Sonja Stirnimann

Der Mensch als Risikofaktor bei Wirtschaftskriminalität

Handlungsfähig bei Non-Compliance und Cyberkriminalität

2. Auflage

Springer Gabler

Der Mensch als Risikofaktor bei Wirtschaftskriminalität

Sonja Stirnimann

Der Mensch als Risikofaktor bei Wirtschaftskriminalität

Handlungsfähig bei Non-Compliance und Cyberkriminalität

2., vollständig überarbeitete und ergänzte Auflage

Springer Gabler

Sonja Stirnimann
Zug, Schweiz

ISBN 978-3-658-34630-0 ISBN 978-3-658-34631-7 (eBook)
https://doi.org/10.1007/978-3-658-34631-7

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler

Lektorat/Planung: Catarina Gomes de Almeida
Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Für Dich, Maxim!
Es ist immer wieder faszinierend und wunderbar zu beobachten, wie Du – großes kleines Vorbild unserer Gesellschaft – auf neue Themen und Herausforderungen mit Neugier und Begeisterung reagierst!

Vorwort

„Integrity is doing the right thing, even when no one is watching“. (C. S. Lewis)

Wirecard, Greensill, Panama und Paradise Papers, Offshore Leaks, Datenklau und Cyberattacken: Die Medien berichten beinahe täglich aus der Welt der Wirtschaftsdelikte. Im Fokus stehen insbesondere überzeugende, charismatische Persönlichkeiten, die das Vertrauen ihrer Anleger, Aktionäre und Stakeholder aufs Gröbste missbraucht haben, sowie Korruptions- und Bestechungsskandale namhafter Vertreter der Wirtschaft und Politik. Die Vorkommnisse lassen sowohl bei direkt wie indirekt Betroffenen das beklemmende Gefühl zurück, niemandem mehr trauen zu können. Die Handlungsfähigkeit dieser betroffenen Verantwortungsträger ist innerhalb weniger Augenblicke in Gefahr und droht ins Abseits zu gelangen. Von rationalen Entscheidungen fehlt in diesem Moment jede Spur. Zu viele Einflussfaktoren lenken das Verhalten. Die Folgen von Wirtschaftsdelikten, Non-Compliance und Cyberkriminalität sind verheerend.

Die Agenden dieser Verantwortlichen sind voll von Themen, die neben dem Tagesgeschäft und Ausnahmesituationen höchste Aufmerksamkeit fordern, um wettbewerbsfähig zu bleiben. Die folgenden sind nur ein kleiner Ausschnitt davon und veranschaulichen, dass große Entscheidungen anstehen:

- Neue Technologien bedingen ein Überdenken bestehender Geschäftsmodelle. Unternehmen, die noch nicht im digitalen Zeitalter angekommen sind, stehen von verschiedenen Seiten unter großem Druck. Gewisse Verantwortliche lassen sich dann zu Aktionen verleiten, ohne adäquat an die daraus entstehenden Risiken und Konsequenzen zu denken. Nicht zuletzt, weil gewisse Risiken noch zu unbekannt und wenig greifbar sind, um es auf den Risikoradar der Verantwortlichen geschafft zu haben. Mithalten und mitreden können heißt das Credo. Die Verlockung, einem allgemeinen Trend zu folgen, ist groß – und allzu menschlich. Wer es wagt, diese neuen Technologien aus verschiedensten Perspektiven zu beleuchten und – insbesondere gegen die Mehrheit – infrage zu stellen, wird oft als „Spaßbremse“ in die Schranken gewiesen oder zumindest belächelt. Professionelle Skepsis? Oft schneller verpönt als geschätzt. Zu Unrecht, wie

die Realität zeigt. Es bleibt existenziell, die sich verändernden Risiken zu erkennen und den Umgang damit bewusst zu entscheiden.

- Begriffe wie „Artificial Intelligence (AI)“ und „Internet of Things (IoT)“ sorgen vom Generalisten über den Spezialisten bis hin zum Aufsichts- oder Verwaltungsrat und dem Vorstand für erhitzte Gemüter. Wie sieht die Zukunft der eigenen Berufsgattung aus? Wie diejenige der eigenen Daseinsberechtigung? Wie wirken sich die demografischen Veränderungen und die steigende Diversität auf die Risiken wirtschaftskrimineller Handlungen aus? Die globale Vernetzung von Menschen und Objekten schreitet weiter voran und damit die Möglichkeiten und Herausforderungen für Verantwortungsträger.
- „Leadership“ im weiteren Sinne, und auch die damit einhergehende Vorbildfunktion jedes einzelnen, muss neu überdacht werden. Wollen wir markt- und wettbewerbsfähig bleiben, müssen neue Dimensionen – insbesondere die Dimension der Cyberwelt – miteinbezogen werden, bis in die letzte Konsequenz. Das gilt für jedes Individuum sowohl persönlich als auch in der Funktion als Verantwortungsträger von Unternehmen oder Organisationen.

Gefälschte oder manipulativ eingesetzte Informationen in Medien beeinflussen das Verhalten von Verantwortungsträgern und verleiten sie dazu, den falschen Personen und Informationen zu trauen. Individuelle Stereotypen verleiten die Opfer zu verfälschten Annahmen. Die eigene Befangenheit und der Verlust der Objektivität tragen ihren Anteil bei. Die Delinquenten verstehen es bestens, ihre (wirtschafts)kriminelle Energie zu verbergen und ihre Mitmenschen durch ihr manipulatives Verhalten zu täuschen. Diese Manipulationen in Form des Social Engineering sind nichts Neues – sie finden seit Anbeginn der Menschheit statt. Bis heute sind jedoch die wenigsten potenziellen Opfer diesbezüglich sensibilisiert. Der bewusste Umgang mit dieser Art der Bedrohung wird erst von wenigen Exponenten professionell gepflegt. Trotz aller technologischen Fortschritte:

► Hinter jedem Algorithmus stecken Menschen mit Interessen und Absichten.

Es gibt weder kriminelle Computer noch kriminelle Codes. Wenn es darum geht, wirtschaftskriminelle Ereignisse, Non-Compliance oder Cyberangriffe zu initiieren, abzuwehren und aufzuarbeiten, ist der Mensch das schwächste Glied in der Kette. Auch wenn wir in den vergangenen drei Jahrzehnten einen rasanten technologischen Wandel erleben durften und wir aufgrund unserer Demografie mit drei verschiedenen Generationen verhandeln, wirtschaften und Lösungen finden: Unsere Adaption von der analogen zur digitalen Welt gelingt nicht in jeder Beziehung und in jeder Konstellation gleich gut. Wir sind langsamer als die technologischen Entwicklungen und hinken hinterher. Insbesondere wenn es darum geht, Risiken zu identifizieren, abzuwägen und mit der eigenen Risikotoleranz abzugleichen, sind die Verantwortungsträger in der Praxis noch zurückhaltend.

Im Fokus dieses Buches steht der Mensch mit seinen Dispositionen, in seinen unterschiedlichen Rollen und seinem situativen Verhalten. Sei es als Verantwortlicher einer

Organisation, als direkt oder indirekt Betroffener eines wirtschaftskriminellen Ereignisses, als Experte im Rahmen einer Sachverhaltsermittlung, als Konsument von Medienmitteilungen oder als Täter wirtschaftskrimineller Handlungen, Non-Compliance oder Cyberkriminalität. Jeder von uns hat unterschiedliche Rollen inne und möchte den damit assoziierten Erwartungen in der einen oder anderen Form gerecht werden. Entsprechend sind Sie eingeladen, das Buch aus unterschiedlichen Perspektiven zu lesen und die Themen anhand zusätzlicher zur Verfügung stehenden Fragestellungen zu vertiefen. Sie als Leser werden aufgefordert und angeleitet, sich und Ihr Umfeld zu analysieren. Die Praxis stellt uns allen genügend Beispiele zur Verfügung, um sich zu hinterfragen, ob dieses Betrugsmuster auch für unseren Verantwortungsbereich zutreffen könnte. Eine Reflektion darüber ist ein erster Schritt Richtung Sensibilisierung.

Die Beleuchtung der Themen Wirtschaftskriminalität, Non-Compliance und Cyberkriminalität mit dem Fokus auf den Menschen soll sensibilisieren und motivieren:

a) hinzuschauen,
b) zu hinterfragen und
c) sich eine eigene Meinung zu bilden.

Nur durch proaktives Mitwirken aller Exponenten wird es in Zukunft gelingen, die neuen Herausforderungen sportlich zu nehmen und an ihnen zu wachsen. Dass die Veränderungen rasanter sind als noch vor 50 Jahren ist eine Tatsache, die wir nicht ändern können. Aus diesem Grund motiviere ich alle, sich auf die Stärken jedes einzelnen Individuums zu fokussieren und diese nutzenstiftend einzubringen. Kennen Sie Ihre eigene kriminelle Energie und nutzen Sie diese, um Risiken in Ihrem Unternehmen zu identifizieren?

Zur Bekämpfung von Wirtschaftsdelikten bedarf es der Kombination verschiedener Disziplinen, um den potenziellen Schaden für Gesellschaft, Wirtschaft, Organisationen und Individuen zu mildern und im besten Fall abzuwehren. Das Buch vermittelt Ihnen das Wissen hierzu und stellt die verschiedenen Komponenten zur Anreicherung der bestehenden Disziplinen zur Verfügung. Durch die Einbindung des Risiko- und Erfolgsfaktors Mensch in den gesamten Prozess der Prävention, der Aufdeckung und der Aufarbeitung wirtschaftskrimineller Handlungen werden die Maßnahmen effektiv und ressourcenorientiert implementiert. Eine professionell strukturierte Vorgehensweise im Rahmen der internen und externen Sachverhaltsermittlung mit all ihren verschiedenen Komponenten erlaubt es den Verantwortlichen, die Handlungsfähigkeit zu wahren und die Reputation zu schützen.

Vor über 25 Jahren, als ich zum ersten Mal in Kontakt mit der Thematik „Unregelmäßigkeiten in Unternehmen“ (nach heutiger Terminologie „Non-Compliance“) kam, nutzte noch niemand die Begriffe Wirtschaftskriminalität oder Non-Compliance. Die Grundproblematik, das Vorgehen und die Muster waren jedoch exakt dieselben. Man belehrte mich gönnerhaft, dass so etwas nur „über dem Teich“ geschehe, nicht jedoch im deutschsprachigen Raum oder in Europa. Zu stark waren die eingefahrenen Glaubensmuster, als dass die Verantwortlichen die Risiken und bereits begangene Delikte hätten

erkennen können. Wir alle wissen, wie sich die Welt – insbesondere auch die Welt der Finanzinstitute – in den letzten zwei Dekaden gedreht hat.

Mit großer Neugier auf das Neue freue ich mich auf die zukünftigen Herausforderungen und bin überzeugt, dass wir alle daran wachsen werden. Einfacher wird es nicht, doch das war es auch für unsere Vorfahren nicht. Die „guten alten Zeiten" heraufzubeschwören ist Teil unserer Befangenheit, wie wir in den folgenden Kapiteln sehen werden.

Freche Dachse, falsche Nattern und diebische Elstern gab es schon immer und wird es immer geben. In diesem Sinne wünsche ich Ihnen die richtige Portion Neugier, Vertrauen in Ihre Intuition und Hartnäckigkeit beim Erkennen persönlicher Verhaltensmuster, beim interdisziplinären Aufdecken von Manipulationen, beim Analysieren von Fakten und beim Wahren Ihrer eigenen Handlungsfähigkeit und Reputation im Ereignisfall!

Zug, Schweiz Sonja Stirnimann
Frühling 2021

Danksagung

„Gedenke der Quelle, wenn du trinkst“. (aus China)

Ich danke allen, die während der Monate meiner Versenkung auch nur einen Funken Verständnis hatten und mich damit tatkräftig in meinem Vorhaben, dieses Buch zu schreiben, unterstützten. Ihr hattet somit etwas mehr Ruhe vor all meinen Ideen, die mich jeweils umtreiben – das ist nun wieder vorbei.

Insbesondere meiner Familie danke ich von Herzen für ihr Verständnis. Während vieler Stunden habt ihr auf meine Anwesenheit verzichtet und der Manuskriptabgabe entgegengefiebert. Viele Familiengespräche handelten von den dunklen Seiten der Menschen, Risiken und der alltäglich erlebten Einflussnahme und Manipulation. Die daraus entstandenen Insider-Witze werden uns drei noch lange begleiten und ein Lachen ins Gesicht zaubern.

Ebenfalls ein großes Dankeschön an die freiwilligen Leser des Manuskripts. Wenn man als Autorin die eigenen Sätze nicht mehr lesen kann, jeden Satz zum hundertsten Mal hinterfragt und alles ändern will … In diesem Moment seid ihr in akribischer Sorgfalt über die Zeilen gewandert und Fehlern auf die Spur gekommen. Mit professioneller Skepsis habt ihr meine Sätze durchleuchtet.

Danke!

Inhaltsverzeichnis

Teil II Erfolgsfaktoren erkennen

Über die Autorin

Sonja Stirnimann beschloss anfangs der 90er-Jahre aufgrund ihres ersten Mitwirkens bei der Aufdeckung von „Non-Compliance“ im professionellen Umfeld Wirtschaftsprüferin zu werden – mit dem Ziel, durch konsequentes Hinterfragen von Handlungen die Zusammenhänge zwischen menschlichem Verhalten, Finanzzahlen und gesetzlichen Rahmenbedingungen zu verstehen und Unregelmäßigkeiten aufzudecken. Die Faszination rund um die Thematik „Integrität, Wirtschaftsdelikte und Non-Compliance“ blieb über die Jahre ungebrochen, entwickelte sich im Zeitalter der digitalen Informationen laufend weiter und ergänzte sich um das Territorium „Cyber“.

Die Autorin verfügt über mehr als 25 Jahre Berufserfahrung auf diesem Spezialgebiet in verschiedenen Branchen. Ihre Rollen und Verantwortlichkeiten bei globalen Finanzdienstleistern, produzierenden Konzernen sowie Beratungsunternehmen tragen bei zu ihrer breiten internationalen Erfahrung auf den Gebieten Ermittlungen, Finanzen, Governance, Risk & Compliance, Kommunikation und Krisenmanagement.

Als Expertin für Corporate Integrity, Wirtschaftskriminalität und Non-Compliance berät Sonja Stirnimann die höchsten Verantwortungsträger (Verwaltungsrat, Aufsichtsrat und Geschäftsleitungsmitglieder) internationaler Organisationen im Umgang mit diesen sensitiven Themen. Sie setzt sich – aus verschiedenen Perspektiven – für die Prävention sowie die Handlungsfähigkeit und Reputation von Persönlichkeiten und Unternehmen im Ernstfall und in Krisen ein.

Ebenso unterstützt sie Behörden und Regulatoren bei der Aufarbeitung von Fakten anhand umfassender interdisziplinärer Sachverhaltsermittlungen und der Erstellung von Gut-

achten auf nationaler und internationaler Ebene. Ihre professionellen Gesprächsführungs- und Interviewtechniken bilden einen wesentlichen Bestandteil ihrer erfolgreichen Interaktionen und Ermittlungen.

Als Verwaltungsrätin, Vorsitzende von Audit Committees, Mitglied von Risk Committees, von börsenkotierten und privat gehaltenen Unternehmen sowie als Unternehmerin weiß sie, was es heißt, Verantwortung wahrzunehmen.

Sonja Stirnimann ist Ökonomin, diplomierte Wirtschaftsprüferin, Certified Fraud Examiner, hält einen internationalen Executive MBA in Financial Services & Insurance der Universitäten St. Gallen, HEC Montreal, Vlerick Business School Ghent, die Zertifizierung des MIT Boston im Bereich Cybersecurity, ein Ergänzungsstudium in Finanzmathematik und Statistik und ist Wirtschaftsmediatorin. Sie lehrt an verschiedenen Universitäten, Fachhochschulen und in Berufsverbänden im Rahmen von Weiterbildungs- und Executive-Programmen.

Als Gründerin der Structuul AG sowie dem Programm Corporate Integrity Concepts™ setzt sich sie für die nachhaltige Förderung der Unternehmensintegrität und Bekämpfung von Wirtschaftskriminalität auf globaler Stufe ein. Mit der Methode des FraudAidKit™ hat Sonja Stirnimann ein strategisches Instrument entwickelt, das den Entscheidungsträgern präventiv wie auch reaktiv die Handlungsfähigkeit und Reputation eines von Non-Compliance, Wirtschafts- oder Cyberkriminalität betroffenen Unternehmens in einer Krisensituation sicherstellt.

Als leidenschaftliche Sportlerin, Hochseeseglerin und Atlantik-Überquererin sowie Direktbetroffene und Überlebende der Attentate von Brüssel 2016 weiß sie aus Erfahrung, was es bedeutet, mit Krisen und Extremsituationen umzugehen.

Die brisante Kombination und Interaktion von Menschen, Technik, Fakten und Regulierung fasziniert sie immer wieder aufs Neue. Als passionierte, aus breiter Praxis schöpfende Expertin mit globaler Erfahrung auf sämtlichen Hierarchie-Ebenen gilt sie als Vertrauensperson in heiklen Situationen.

Teil I

Basis schaffen

Grundlagen und Theorie – eine Einführung

1

Nichts genügt dem, welchem genug zu wenig ist
(Epikur von Samos, 341–270 v. Chr.).

Zusammenfassung

Wirtschaftskriminalität, Non-Compliance und Cyberangriffe sind Themen, die den Medien immer wieder Titelgeschichten wert sind. In der Politik dienen sie als dankbare Aufhänger für parteispezifische Agenden, betroffene Individuen sowie Verantwortungsträger von Organisationen und Unternehmen – jedoch spricht man nur ungern darüber. Es ist ein Tabu-Thema seit Anbeginn der Menschheit, weil es immer einzelne Individuen oder Gruppierungen gab, die ihre (berufliche) Stellung ausgenutzt haben zum Schaden derjenigen, die ihnen Vertrauen schenkten. Die Betroffenen wollen in den meisten Fällen vermeiden, dass die Angelegenheit an die Öffentlichkeit gelangt – zu groß wäre der drohende Reputationsschaden.

Die Ausdehnung des gesellschaftlichen und wirtschaftlichen Bewegungsradius durch den Cyberspace in den vergangenen Jahrzehnten hat die Anzahl möglicher Deliktmuster potenziert. Weshalb ein Individuum zulässt, dass sich seine (wirtschaftskriminelle) Energie materialisiert, wird im Folgenden analysiert und beantwortet. Die unterschiedlich ausgeprägten Deliktmuster finden sich in einer Kategorisierung, die unter Berücksichtigung der neusten Veränderungen durch den Cyberspace ergänzt wird. Der Mensch steht hierbei im Zentrum des Geschehens (vgl. Abb. 1.1) und ist verantwortlich.

S. Stirnimann, *Der Mensch als Risikofaktor bei Wirtschaftskriminalität*,
https://doi.org/10.1007/978-3-658-34631-7_1

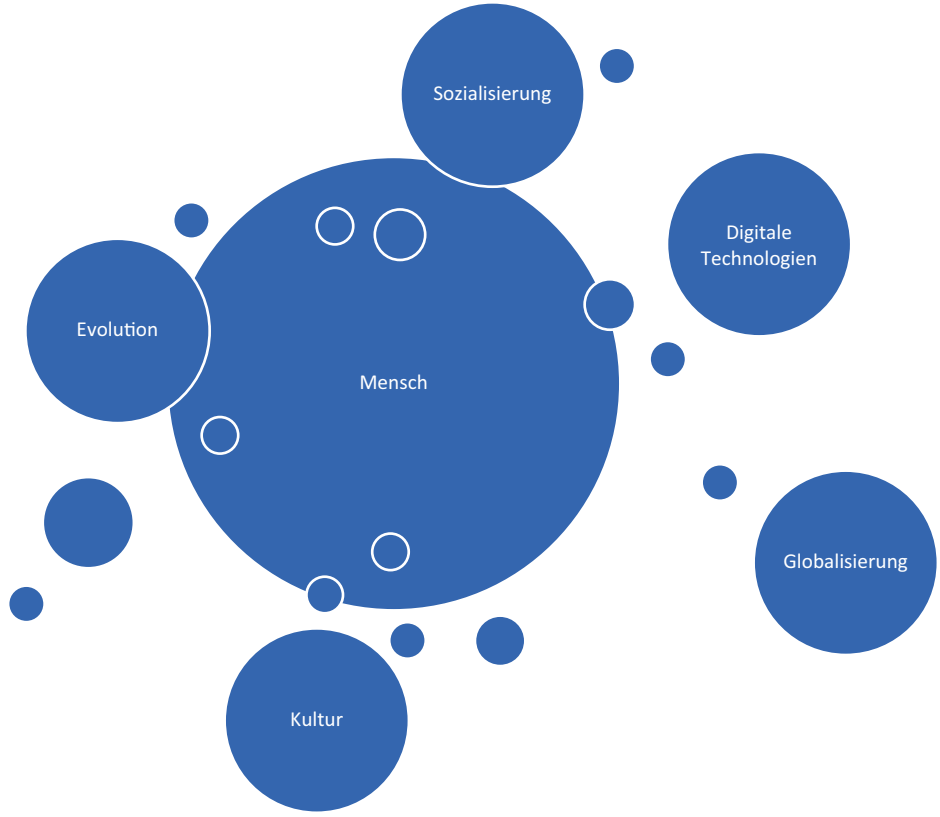

Abb. 1.1 Der Mensch im Zentrum des Geschehens (Eigene Darstellung)

1.1 Der Weg zum Zeitalter digitaler Informationen

Die Fragen, wer wir sind, woher wir kommen und wohin wir gehen, klingen philosophischer als sie sind. Wir leben im sogenannten Informationszeitalter und können auf eine beachtliche Historie zurückblicken. Betrachtet man den Begriff genauer, stellt sich die Frage, ob wir uns im Informationszeitalter oder im Digitalzeitalter befinden. Rückblickend wird uns diese Frage durch Historiker beantwortet werden können. Fakt ist, dass wir längst nicht mehr nur von drei Wirtschaftssektoren sprechen, sondern von vier (Dostal 1995, S. 529). Die prognostizierten Entwicklungen sind eingetroffen, und der Trend hin zu digitalen Informationen und den daraus entstehenden Konsequenzen auf die Volkswirtschaft hält an.

Ein Rückblick ist notwendig, um die Gegenwart zu verstehen und die Zukunft zu antizipieren. Die Wissenschaft spaltete unser Selbstverständnis in Extrovertiertheit und Introvertiertheit. Dieses Verständnis hat sich über die Jahrhunderte hinweg gewandelt, und wir

können von verschiedenen Revolutionen sprechen. Insbesondere von drei wissenschaftlichen Revolutionen, die unsere Gesellschaft wesentlich prägten.

Die globalen gesellschaftlichen Veränderungen haben einen großen Einfluss auf die Selbstwahrnehmung jedes einzelnen Individuums. Die Zusammenfassung stellt sich folgendermaßen dar:

Von **Kopernikus** (1473–1543)[1] lernten wir, dass die Planeten um die Sonne kreisen – und wir Bewohner der Erde somit nicht im Mittelpunkt stehen. Er brachte mit seiner Erkenntnis unbewusst eine Revolution in Gang, die zu einer radikalen wissenschaftlichen Transformation führte. Seit diesem Zeitpunkt befassen wir uns mit den Konsequenzen der durch Kopernikus festgestellten Theorien und Fakten. Nach Kopernikus' Revolution konnten wir zwar nicht mehr davon ausgehen, dass wir das absolute Zentrum des Geschehens darstellen, zumindest jedoch den Mittelpunkt auf der Erde.

Im Jahre 1859 publizierte **Charles Darwin** (1809–1882)[2] seine Erkenntnisse der Evolutionsgeschichte. Gemäß seiner These entwickelte sich jedes Lebewesen, basierend auf seinen Vorfahren, durch natürliche Selektion. In diesem Moment erhielt der Begriff „Evolution" eine neue Bedeutung. Wir wurden quasi vertrieben aus unserer biologischen Allmacht. Wie damals zu Zeiten Kopernikus', fanden auch Darwins Erkenntnisse nicht nur Anhänger, und alternative Erklärungen wurden gefunden, um an bestehenden Theorien festzuhalten (z. B. durch religiöse Gemeinschaften). Die Rolle der allmächtigen und im Zentrum stehenden Individuen war uns abgesprochen worden. Was uns aber niemand nehmen konnte, war unser Geist.

Die Gedanken sind frei – und wir sind allein verantwortlich für deren Auswüchse. **René Descartes** (1596–1650)[3] untermauerte dies mit dem Satz „Ich denke, also bin ich". Dieser Satz könnte Folgendes bedeuten: Die astronomische und biologische Daseinsberechtigung haben wir mit den beiden vorangegangenen Revolutionen durch Kopernikus und Darwin abgegeben – nun bleibt uns der Geist, über den wir uns definieren können. Wir sind nach wie vor noch Herr über unsere Motivationen, Ideen, Emotionen und Glaubenssätze.

Erst **Freud** stahl uns auch diese Illusion durch seine psychotherapeutischen Theorien. Er läutete somit die dritte Revolution ein, indem er verkündete, dass der Geist auch unbewusst gelenkt wird und Abwehrmechanismen in sich trägt, die zu Verdrängungen führen können.

▶ Heute wissen wir, dass vieles, was wir tun und entscheiden, unbewusst abläuft. Dass Fakten weniger eine Rolle spielen als die bereits verinnerlichten Stereotypen und Glaubenssätze. Bewusst formen wir glaubwürdige Geschichten, um unsere Handlungen nachträglich zu rechtfertigen.

---

[1] Nicolaus Copernicus. Gesamtausgabe. Band 6, Teil 2, S. 28.

[2] Nora Barlow (Hrsg.): The Autobiography of Charles Darwin 1809–1882. With the Original Omissions Restored. Edited and with Appendix and Notes by his Granddaughter Nora Barlow. 1958.

[3] https://plato.stanford.edu/entries/descartes/ (Zugegriffen am 26.11.2017).

Dass wir den Inhalt unserer Gedanken, ihre Herkunft und Verknüpfungen nicht in gleicher Art und Weise überprüfen können wie wir die Inhalte einer Festplatte durchsuchen, haben wir verstanden. Wir wurden verstoßen aus dem Verständnis des absoluten Bewusstseins und akzeptieren, dass wir für uns selbst undurchsichtig sind.

Fragen

Woher kommt der Irrglaube, dass andere Individuen für uns greifbarer sind als wir selbst und wir sie einschätzen können? Warum schenken wir unbekannten Personen bedingungsloses Vertrauen? Aus welchem Grund fürchten wir uns vor den neuen Technologien des Cyberspace und nicht vor den Individuen dahinter?

Der Begriff Bewusstsein hat sich stetig verändert, und um wissenschaftlich fundiert zu bleiben, ersetzen wir die Psychoanalyse mit Neurowissenschaften, was der Thematik näherkommt.

Die dritte Revolution wurde durch **Alan Turings** Arbeit abgelöst, indem er uns die privilegierte, einmalige Situation des logischen Denkens, der Informationsverarbeitung und des geschickten Verhaltens entzog (Turing 1937, S. 232). Die Technologie nahm uns Arbeit ab. Der Begriff Computer, der im Englischen im 16. und 17. Jahrhundert als Synonym für rechnende Menschen genutzt wurde, erhielt eine neue Bedeutung. Bis dahin gab es im ganzen Universum keine andere Möglichkeit, autonom etwas zu berechnen, als durch den Menschen. Ab dem Zeitpunkt von Turings Publikation war das Wort für programmierbare Maschinen besetzt. Auch mit dieser vierten Revolution wurde unser Selbstverständnis grundlegend verändert – intern wie extern. Langsam, aber sicher akzeptieren wir, dass wir nicht autark sind (Floridi 2014, S. 93).

> Wir sind mitteilsame Organismen, gegenseitig verbunden und eingebettet in ein informationelles System, das wir mit anderen mitteilsamen natürlichen und künstlichen Systemteilnehmern teilen und Informationen logisch und autonom verarbeiten (Floridi 2014, S. 93).

Willkommen im Zeitalter digitaler Informationen! Entgegen der Aussage von Floridi bin ich überzeugt, dass diese künstlichen Intelligenzen im Rahmen des Möglichen technisch intelligent sind und somit berechenbarer als der Mensch. Aus diesem Grund ist und bleibt der Mensch der Erfolgsfaktor Nummer Eins. Vorausgesetzt, er wird in all seinen Ausprägungen erkannt und richtig eingesetzt, und wir nutzen die vorhandenen Werkzeuge, um das Potenzial jedes einzelnen Individuums zum Wohle aller einzusetzen. Andernfalls wird der Erfolgsfaktor zum Risikofaktor.

All diesen Fragen rund um den Risikofaktor Mensch werden wir auf den Grund gehen. Abschn. 1.3 wird Sie in die Grundlagen und Theorien von Wirtschaftskriminalität, Non-Compliance und Cyberkriminalität einführen. Verschiedene Begrifflichkeiten, Perspektiven und eigene Erkenntnisse, bei denen der Risikofaktor Mensch mit all seinen Facetten, Ausprägungen und Einflüssen auf die Thematik im Fokus steht, werden dies anhand des Lebenszyklus wirtschaftskrimineller Handlungen und Non-Compliance ver-

anschaulichen. Dem Aspekt der Befangenheit wird große Beachtung geschenkt. Mit einem Blick darauf, wie sich unser Selbstverständnis entwickelt hat und wo wir mit der dritten Revolution angekommen sind, schließt sich der Kreis mit der Erkenntnis und Akzeptanz, dass wir bei uns selbst (oft) noch im Dunkeln tappen.

- Wenn wir die „Handlungsfähigkeit im Ernstfall" sicherstellen wollen, bedarf es der Analyse entlang des Lebenszyklus wirtschaftskrimineller Handlungen, Non-Compliance und Cyberkriminalität. Sei dies im privaten Umfeld, wenn wir unser Dasein und unsere Beziehungen betrachten, sei es im professionellen Umfeld, wenn wir von Produkten und Dienstleistungen sprechen, oder rund um die Thematik der Verhaltensweisen und Handlungen, die Wirtschaftskriminalität, Non-Compliance und Cyberkriminalität begünstigen, fördern und geschehen lassen.

Die einzelnen Kapitel sind die Mosaiksteine eines großen Bildes, das im ständigen Wandel ist aufgrund der verschiedenen Einflussfaktoren, mit denen wir es im Zeitalter digitaler Informationen auf verschiedenen Ebenen zu tun haben. Entsprechend ist die Agilität der involvierten Individuen existenziell – man wagt zu behaupten, dass die Halbwertzeit sich nochmals drastisch verringert. Umso wichtiger ist die stetige Beobachtung und Auseinandersetzung mit der Thematik. Ob in der Rolle der Verantwortlichen der Unternehmen und Organisationen, des Regulators oder der Aufsichtsbehörden, der Strafverfolger oder auch der Experten, die potenziell oder tatsächlich direkt oder indirekt Betroffene durch diese unsicheren, teils stürmischen und bedrohlichen Themen führen. Die Handlungsfähigkeit als solche muss bei den Verantwortlichen zwingend sichergestellt werden, denn sie lässt sich beim besten Willen nicht auslagern – egal für wie viel Geld. Das Gleiche gilt für die Verantwortung.

- Ziel dieses Buches ist, die Sensibilisierung der Verantwortungsträger für den Faktor „Mensch" und deren Bewusstsein für dessen Potenziale zu schärfen.

- Ob bei der Prävention, Aufdeckung oder Reaktion auf Ereignisse im Bereich Wirtschaftsdelikte, Non-Compliance oder Cyberkriminalität: Das Zünglein an der Waage ist der Mensch in seinem Denken und seinem daraus abgeleiteten Verhalten.

- Durch eine solche Sensibilisierung wird es den Verantwortlichen gelingen können, ihre eigene Handlungsfähigkeit im Ereignisfall strategisch und professionell zu wahren und die verschiedenen kritischen Elemente auf dem eigenen Radar proaktiv zu bewirtschaften.

1.2 Historischer Abriss des wirtschaftlichen Zusammenlebens

Regelverstöße gibt es nicht erst seit wenigen Jahren. Die Tendenz, in der näheren Vergangenheit zu suchen, ist verlockend, beeinflusst aber die objektive Wahrnehmung im Hinblick auf die lange Historie der Wirtschaftsdelikte. Fälle von Wirtschaftskriminalität

und Non-Compliance, wie die Unterstützung bei Bilanzmanipulationen und die Beweisvernichtungen seitens Enron, der Millionenbetrug gegenüber Anlegern von Bernie Madoff, die Schein-Absicherungsgeschäfte von Kweku Adoboli in der Finanzindustrie oder der Abgasskandal der Automobilbranche, ausgelöst durch VW, lassen uns gedanklich gar nicht allzu weit in die Vergangenheit schweifen. Doch der Schein trügt, und die neuen Medien tragen mit dazu bei, dass wir heute einen anderen Zu- und Umgang mit diesen Informationen haben. Unsere Wahrnehmung und Entscheidungsfindung wird gesteuert. In Kap. 4 werden die entsprechenden einflussnehmenden und manipulierenden Taktiken behandelt. Dass regelwidriges Handeln im Zusammenhang mit ökonomischem Verhalten schon immer ein Teil der Wirtschaft war, ist eine Tatsache.

1.2.1 Wirtschaftskriminalität und Non-Compliance – zurück zum Ursprung

Was im Zusammenhang mit Wirtschaftsdelikten nur ungern gehört wird, bringt ein deutsches Sprichwort auf den Punkt: „Wo gehobelt wird, fallen Späne." Stellvertretend dafür könnte man auch sagen: „Der Zweck heiligt die Mittel." Wie sich diese beiden Sprichwörter zum Lebenszyklus wirtschaftskrimineller Handlungen verhalten, werden die folgenden Kapitel analytisch darstellen.

Lange bevor der Begriff „Wirtschaft" entstand, manipulierten Menschen andere zu ihren Gunsten. Tauschgeschäfte wurden so aufgesetzt, dass jede der Parteien das Gefühl haben konnte, den besseren Abschluss erzielt zu haben – dies mit mehr oder weniger ehrenvollen Mitteln. Schon die Qualität des Handelsgutes dürfte je nach Lieferant um die eine oder andere Komponente beeinflusst worden sein. Wo die gute Ware erhältlich war, erschloss sich nur einem inneren Kreis, der auch die notwendigen Gegentauschmittel und deren Umfang festlegte. Zu jener Zeit sprach noch niemand von illegalen Absprachen oder Korruption. Doch die Mechanismen bestanden bereits und gehörten zum alltäglichen Umgang zwischen den Exponenten – bereits im Steinzeitalter. Jede Gesellschaft verfügt über eigene Normen und Regeln. Unabhängig davon, wie diese verankert sind oder waren, ist jedes Abweichen von diesen Normen regelwidrig. Das kann im übertragenen Sinne heißen, dass es kriminell oder non-compliant ist, weil es nicht den definierten und vereinbarten Normen und Regeln entspricht. Die soziale Kontrolle stellte bereits damals sicher, dass sich die einzelnen Mitglieder der Gesellschaft innerhalb der Vorgaben verhielten. Die soziologischen Aspekte rund um die Einhaltung von Normen und Regeln sind weitreichend und werden in die Thematik der Wirtschaftskriminalität miteinbezogen. Im Mittelpunkt stand und steht der Mensch, der mit seinem Handeln Reaktionen und somit Konsequenzen auslöst.

Als die ersten Technologien entstanden – etwa Messsysteme wie das Metermaß oder die Waage –, wurden sie auch sogleich anfällig für Manipulationen. Der Vorreiter der Abgasmanipulation, der sogenannte „Diesel-Gate", manifestierte sich in einem der ersten Fraud-Schemas. Die Einführung von normierten Tauschwährungen in Form von Münzen

und später Noten brachte mit sich, dass Menschen neue Vorgehensmuster ersannen, um sich Vorteile gegenüber anderen Marktteilnehmern zu verschaffen. Diese wurden und werden beständig ausgearbeitet – dem Gesetz und den Regulierungen meist einen Schritt voraus –, indem Graubereiche als Schlupflöcher identifiziert und zum Nutzen der eigenen Interessen eingesetzt werden. Der Ursprung dieser Muster liegt im (Wirtschafts-)Delikt, das den Gesetzgeber, die Straffverfolgung sowie die betroffenen Verantwortlichen von Staat, Organisationen und Unternehmen herausfordert.

1.2.2 Territorium Cyberspace – zurück in die Zukunft

Die Theorien und Erkenntnisse des amerikanischen Soziologen Lewis Mumford aus dem Jahr 1934 bilden die Basis für die ersten Schritte in Richtung des Territoriums, das wir Cyberspace nennen (Leukfeldt und Stol 2012, S. 20). Er beschäftigte sich eingehend mit der Thematik „Technik und Zivilisation". Mumford demonstrierte einleuchtend, dass weniger die Technik die historischen Pfade beeinflusst, als vielmehr die mentalen Entwicklungen der Menschheit. Mit anderen Worten: Die Kultur beeinflusst die Geschichtsschreibung. Es sind weniger die technologischen Erfindungen als die geistigen Verfassungen, in denen sich die Gesellschaft zu einem Zeitpunkt befindet, die festlegen, welche Technologien weiterentwickelt und implementiert werden.

Basierend auf dieser soziologischen Analyse ist es nicht verwunderlich, dass das Internet zu einem Zeitpunkt Anklang fand, als es auf der Erde nicht mehr viele weitere Territorien zu erschließen gab. Die Mondlandung – eines der größten Ziele – war geglückt. Die Tatsache, dass nur eine Minderheit der Bevölkerung die Erde bereist und erforscht, spielt bei der Bewegung hin zum Internet eine sehr untergeordnete Rolle. Es gibt einen wahrgenommenen Mangel an Perspektiven in der Erforschung weiterer Sphären. Das sogenannte Cyberspace ist das Resultat dieses wahrgenommenen Verlustes an Entdeckungsmöglichkeiten. Die Menschheit fand sich eingesperrt in der Enge des Alltags.

> ► Somit ist Cyberspace die Antwort auf die Einschränkungen des Pioniergeistes. Es geht in diesem Sinne auch nicht darum, dass die Menschheit die neuen Technologien der Ingenieure nutzt, weil sie entwickelt wurden, sondern dass diese Technologien entwickelt wurden, weil sie genutzt werden wollen (Leukfeldt und Stol 2012, S. 20).

Mit dieser wahrgenommenen Einschränkung und dem Bedürfnis nach weiteren zu erforschenden Territorien erschließt sich – wie wir noch sehen werden – eine Vielzahl an neuen Herausforderungen. Daraus lässt sich ableiten, dass die Menschheit nicht nur fähig ist, neue Technologien einzuführen, sondern diese auch zu lenken und deren Richtung bei Bedarf zu ändern. Mumford verteidigte diese Tatsache in seinen Forschungsergebnissen schon damals vehement (Mumford 1934, S. 10). Übertragen auf die heutige Zeit der digitalen Informationen, könnte dies nicht zutreffender sein. Als Mumford 1990 im Alter von 94 Jahren verstarb, hatte er den Durchbruch des Internetzeitalters noch in einer ersten

Phase miterlebt (Mumford 2017). Die ursprünglichen Ziele des Cyberspace waren, die Entwicklung voranzutreiben und Möglichkeiten für neue Entdeckungen zu schaffen. Was sich jedoch in jüngster Zeit rund um die Thematik Cyberattacken, Digitalisierung, Datenverluste etc. abspielt, blieb Mumford erspart. Es ergibt wenig Sinn, Technologien zu optimieren, wenn die intellektuellen Fähigkeiten der Menschheit nicht entsprechend entwickelt sind. Dass diese Intelligenz jedoch auch in negativer Hinsicht zur Kriminalität genutzt werden kann und wird, ist eine Tatsache.

▶ Für alle, die sich nun als Opfer dieser neuen Technologien sehen, kann entschärfend in Aussicht gestellt werden: Die Menschheit ist diesen Technologien nicht schicksalhaft ausgeliefert, sondern sie ist eingeladen, dieses Potenzial im Sinne der ursprünglichen Ziele zu nutzen.

Wo Menschen zusammenleben, müssen sie sich nicht nur vor den vier Elementen und dem Tierreich schützen, sondern auch – und im Speziellen – vor ihren Mitmenschen. Ob nun bei einer Expedition in der Antarktis oder im Cyberspace: Das Grundbedürfnis nach Sicherheit ist überall dasselbe. Die Gefahren des Cyberspace finden ihren Ursprung ebenso wie die Gefahren in der realen Welt beim Menschen. Die Sicherheit ist weniger ein technologisches oder physisches Problem, sondern ein sozialwissenschaftliches. Dazu gehören die Soziologie, die Psychologie, die Kriminologie und ergänzend auch die Rechtswissenschaft. Die Technologie spielt hierbei eine untergeordnete Rolle. Zentral für die Sicherheit und somit die Minimierung von Gefahren im Cyberspace ist das Verhalten der Individuen. Es lohnt sich daher, sie zu motivieren und zu unterstützen, ihre intellektuellen Fähigkeiten zum Nutzen aller und nicht zum Schaden anderer einzusetzen. Dieses Wissen kann das eigene Unternehmen genauso wie das anderer effektiv schützen. Am Anfang muss die Frage stehen, wie das menschliche Verhalten hin zu mehr Sicherheit beeinflusst werden kann – nicht nur im Cyberspace, sondern überall. Die Besonderheit im Cyberspace im Gegensatz zu anderen Bereichen ist, dass er verhältnismäßig wenig erforscht und in ständiger rasanter Entwicklung ist. Dieser Umstand erfordert hohe Agilität und den Einbezug unterschiedlicher Disziplinen, wenn es darum geht, die Risiken umfänglich zu erfassen und die entsprechenden unterstützenden Maßnahmen abzuleiten.

Das Internet ist eine Technologie, die wesentlichen Einfluss auf die soziale Entwicklung der Gesellschaft und somit die Geschichtsschreibung hat. Weitere Technologien mit ähnlichem Potenzial sind in Abb. 1.2 illustriert. Die Erfindung der Schrift als Basis für alle nachfolgenden Erfindungen im Zusammenhang mit Kommunikation ist zweifellos von höchster Bedeutung. Damals mussten die Menschen darauf vertrauen, dass ihre Gedanken losgelöst von ihrem Körper ihren eigenen Weg gehen können. Sie mussten sich darauf einlassen, dass Körper und Geist nicht untrennbar sind. Dazu war notwendig, dass Gedanken in einer Form transportiert werden können, die es erlaubt, beim Empfänger mit der gleichen Bedeutung anzukommen. Diese mentale Entwicklung scheint eine der größten in der Geschichte der Menschheit. Zu dieser Genese des Loslassens und Separierens stellt das Internet eine Erweiterung dar.

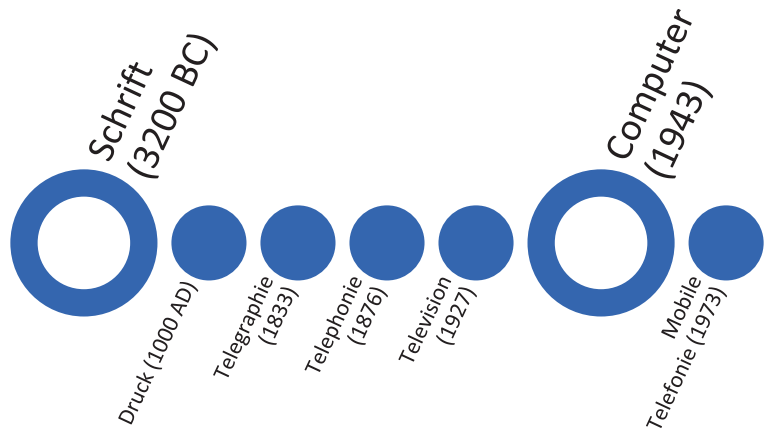

Abb. 1.2 Innovationen der Kommunikationsmittel (Eigene Darstellung)

Vergleichen wir die Innovationen der Kommunikationsmittel in Abb. 1.2, stellen wir einen wesentlichen Unterschied zum Internet fest. Das Internet ist kein reines Kommunikationsmittel, sondern ermöglicht die Bildung sozialer Strukturen im eigenen Territorium.

▶ **Definition** Die soziale Struktur ist die Summe aller mehr oder weniger fixen Verhaltensmuster menschlicher Wechselbeziehungen.

Man kann dagegenhalten, dass auch die anderen Kommunikationsmittel nicht rein diesen einen Zweck verfolgten, sondern durch ihre Existenz soziale Strukturen bauten – dem ist so. Auch die Telefonie ermöglichte die kommunikative Vernetzung über weite Distanzen, was früher mit der Schrift allein noch nicht möglich war. Das Internet stellt mit dem Cyberspace zusätzliches Territorium für soziale Strukturen zur Verfügung. Berücksichtigt werden muss auch die Infrastruktur, die benötigt wird, um diese Beziehung aufrechtzuerhalten. Die sozialen Strukturen werden durch das Kommen und Gehen von Menschen errichtet. Ab dem Zeitpunkt, zu dem die Strukturen geformt sind, weisen sie den kommenden Menschen die Richtung für ihr Verhalten. Diese Theorie geht zurück auf Giddens, der ihr den Namen „Dualität von Strukturen“ gab (Giddens 1984, S. 27). Auch wenn niemand das Internet nutzen würde, bestünde es aus Domains, Webseiten, Blogs, Suchmaschinen und deren Verknüpfung – wenn auch in nicht ganz ausgereifter Form, wie bei vielen Nutzern der Fall. Die Bedürfnisse wachsen mit dem Vorhandensein und der Erforschung der Möglichkeiten. Erinnern wir uns an die ersten Webseiten vor zwei Jahrzehnten, so sehen wir die große Entwicklung aufgrund der Auseinandersetzung verschiedenster Berufsgattungen mit diesem Bestandteil der Struktur „Internet“. Diese (soziale) Struktur mit ihren Ausprägungen ist der sogenannte Cyberspace; er kanalisiert das Verhalten seiner Nutzer mit zwingendem Charakter.

▶ **Definition** Der Cyberspace ist die soziale Struktur im Internet.

Der freiwillige Charakter dieser sozialen Struktur ist die Vernetzung zwischen den Teilnehmern der Struktur. Diese erfolgt über die unterschiedlichsten Komponenten der Struktur: Webseiten, Suchmaschinen, Kanäle sozialer Medien und virtuelle Gemeinschaften. Aufgrund dieser sozialen Struktur kann eine reale Gemeinschaft simuliert werden. Mit der einzigen Ausnahme oder Abweichung der physischen Umgebung. Demzufolge nehmen die räumlichen und zeitlichen Distanzen eine untergeordnete Rolle ein. In Bezug auf die Sicherheit ist es wesentlich, dass die Individuen physisch abwesend sind.

▶ Die zwei wichtigsten Kriterien des Internet lauten:

- Es stellt eine soziale Struktur (Cyberspace) zur Verfügung, die das menschliche Verhalten diktiert und gleichzeitig Möglichkeiten eröffnet.
- Die soziale Struktur des Internets ist frei von einer physischen Umgebung. Zeit und Distanz spielen eine untergeordnete Rolle, und die Individuen sind physisch abwesend.

1.2.3 Territorium Cyber im Zusammenhang mit Sicherheit und Kriminalität

Wenn wir von Cybersicherheit sprechen, umfasst dies den Schutz in den sozialen Strukturen des Internets. Es geht darum, die Menschen vor der Verletzung ihrer physischen oder mentalen Integrität zu schützen. Entsprechend ist der Aspekt der Sicherheit umfassender als jener der Kriminalität. Cybersicherheit greift weiter als Cyberkriminalität. Die Abwesenheit von Sicherheit beginnt dort, wo ein Individuum Schaden nimmt oder absehbar ist, dass eine Schädigung erfolgt.

Die Interpretation der Verletzung physischer oder mentaler Integrität von Individuen bedarf einer flexibleren Betrachtungsweise. Wenn wir uns ausschließlich auf die Individuen konzentrieren, entgehen diejenigen Verhaltensweisen, die sich gegen Organisationen, Unternehmen oder die Gesellschaft richten. Beispiele dafür sind illegale Transaktionen und die Schaffung krimineller Strukturen unter Einbezug der Unterwelt und unrechtmäßigem Wirtschaften (Geldwäsche über Aktivitäten im Internet). Es handelt sich dabei um sogenannte „opferlose Vergehen“.

Obwohl Cybersicherheit mehr umfasst als Cyberkriminalität, spielt letztere eine wichtige Rolle in der Cybersicherheit. Es kursieren unterschiedliche Definitionen zu Cyberkriminalität und genauso wenig gibt es ein konzeptionelles Rahmenwerk für diese Art von Kriminalität. In Abschn. 1.3.4 wird Cyberkriminalität mit ihren diversen Ausprägungen den konzeptionellen Rahmen in Form von Mustern erhalten. Ebenso wird mit unterschiedlichen Terminologien und Kategorisierungen gearbeitet, wobei sich folgende Merkmale abzeichnen: Es gibt Delikte, bei denen ICT (Information and Communication Technology)

a) das Ziel und Mittel darstellt (Hacking, Verbreitung von Viren) und
b) ausführend, aber nicht das Ziel ist (e-Fraud, Verbreitung von Kinderpornografie).

Daraus lässt sich schließen, dass Cyberkriminalität als übergeordneter Begriff verstanden werden kann für Delikte, bei denen die ICT eine wesentliche Rolle spielt. Die beiden abzuleitenden Unterkategorien sind Cyberkriminalität

- im engeren Sinne, bei der ICT als Ziel und Mittel eingesetzt wird,
- im weiteren Sinne, bei der ICT verantwortlich für die Ausführung, aber nicht das Ziel ist.

Was ist der Unterschied zwischen der Verantwortlichkeit von ICT in der Ausführung und der Nutzung von ICT als Werkzeug? Wenn ICT ausschließlich als Werkzeug genutzt wird, sprechen wir in der Regel nicht von Cyberkriminalität. Zum Beispiel, wenn sich ein Krimineller mithilfe von Google Maps die Tankstellen für seinen nächsten Überfall heraussucht. Cyberkriminalität wird in Zukunft für diejenigen Delikte eingesetzt, die ICT als Ziel und Mittel verwenden.

► Cyberkriminalität im weiteren Sinne wird wegfallen, da es sich nur noch um den Modus Operandi handelt, wie ein Vergehen durchgeführt wurde.

Der Begriff „Cyberkriminalität“ wird weder in Anspruch genommen, um eine kriminologische Einordnung der Studienrichtung zu erklären, noch, um die technischen Vorgehensweisen zur Begehung des Deliktes zu definieren. Auch die Strafverfolgung braucht, trotz Internetzeitalter, diesen Begriff nicht für die Ahndung von Taten. Der Begriff „Cyberkriminalität“ klärt insofern nichts. Delikte sollten nicht nach den eingesetzten Mitteln (Cyber) benannt werden. Dies würde sonst bedeuten, dass sich mit jeder neuen Technologie oder dem Einsatz von Mitteln zur Begehung eines Verbrechens die Taxonomie der Kriminalität verändert. Das heißt, dass wir die soziale Relevanz der Informationstechnologie nicht von der Technik her verstehen sollten, sondern von den sozialen Prozessen, auf denen die Technik basiert (vgl. z. B.: Brissy 1990; Danziger 1985; De Sola Pool 1984). Kurz: Auch wenn Computer eingesetzt werden: Ein (Wirtschafts)delikt ist und bleibt ein (Wirtschafts)delikt. Relevant für die erfolgreiche Aufarbeitung von (Cyber-)Kriminalität ist der Fokus von den eingesetzten Mitteln hin zum Delikt.

Beispiel

Die Spezialisten der englischen „High-Tech Crime Unit“ wurden bereits 2006 zurück in die Abteilung der organisierten Verbrechen (Serious Organised Crime Agency SOCA) integriert. Somit war es wieder möglich, sich weg von den Werkzeugen, hin zum Verbrechen selbst zu fokussieren. Ein zu starker Fokus auf die Technologie blockiert die Sicht auf die soziale Realität (Leukfeldt und Stol 2012). ◄

Sprechen wir hier nun von altem Wein in neuen Schläuchen? War es nicht auch eine Aufrüstung, als es plötzlich Türen und Schlösser gab statt Säcke? Für Säcke waren noch keine Werkzeuge wie ein Dietrich nötig, mit der Einführung von Türen und Schlössern jedoch schon. Die Analogien könnten beliebig weitergeführt und Beispiele gefunden werden. Mit dem Cyberspace eröffnen sich ganz neue Möglichkeiten und damit auch die entsprechenden potenziellen Gefahren.

1.3 Wirtschaftskriminalität und Non-Compliance – Grundlagen und Theorie

Der Begriff „Wirtschaftskriminalität", im angelsächsischen Sprachraum „Economic Crime", sehr häufig auch „Fraud", wird unterschiedlich interpretiert und in verschiedenen Kontexten angewandt. Zusätzlich, aufgrund der Veränderungen und Entwicklungen im wirtschaftlichen Umfeld in den vergangenen Jahren, erhöhte sich die Publizität und Medienpräsenz des Begriffes um ein Vielfaches. Jeder spricht über Wirtschaftskriminalität und Non-Compliance, und entsprechend gibt es eine enorme Anzahl an Fällen, Geschichten und Definitionen.

Der folgende Abschnitt stellt einige der möglichen Definitionen der Begriffe „Wirtschaftskriminalität" und „Non-Compliance" dar und ist eine Basis für die weiterführenden Themen entlang des Lebenszyklus wirtschaftskrimineller Handlungen.

1.3.1 Definitionen und Begrifflichkeiten

In den vergangenen Jahren haben die Begrifflichkeiten rund um Wirtschaftsdelikte massiv an Popularität gewonnen, wobei diese Entwicklungen vor allem den Fällen aus der Praxis zu verdanken sind. Erwähnt werden können an dieser Stelle unter anderem das berühmte Ponzi-Schema von Bernard Madoff, die Bilanzmanipulation im Fall Enron sowie die Korruptionsthemen rund um Siemens Panalpina und weiteren Konzernen. In jüngster Vergangenheit findet die Automobilbranche hohe Resonanz in den On- und Offline-Medien aufgrund ihrer Abgas-Skandale. Die Ausprägungen all dieser Fälle sind unterschiedlich und folgen einem anderen Muster. Ihnen gemeinsam ist die Tatsache, dass sie sich unter die Begriffe „Wirtschaftsdelikte und Non-Compliance" subsumieren lassen. Sich entgegen den gesetzlichen, regulatorischen, internen und externen Regelungen, Richtlinien und Anforderungen zu verhalten, setzt das Unternehmen, für das man handelt, genauso wie die eigene Person dem Risiko aus, sich für das Handeln (oder Unterlassen) schuldig zu machen.

Was jedoch gemeint ist, wenn der Begriff „Wirtschaftskriminalität" verwendet wird, ist nach wie vor nicht definitiv ergründet. Eine allgemeingültige Definition, die über die wissenschaftlichen Disziplinen und behördlichen Instanzen hinweg angewendet werden kann, existiert nicht. Sozial-, Politik- und Rechtswissenschaften, Betriebswirtschaft,