufbau eines deutschen forensischen Kooperationsnetzwerkes.

Abkürzungsverzeichnis

m. w. N.	mit weiteren Nachweisen
StPO	Strafprozessordnung
StGB	Strafgesetzbuch
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TKÜV	Telekommunikationsüberwachungsverordnung
GG	Grundgesetz
BGH	Bundesgerichtshof
EMRK	Europäische Menschenrechtskonvention
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz)
ATDG	Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz)
UrhG	Urheberrechtsgesetz
GVG	Gerichtsverfassungsgesetz
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IPBPR	Internationaler Pakt über bürgerliche und politische Rechte
IRG	Gesetz über internationale Rechtshilfe
CSI	Crime Scene Investigation
FAR	False Acceptance Rate
FRR	False Rejection Rate
AFIS	Automatisches Fingerabdruck-Identifizierungssystem
CMOS	complementary metal-oxide-semiconductor
CCD	charge-coupled device

FMR	false matching rate
FNMR	false non-matching rate
OBIE	ontology-based information extraction

Inhaltsverzeichnis

Herausgeber und Mitarbeiter

Herausgeber

Prof. Dr. rer. nat. Dirk Labudde
Lehrstuhl für Bioinformatik und Forensik, Leiter Forensic Science Investigation Lab (FoSIL), University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: labudde@hs-mittweida.de

M. Sc. Inf. Michael Spranger
Wissenschaftlicher Mitarbeiter im Forensic Science Investigation Lab (FoSIL), University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: spranger@hs-mittweida.de

Mitarbeiter

M. Sc. Molekularbiologie Sven Becker
Wissenschaftlicher Mitarbeiter im Forensic Science Investigation Lab (FoSIL), University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: becker1@hs-mittweida.de

Prof. Dr. jur. Frank Czerner
Lehrstuhl Recht in der Sozialen Arbeit, University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: czerner@hs-mittweida.de

Dr. Tina Geweniger
Mitglied der Computational Intelligence Group, University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: tgewenig@hs-mittweida.de

Prof. Dr. rer. nat. Christian Hummert
Inhaber des Lehrstuhls für IT-Sicherheit/Digitale Forensik, University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: hummert@hs-mittweida.de

Dr. rer. nat. Marika Kaden
Mitglied der Computational Intelligence Group, University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: kaden1@hs-mittweida.de

Prof. Dr. Dr.-Ing. Hartmut Luge
Lehrstuhl für Kommunikationstechnik, University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: luge@hs-mittweida.de

Prof. Dr. rer. pol. Pawlaszczyk
Lehrstuhl Informatik/Objektorientierte Softwareentwicklung, University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: pawlaszc@hs-mittweida.de

M. Sc. Molekularbiologie Anne-Marie Pflugbeil
Wissenschaftliche Mitarbeiterin im Forensic Science Investigation Lab (FoSIL), University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: pflugbei@hs-mittweida.de

OA Dr. med. Karlheinz Thiele
Gesundheitsamt – Landkreis Zwickau, Werdauer Straße 62, 08056 Zwickau, Deutschland,
E-Mail: karlheinz.thiele@landkreis-zwickau.de

Prof. Dr. rer. nat. habil. Thomas Villmann
Lehrstuhl für Computational Intelligence, University of Applied Sciences Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland,
E-Mail: thomas.villmann@hs-mittweida.de

Einführung

1

Dirk Labudde, Frank Czerner und Michael Spranger

1.1 Forensik – ein aktueller Ein- und Rückblick und der CSI-Effekt

Ein Blick in die menschliche Natur zeigt, dass eine große Anziehungskraft in Bezug auf Verbrechen und deren Aufklärung existiert. Diese Phänomene haben sich auch die Medien zu eigen gemacht und benutzen diese Eigenschaft oder auch Schwäche. Das Fernsehprogramm ist fest in der Hand von ausgefuchsten Polizeibeamten oder Privatdetektiven. Sie bewegen sich oft als Einzelkämpfer über den Bildschirm und lösen ihre Fälle durch Intuition und logischen Spürsinn. Doch Persönlichkeiten, wie „Der Alte", „Derrick", „Kommissar Schimanski" und viele andere gehören der Vergangenheit an. Analysiert man die neuen Serien, unter dem Akronym CSI[1], so rücken immer mehr clevere Wissenschaftler in den Mittelpunkt. Dieser Trend steht für den Begriff *forensische Wissenschaft*. Das forensische Labor steht zunehmend im Mittelpunkt der Ermittlungen. Wissenschaftler arbeiten in Teams und akribisch an den anfallenden Spuren. Sie sind die

[1] Crime Scene Investigation.

D. Labudde (✉)
Lehrstuhl für Bioinformatik und Forensik, Leiter Forensic Science Investigation Lab (FoSIL), University of Applied Sciences Mittweida
Technikumplatz 17, 09648 Mittweida, Deutschland
E-Mail: labudde@hs-mittweida.de

F. Czerner
Lehrstuhl Recht in der Sozialen Arbeit, University of Applied Sciences Mittweida
Technikumplatz 17, 09648 Mittweida, Deutschland
E-Mail: czerner@hs-mittweida.de

M. Spranger
Wissenschaftlicher Mitarbeiter im Forensic Science Investigation Lab (FoSIL), University of Applied Sciences Mittweida
Technikumplatz 17, 09648 Mittweida, Deutschland
E-Mail: spranger@hs-mittweida.de

D. Labudde, M. Spranger (Hrsg.), *Forensik in der digitalen Welt*,
DOI 10.1007/978-3-662-53801-2_1

Beherrscher von forensischen Methoden und Instrumenten, seien es Massenspektrometer, Bedampfungsanlagen oder Mikroskope. An dieser Stelle sei darauf hingewiesen, dass oft tief in die Trickkisten der Filmemacher gegriffen wird. Die Abfolge und zeitliche Aufteilung der Analysen sind stark überzeichnet und oft wird das gesamte Expertenwissen in einer Person vereint. Nicht zuletzt tauchen Begriffe wie *Cybercrime*, *Profiling* oder *Predictive Policing* in Serien auf.

Jedoch bleiben diese Serien nicht ohne Folge. In der Literatur wird über den „CSI-Effekt" diskutiert, welcher verschiedene Auswirkungen auf das Erscheinungsbild von Ermittlungen in der Gesellschaft hat. So wird beispielsweise jeder Zuschauer zu einem Experten und erwirbt so ein scheinbares Recht, an der allgemeinen Diskussion und Beurteilung von realen Verbrechen teilzunehmen. Die Veranschaulichung der Unfehlbarkeit der forensischen Wissenschaft durch den „CSI-Effekt" setzt die Ermittlungsbehörden stark unter Druck. Die Faszination, die von diesen Serien ausgeht, führt zu einer hohen Nachfrage an Büchern und Materialien, die sich ernsthaft mit den forensischen Wissenschaften auseinandersetzen. In Deutschland ist dieses Interesse auch bei Jugendlichen angekommen, und der Ruf nach einer Ausbildung in der Forensik steigt. Universitäten und Hochschulen nehmen diesen Trend auf und schaffen Module mit forensischen Inhalten. Sicher tun sie dies auch aus ganz persönlichen Gründen. Nichts ist für einen Hochschullehrer angenehmer, als ein Hörsaal voller Interessierter. Daneben lässt sich Motivation für die naturwissenschaftlichen Fächer wecken.

Doch wo kommt eigentlich diese Faszination her? Ein kurzer Blick in die Geschichte der klassischen Forensik gibt Aufschluss darüber. Geringe Mengen an Blut, ein latenter Fingerabdruck oder Audiofiles stehen heute am Anfang der Spurenanalyse und können so helfen, Täter zu überführen bzw. Beschuldigte zu entlasten. Man sollte den Fakt berücksichtigen, dass noch im 18. Jahrhundert ein Geständnis durch Folter erzwungen wurde. Ein Pionier, der Beweise in den Mittelpunkt rückte, war der Österreicher Hans Gross[2]. In seinem von 1899 stammenden *Handbuch für den Untersuchungsrichter*, forderte er objektive Befunde und Spuren neben den Aussagen von Beschuldigten und Zeugen als die wichtigsten Beweismittel im Strafverfahren. Dies konnte als Übergang der Subjektivität in eine begründbare Objektivität angesehen werden. „Mit jedem Fortschritt in der Kriminalistik fällt der Wert der Zeugenaussagen, und es steigt die Bedeutung der realen Beweise"[6]. Der französische Mediziner Dr. Edmond Locard[3] formulierte und bewies das bis heute gültige Austauschprinzip. Jeder und alles an einem Tatort nimmt etwas mit und lässt etwas dort zurück [10]. Allgemein definiert man den Tatort als Ort, an dem sich kriminalistisch relevante oder gerichtlich strafbare Handlungen ereignet haben. Der Tatort beschränkt sich nicht auf den Ort des Geschehens oder der Ereignisse, sondern auch auf jene Bereiche, in welchen vor oder nach der Tat relevante Handlungen stattgefunden haben.

[2] * 26. Dezember 1847 in Graz; † 9. Dezember 1915 ebenda.
[3] * 13. Dezember 1877 in Saint-Chamond (Loire); † 4. April 1966 in Lyon.

Der Berliner Polizist Ernst August Ferdinand Gennat[4] gilt als Urvater der Strukturierung von Ermittlungsmethoden. Bis in die 1920er Jahre gab es in der Polizeiarbeit kein Morddezernat, keine Verhörprotokolle und keine Obduktionsberichte. Erst Ernst Gennat konzipierte und strukturierte die Ermittlungsmethoden und konnte so eine überdurchschnittliche Aufklärungsquote erreichen. Diese und viele andere Persönlichkeiten reformierten die Ermittlungsarbeit und ebneten den Weg für die heutige Spurenanalyse und deren Einbindung in die Gerichtsbarkeit. Die moderne forensische Wissenschaft lebt von den Methoden aus den Geistes- und Naturwissenschaften. Mit modernsten Methoden, Techniken und Technologien, wie biologischen, geologischen, geotopologischen, ballistischen und digitalen Aufzeichnungen versuchen heute forensische Experten, Verbrechen aufzuklären, Tatorte und Spuren zu analysieren und den gesamten Tathergang zu rekonstruieren. Im Prozess der Rekonstruktion sollte man auf erkenntnistheoretische Ansätze zurückgreifen und mit der Falsifizierung von Hypothesen arbeiten. Gerade die Forensik profitiert von den Entwicklungen in den angrenzenden Wissenschaften. Der Siegeszug der Computertechnik hat auch Spuren in der Forensik hinterlassen. Dabei ist nicht nur das neue Tatwerkzeug Computer gemeint. Vielmehr ist auch in der Analyse digitaler und digitalisierter Spuren moderne Rechentechnik nicht mehr wegzudenken. Beispiele sind Audio-, Video-, Fotoanalyse und die Möglichkeit der 3D-Rekonstruktion von Tatwerkzeugen und ganzer Tatorte. Auf der anderen Seite können Vergleiche von Spuren durch den Einsatz von Datenbanken sicher und erfolgreich gestaltet werden. Jedoch gehört auch hier eine gesunde Skepsis dazu. Wie in anderen Wissenschaften auch, müssen Ergebnisse nachvollziehbar und verständlich sein.

Ob aus der Presse oder durch eigenes Erleben ist heute jeder mit den Begriffen *Hacking*, *Cybercrime*, *Cyberspace*, *Cybermobbing* oder *digitaler Identitätsklau* in Berührung gekommen. Auch der Begriff Hackerattacke ist in unsere Alltagssprache eingezogen. Der Begriff Hacker hat eine Metamorphose in seiner Begrifflichkeit durchlebt. Waren am Anfang damit besondere Tüftler gemeint, so wird er heute im Zusammenhang mit Cyberverbrechen benutzt. In den 1960er Jahren tauchte der Begriff Hacker zum ersten Mal in den USA am MIT (Massachusetts Institute of Technology) auf. Hier wurde ein Team von Studenten als Hacker betitelt, die Maschinen auseinanderbauten, um sie im Anschluss umzubauen. Ziel war neben dem haptischen Gefühl, eine deutliche Leistungssteigerung. Es wurden keine umtriebigen Absichten mit diesen Arbeiten verfolgt. Das Jahr 1969 kann als Geburtsstunde des Hackens gesehen werden. Wie so oft in der technischen Entwicklung wurde auch dieses Ereignis durch einen Zufall gefördert. Der Amateurfunker John Thomas Draper[5], später als „Captain Crunch“ bezeichnet, entdeckte, dass eine Spielzeugpfeife, welche in Frühstücksflocken der Marke Captain Crunch als Werbegeschenk enthalten war, benutzt werden kann um einen Ton (2600 Hz) zu erzeugen, der Ferngespräche freischaltete. Dieser Tipp machte die Runde und schon konnten Freunde und Bekannte kostenlos telefonieren. Von diesem zufälligen Ereignis beflügelt gründete sich

[4] * 1. Januar 1880 in Plötzensee; † 21. August 1939 in Berlin.
[5] * 1944.

einer der ersten Computer Clubs. In den 1980er Jahren sind die Hacker dann aus dem Schatten getreten und wurden auch bald von der breiten Öffentlichkeit wahrgenommen. Der damals erst 17-jährige Kevin Poulsen[6] alias Dark Dante drang in das ARPANET (Vorläufer des heutigen Internets)[7] ein. Jedoch war dies nur dem Militär und den führenden Universitäten vorbehalten. 1983 lief in den Kinos der Streifen „Wargames – Kriegsspiele" von John Badham, hier wurde die Geschichte eines jungen Hackers erzählt. Durch diesen filmischen Katalysator tauchten 1988 die ersten Computerviren auf. Von nun an war der Begriff „Hacker" eindeutig negative belegt. In den 1990er Jahren wurden das gesamte Ausmaß und die dunklen Seiten des Hackens deutlich. Durch das Internet wurden die ersten Straftaten in Bezug auf Cyberkriminalität begangen. Die Gemeinde spaltete sich nun in eine schwarze und weiße Community. Diese Aufspaltung gilt bis zum heutigen Tage. Auf der einen Seite stehen die „Black-Hats", die aus kriminellen Gründen hacken, und auf der anderen die „White-Hats", die vor allem auf Lücken in Sicherheitssystemen hinweisen wollen. Der Umfang und die Schwere der Taten der Black-Hats nahmen bald gewaltige Dimensionen an. Die ersten Fälle von Online-Banking-Missbräuchen gingen durch die Presse. Dies setzte sich in das 21. Jahrhundert fort. Der Begriff „Cracking", das Überwinden von Sicherheitshindernissen, machte die Runde und ergänzte die Cyberkriminalität. Das Kopieren von DVDs und passende Plattformen zum Austausch wurden erschaffen. Aber auch Webseiten wie „WikiLeaks"[8] wurden geschaffen, um sensible und geheime Dokumente der allgemeinen Bevölkerung zugänglich zu machen. Die heutigen Ausprägungen der Hacker und deren Schwerpunktziele sind vielschichtiger geworden. Nachfolgend der Versuch einer Systematisierung der „Hats". Der „Black-Hat" hackt Datensysteme mit der Absicht, Schaden anzurichten oder nimmt diesen zumindest billigend in Kauf. Das Hauptziel eines „White-Hat" ist es, Sicherheitslücken in Systemen aufzudecken mit der Absicht, diese den Verantwortlichen zu melden. Dabei wird mitunter ein entstehenden Schaden in Kauf genommen. Zwischen beiden agiert der „Grey-Hat", der sowohl zur Verbesserung der Systemsicherheit beiträgt als auch Schäden anrichtet. Die Gruppe der Wettstreiter (aus sportlicher Absicht oder zum Zeitvertreib) bekommt den Namen „Script Kiddies". Sie haben kaum technische Kompetenzen und bedienen sich der Tools anderer. Nach dem Motto: Wer will mal ein Hacker sein. Neu ist die Gruppe der „Hacktivisten". Diese setzen ihr technisches Wissen für einen politischen Zweck ein und verändern zum Beispiel eine Homepage, um politische Botschaften zu verbreiten oder um auf Missstände aufmerksam zu machen.

Zum Abschluss noch ein Rat für alle diejenigen, die jetzt überlegen, in welcher Gruppe sie sich selbst wiederfinden: Hacking bringt nicht nur viele neue Freunde, sondern auch genauso viele neue Feinde.

[6] * 1965 in Pasadena, Kalifornien.
[7] Advanced Research Projects Agency Network.
[8] https://wikileaks.org/

1.2 Forensik im System der Wissenschaften

Der Begriff Forensik stammt vom lateinischen Wort *forēnsis* ab und bedeutet so viel wie „im oder vor dem Forum (Marktplatz)“. Historisch gesehen war der Marktplatz oder Mittelpunkt einer urbanen Gemeinschaft oft der Schauplatz der Gerichtsbarkeit. Alle Wissenschaften oder Teildisziplinen einer Wissenschaft können das Adjektiv „forensisch“ tragen. Dies signalisiert den Bezug zum jeweiligen Rechtssystem.

Die **Forensik** umfasst alle Arbeitsgebiete, die strafrechtlich und zivilrechtlich relevante Handlungen identifizieren, ausschließen, analysieren und rekonstruieren.

In Deutschland wird dies vor allem durch die Zusammenarbeit von verschiedenen Fachgruppen und Spezialisten erreicht. In den USA hingegen schließt der Begriff Forensic Science (Forensics) eine spezielle Ausbildung ein, welche kriminalistisches und rechtsmedizinisches Wissen vereint. Beide Betrachtungsweisen deuten auf den Charakter einer Querschnittswissenschaft innerhalb der Naturwissenschaften hin, welche ihren Rahmen von den Rechtswissenschaften vorgegeben bekommt und sich in der Umsetzung auch Methodiken der Ingenieurswissenschaften bedient. Im deutschsprachigen Raum spricht man auch vom System der Kriminalwissenschaften. In diesem ist die Forensik, neben weiteren Wissenschaftszweigen wie Kriminalistik oder Kriminologie, als Teil der nichtjuristischen Kriminalwissenschaften den Naturwissenschaften zugeordnet (Abb. 1.1).

Als empirische, nicht-juristische Kriminalwissenschaft, umfasst die Lehre der **Kriminalistik** sämtliche präventiven und repressiven Maßnahmen sowie damit verknüpfte Techniken, die zur Bekämpfung von Straftaten und des Verbrechertums notwendig sind [5].

Abzugrenzen ist die kriminalistische Lehre von dem Fach der Kriminologie. Letzteres beschäftigt sich mit den Erscheinungsformen und Ursachen von Kriminalität. Ziel der Kriminalistik ist die Ermittlung und Zusammenführung von straftatrelevanten Beweisen. Darüber hinaus sollen Gefahren abgewehrt bzw. Straftaten abgewendet werden. Es können verschiedene Teildisziplinen unterschieden werden [5]:

1. Maßnahmen, welche die Vorgehensplanung bei der Verbrechensbekämpfung implizieren, werden innerhalb von Kriminalstrategien erarbeitet. Dazu werden ebenfalls Vorbeugungsmaßnahmen gezählt.
2. Innerhalb der Kriminaltaktik, als weitere Teildisziplin, werden zweckgebundene Vorgehensplanungen im Rahmen der Verbrechensbekämpfung erarbeitet (z. B. Vernehmungstaktik).

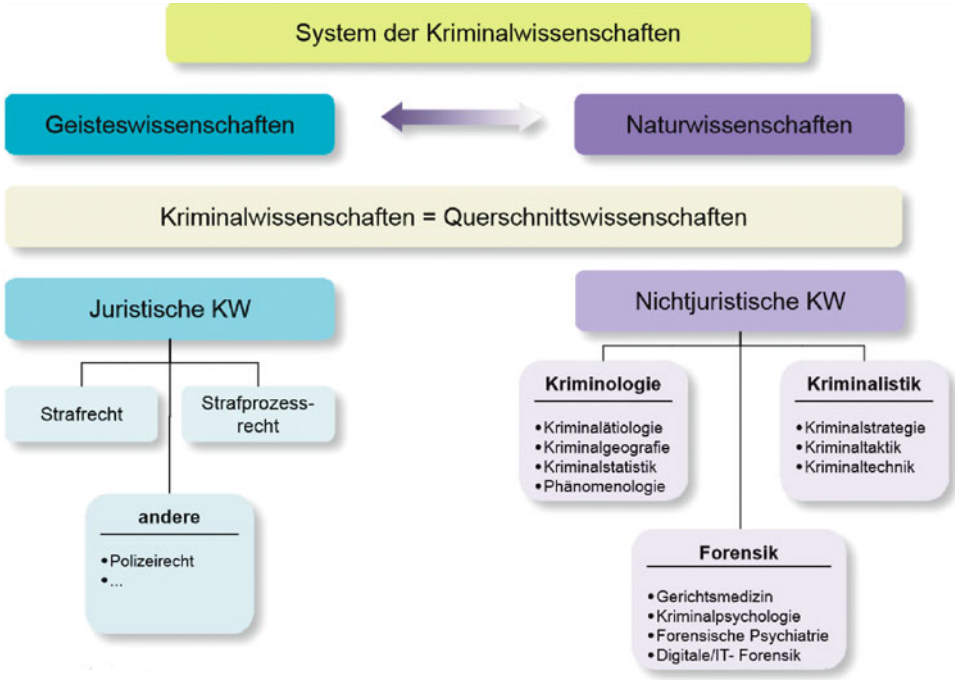

Abb. 1.1 System der Kriminalwissenschaften nach Berthel [1]

3. Die Kriminaltechnik umfasst sämtliche Erkenntnisse und Maßnahmen zur Anwendung wissenschaftlicher und empirischer Resultate in Bezug auf Spurensicherung und -analyse.
4. Die Regelung des Dienstbetriebes sowie die innerhalb spezifischer Richtlinien und Anordnungen geregelte Handhabung kriminalpolizeilicher Mittel fallen in den Bereich der Kriminaldienstkunde.
5. Der Bereich der Kriminalprävention beschäftigt sich mit der Vorbeugung und Früherkennung von Risiken für kriminelles Verhalten.

Eng verknüpft mit der Kriminalistik, stellt die **Kriminologie** als ebenfalls nichtjuristische, empirische Kriminalwissenschaft das geordnete oder systematische Wissen über Verbrechen, Verbrecher, die strafrechtliche Sozialkontrolle sowie das Verbrechensopfer dar. Im Allgemeinen ist darin eine Summierung vielfältiger wissenschaftlicher Beiträge bezüglich Kriminalität und ein in Verbindung damit stehendes Verhalten zu sehen. Im speziellen bestehen Bezüge zum Opfer und zur Kriminalitätsprävention [8].

Die Kriminologie ist eng verzahnt mit diversen Bezugswissenschaften, wie u. a. Psychiatrie, Psychologie, Soziologie, Rechtswissenschaft und Ökonomie.

1.3 Tatort in der modernen Forensik

1.3.1 Der moderne Tatortbegriff

Schauen wir uns das Wort „Tatort" an, so ist dieser in unserer Gesellschaft mit einer negativen Assoziation verknüpft, obwohl beide Begriffe „Tat" und „Ort" mit einer positiven Auffassung verbunden sind.

Seit Bestehen von Gesellschaften ist das Handeln eines jeden Einzelnen an ein definiertes Regelwerk der Gemeinschaft, die Gesetze, Verordnungen und Konventionen, gekoppelt. Dem Staat, als Inhaber des Gewaltmonopols, obliegt es, diese Regelwerke durchzusetzen, Verstöße zu verfolgen und ggf. zu ahnden. Dafür bedarf es jedoch eines Beweises, im Sinne einer eindeutigen Zuordnung eines Tatverdächtigen oder Opfers zu einer konkreten Tat. Dem Auffinden derartiger Beweise bzw. dem Nachweis einer Tat dient, neben der Vernehmung von Beteiligten und Zeugen, vor allem die Untersuchung von Spuren (Daten).

Unter einer Straftat wird gemeinhin ein schwerwiegender Verstoß gegen die Rechtsordnung einer Gesellschaft oder die Grundregeln menschlichen Zusammenlebens verstanden. Allgemein gesprochen handelt es sich um eine von der Gemeinschaft als Unrecht angesehene und von ihrem Gesetzgeber als kriminell qualifizierte und mit Strafe bedrohte Verletzung eines Rechtsgutes durch den von einem oder mehreren Tätern schuldhaft gesetzten, verbrecherischen Akt. Die Rechtswissenschaft versteht unter einem Vergehen/Verbrechen in erster Linie eine strafbare Handlung (Straftat) an sich und als solche. Das Strafgesetzbuch (§ 12 StGB) unterscheidet in Abhängigkeit der Schwere der Tat und der damit verbundenen Strafandrohung Straftaten in Vergehen (Strafandrohung im Mindestmaß unter einem Jahr Freiheitsstrafe oder Geldstrafe) und Verbrechen (Strafandrohung im Mindestmaß von einem Jahr Freiheitsstrafe oder darüber). Gesellschaftswissenschaftlich befasst sich die Kriminologie mit dem Phänomen des Verbrechens und seinen Erscheinungsformen und Ursachen. Mit den Mitteln und Methoden der Verbrechensbekämpfung und -aufklärung beschäftigt sich die Kriminalistik. In diesem Kontext wird der Ort der Tat, also der Ort an dem eine Straftat verübt wurde, als Tatort bezeichnet. Was auf den ersten Blick relativ trivial klingt, ist jedoch bei genauerer Betrachtung oft schwer zu beschreiben. Allgemein definiert man den Tatort als Ort, an dem sich kriminalistisch relevante oder juristisch strafbare Handlungen ereignet haben. Der Tatort beschränkt sich nicht nur auf den Ort des Ereignisses, sondern auch auf jene Bereiche, in welchen vor oder nach der Tat relevante Handlungen stattgefunden haben. Man unterscheidet den unmittelbaren Tatort, an dem die Tat ausgeführt wurde und an dem auch die meisten Spuren (Daten) erwartet werden können sowie den Tatort im weiteren Sinne. Dieser bezieht sich auch auf die nähe-

re Umgebung. Es lassen sich in der klassischen Forensik folgende Abschnitte dem Tatort zuordnen:

- Vorbereitungsort,
- Annährungsort,
- Ereignisort.

Der Begriff Tatort im weiteren Sinn schließt auch den Fundort des Opfers, den Fluchtweg des Täters, das Fluchtfahrzeug, Aufbewahrungsorte von Beute oder Tatwerkzeugen sowie den Wohnort des Tatverdächtigen mit ein. An einem Tatort ist die Wahrscheinlichkeit sehr hoch, fallrelevante Spuren zu finden und diese als grundlegende Beweise aufzubereiten. Spuren im kriminaltechnischen Sinne sind sichtbare oder latente materielle Veränderungen, die im Zusammenhang mit einem kriminalistisch relevanten Ereignis entstanden sind und zu dessen Aufklärung beitragen können. In der Literatur spricht man oft vom Spurenlesen. Eine Annäherung an den Begriff „Lesen“ lässt einen Vorgang oder Prozess erkennen. Dieser Vorgang beschreibt den Transfer von der Ebene der Zeichen (Spur) auf die Ebene der Bedeutung (Beweis). Das abschließende Wissen unterliegt der Kausalität (Ursache-Wirkung) [7]. Diese Ebenen spiegeln sich in der Wissenspyramide wider. Objektive Befunde und Spuren sind neben den Aussagen von Beschuldigten und Zeugen die wichtigsten Beweismittel im Strafverfahren.

Im Zusammenhang mit dem Tatort im klassischen Sinne sind drei Anmerkungen zu Spuren von Bedeutung:

- am Tatort sind Spuren oft noch nicht differenzierbar,
- der Tatbezug kann noch nicht in allen Fällen abgeschätzt werden,
- nicht unmittelbar gesicherte Spuren sind oft unwiderruflich verloren.

Eine koordinierte und gründliche Tatort- und Spurensicherung ist entscheidend für die erfolgreiche und fachgerechte Aufklärung einer Straftat. Es ist dafür zu sorgen, dass der Tatort so wenig wie möglich an Informationen verliert bzw. neue hinzukommen. Informationen ergeben sich aus der Analyse der Spuren (Daten), die in der Phase der Rekonstruktion des Tatortes und des Tatherganges abgeleitet werden. Veränderungen des Tatortes vor dem Eintreffen der Forensikexperten (bewusst oder unbewusst) verursachen Rekonstruktionen, welche im Detail von der Realität abweichen.

Die virtuelle Welt, der Cyberspace, in dem wir uns täglich mehrere Stunden bewegen, führt zwangsläufig zu einer notwendigen Erweiterung bzw. Neudefinition des Begriffs Tatort. Um dies verständlich zu machen, werden nun physische und virtuelle (digitale) Spuren verglichen.

Digitale Spuren (digital evidence) sind Spuren, die auf Daten basieren, welche in Computersystemen gespeichert oder übertragen worden sind [2].

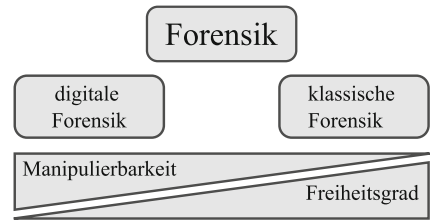

Abb. 1.2 Die Eigenschaft der Manipulierbarkeit ist bei digitalen Spuren (Daten) im Vergleich zu physischen Spuren aus der klassischen Forensik wesentlich größer. Die Eigenschaft Freiheitsgrade verhält sich jedoch umgekehrt

Zunächst sind dies analog zur klassischen Forensik physische Spuren, wie

- Magnetisierung auf der Oberfläche einer Festplatte,
- elektromagnetische Wellen auf einem Datenkabel,
- Ladezustand von Speicherzellen im Hauptspeicher.

An dieser Stelle kann davon ausgegangen werden, dass die Prinzipien der klassischen Forensik anwendbar sind. Die Form der diskreten Repräsentation („Null“ und „Eins“) wird durch verschiedene Anwendungen in eine für den Menschen lesbare Form überführt. Unterschiede zwischen digitalen und analogen (physischen) Spuren existieren gerade in Bezug auf die Eigenschaften Manipulierbarkeit und Freiheitsgrade. Abb. 1.2 demonstriert das Verhältnis dieser Eigenschaften in Bezug auf physische und digitale Spuren. Die Manipulierbarkeit und der Anzahl der Freiheitsgrade sind sich gegenseitig bedingende Eigenschaften. Digitale Spuren unterliegen einer hohen Manipulierbarkeit, was den Raum der Analyse, also das Betrachten der Spuren, einschränkt (Anzahl der Freiheitsgrade in der Analyse).

Digitale Spuren besitzen die folgenden elementaren Eigenschaften:

- Flüchtigkeit
  - persistente, gespeicherte Daten,
  - semipersistente Daten im Arbeitsspeicher,
  - flüchtige Spuren, nur temporär vorhanden,
- technische Vermeidbarkeit (Systemdaten),
- Manipulierbarkeit,
- Kopierbarkeit.

Detaillierte Ausführungen zum Vergleich von digitalen und realen Spuren finden Sie im Buch *Forensische Informatik* [4]. Digitale Spuren haben im Gegensatz zu physischen Spuren einen komplexeren geografischen Aufbau und Entstehungsmechanismus. Dieser setzt sich aus drei ineinandergreifenden Ebenen zusammen: Internet, LAN bzw. WLAN und dem Kerngerät (PC, Smartphone, Tablet). Ein virtueller Tatort oder digitaler Tatort kann somit nur schwer bzw. gar nicht definiert werden. Möglichkeiten einer Definition ergeben sich durch Einbeziehung der geografischen Ebenen. Wenn „Von einem unbekannten

Tatort aus begangenen Cybercrimedelikt“ [3] gesprochen wird, muss sich der unbekannte Tatort auf auf IP-Adressen bzw. MAC-Adressen von verwendeten Geräten einschließlich Servern beziehen. Somit erfolgt eine Zuordnung zu Geräten in einem gesonderten Schritt.

Digitale Ermittlungen unterscheiden sich von herkömmlichen Ermittlungen in der Wahl der verwendeten Werkzeuge. Die allgemeine Vorgehensweise, welche aus drei Phasen besteht und durchgängig von Experten akzeptiert ist, kann direkt auf Ermittlungen in der virtuellen Welt (Cyberspace) übertragen werden. Diese Phasen sind: Sicherung, Analyse und Präsentation (SAP).

Securephase: beinhaltet die sorgfältige Erfassung aller Daten,
Analysephase: sorgfältige Überprüfung und objektive Bewertung der gesicherten Spuren und Beweise,
Präsentationsphase: nachvollziehbare Darlegung des Ermittlungsprozesses.

In der Literatur existiert eine Reihe von weiteren Vorgehensmodellen, die sinnvolle Präzisierungen vornehmen. Abb. 1.3 zeigt verschiedene Vorgehensmodelle in ihren unterschiedlichen Präzisierungen.

An dieser Stelle sei nocheinmal auf eine Abgrenzung der Begriffe Modell, Prozess und Methode im Zusammenhang mit Vorgehensweisen hingewiesen.

Modell:
- Ablauf einer Untersuchung (vereinfachte Weise),
- einzelne Arbeitsschritte,
- gibt keinen Aufschluss über die Schritte innerhalb eines Abschnitts.

Prozess:
- Ablauf in detaillierter Form,
- Abschnitte aus dem Modell in kleine Phasen,
- Reihenfolge des Ablaufs einer Untersuchung.

Methode:
- im Arbeitsschritt eingesetzten Werkzeuge und Verfahren.

Die spezifische, auf eine konkrete Ermittlung ausgerichtete Umsetzung eines Vorgehensmodells muss im Einklang mit den aufgestellten forensischen Hypothesen stehen. In Ermittlungsverfahren, sowohl in der virtuellen als auch in der physischen Welt, sind an den Prozess der Hypothesenentwicklung analoge Bedingungen geknüpft. Aus der Menge der Spuren (Daten, Fakten, Zahlen) werden durch wissenschaftliche Methoden Informationen generiert. Als wissenschaftliche Methoden gelten Verfahren, Algorithmen und