TAGUNGSBERICHTE

Erlanger Cyber² Crime Tag 2020: IT-Forensik und Strafprozessrecht

von Dr. Christian Rückert und
*Wiss. Mit. Marlene Wüst**

Der Tagungsbericht enthält sprachlich bereinigte Zusammenfassungen der Transkriptionen der Vorträge und Diskussionsbeiträge. Der Vortragsstil der einzelnen Beiträge wurde überwiegend beibehalten. Dementsprechend wurde generell auch auf Fußnoten verzichtet. Der Erlanger Cyber² Crime Tag 2020 und die Erstellung dieses Tagungsberichts wurden vom Bundesministerium des Innern, für Bau und Heimat gefördert.

Am 30. September 2020 fand der Erlanger Cybercrime Tag (ECCT) zum vierten Mal statt– allerdings anders als die vergangenen Jahre. Die Corona-Pandemie berücksichtigend nahmen *Professor Dr. Christoph Safferling,* LL.M. (LSE) und sein Team der International Criminal Law Research Unit (ICLU) den „Cyber"crime Tag beim Wort und verwandelten die Tagung als „Erlanger Cyber² Crime Tag" in eine rein virtuelle Veranstaltung. Verschiedene Kommunikationsmöglichkeiten der Tagungsplattform wie Workshop-Räume und Coffee&Talk-Räume ermöglichten den knapp 130 Teilnehmenden, sich wie gewohnt über die Vorträge auszutauschen und zu vernetzen.

Mit dem Thema „IT-Forensik und Strafprozessrecht" widmete sich der EC²CT nicht überwundenen Herausforderungen und zu diskutierenden Fragestellungen der Strafverfolgungs- und Strafverteidigungspraxis. Die zu beobachtende rasante Entwicklung der Informationstechnik geht mit einer zumindest vorübergehenden Speicherung großer Datenmengen einher. Diese Daten enthalten Spuren, die menschliches Verhalten nachweisbar machen, was nicht nur bei Cyberkriminalität, sondern in allen Deliktsbereichen zunehmend relevant wird. Dies führt unter anderem zu folgenden Fragen: Wie können digitale Spuren in einem rechtsstaatlichen Verfahren gesichert werden? Bietet die StPO ausreichende Ermittlungsgrundlagen hierfür? Wie kann sichergestellt werden, dass digitale Spuren gerichtsverwertbar forensisch ausgewertet und die notwendigen Standards eingehalten werden? Werden die digitalen Beweismittel durch die an einem Strafverfahren beteiligten Strafjuristen[1] methodisch bewertet und kritisch überprüft?

Diese und weitere Fragen thematisierten die Experten *Juniorprofessor Dr. Dominik Brodowski,* LL.M. (UPenn) (Universität des Saarlandes), Staatsanwalt *Andreas Brück* (ZAC, NRW), *Johannes Pollach,* M.Sc. (ZCB) und Rechtsanwalt *Dr. Uwe Ewald* (Berlin) in ihren informativen Vorträgen auf der virtuellen Hauptbühne. Als mögliche Lösungsansätze zogen sich die Worte „Interdisziplinarität", „Austausch", „Standards" und „Expertise" wie ein roter Faden durch den Veranstaltungstag. Schon bei der Begrüßung durch die Vizepräsidentin Education der FAU, *Professor Dr. Bärbel Kopp*, den Grußworten von Generalstaatsanwalt *Thomas Janovsky* (ZCB) sowie in der Einführungsrede des Veranstalters, *Professor Dr. Christoph Safferling*, LL.M (LSE) wurde deutlich, dass die Beseitigung von Kompetenzdefiziten der eingesetzten IT-Forensiker, der am Strafverfahren beteiligten Juristen und der im Gesetzgebungsverfahren involvierten Abgeordneten und Beamten bereits bei einer fächerübergreifenden und innovativen Ausbildung ansetzen müsse. Ganz in diesem Sinne stand ein besonderes Highlight des diesjährigen EC²CT: die Unterzeichnung der Kooperationsvereinbarung zwischen der bei der Generalstaatsanwaltschaft Bamberg angesiedelten Zentralstelle Cybercrime Bayern (ZCB) und der Friedrich-Alexander-Universität Erlangen-Nürnberg. Mit dieser beginnt eine noch intensivere und engere Zusammenarbeit zwischen ZCB und FAU mit dem gemeinsamen Ziel, die Forschung, Lehre und Strafverfolgung auf dem Gebiet der Cyberkriminalität stärker voranzubringen und innovative Lösungen für anstehende Herausforderungen zu entwickeln.

I. Digitale Beweismittel im Strafverfahren – von 1877 bis 4.0 (*Juniorprofessor Dr. Dominik Brodowski*, LL.M. [UPenn], Universität des Saarlandes)

Eröffnet wurde die Vortragsrunde von *Dr. Dominik Brodowski*, Juniorprofessor an der Universität des Saarlandes. *Brodowski* nahm das interessierte Publikum mit auf einen Streifzug zu Problemen rund um digitale Beweismittel im Strafverfahrensrecht vom Jahr 1877 bis hin zu ungelösten Fragen der heutigen Debatte um die Digitalisierung.[2]

* *Dr. Christian Rückert* ist Habilitand und *Marlene Wüst* ist Doktorandin jeweils am Lehrstuhl für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht von *Professor Dr. Christoph Safferling*, LL.M. (LSE) an der Friedrich-Alexander-Universität Erlangen-Nürnberg.

1 Aus Gründen der besseren Lesbarkeit wurde an gegebenen Stellen das generische Maskulinum verwendet. Diese Formulierung umfasst gleichermaßen weibliche und männliche Personen.

2 Eine – auf älterem Rechtsstand beruhende – Langfassung des Vortrags findet sich bei *Jahn/Brodowski*, in: FS Rengier, 2018, S. 409-422, sowie *dies.*, in: Kudlich/Hoven (Hrsg.), Digitalisierung und Strafverfahren, 2020, S. 67-102.

1. Digitale Spuren und Beweismittel

Mehr und mehr Kriminalitätsformen sind heutzutage mit digitalen Spuren verbunden. Dies beruht im Wesentlichen auf drei Entwicklungstendenzen. Zunächst hat Cyberkriminalität im engeren Sinn an Bedeutung gewonnen. Darüber hinaus verlagert sich die Tatbegehung bei herkömmlicher Kriminalität zunehmend in das Internet und zuletzt gewinnen auch bei sonstigen Kriminalitätsformen digitale Spuren an Bedeutung. Die massenhafte Verbreitung von Smartphones führt dazu, dass mit diesen Geräten bewusst oder unbewusst von Tätern, Verletzten oder unbeteiligten Dritten erzeugte Daten wertvolle Anhaltspunkte für die Strafverfolgung liefern können. Doch was sind digitale Spuren? Gemeinhin werden diese als Spuren definiert, die auf Daten basieren, welche auf Computersystemen gespeichert oder übertragen worden sind. Sie stellen den tatsächlichen Ausgangspunkt in der Außenwelt dar, bedürfen aber einer digitalforensischen, kunstgerechten Erhebung, Auswertung und Interpretation, um aus ihnen strafverfolgungsrelevante Erkenntnisse zu gewinnen. Soweit solche digitalen Spuren als Beweismittel in einem Strafverfahren Verwendung finden sollen, bietet sich der Begriff des digitalen Beweismittels oder des elektronischen Beweismittels an.

2. Erhebung digitaler Spuren

Im Hinblick auf die Erhebung digitaler Spuren in einem strafrechtlichen Ermittlungsverfahren sowie deren Transfer in eine Hauptverhandlung finden sich in der StPO nur unzureichende Regelungen. Die zentralen Normen aus diesem Bereich stammen aus dem Jahr 1877 und werden in der praktischen Anwendung eher schlecht für Fragen der Digitalisierung passend gemacht. Grundlegend lassen sich drei fundamentale Differenzierungen im Rahmen der Erhebung digitaler Spuren vornehmen. Zunächst muss unterschieden werden zwischen bestehenden Daten, die bereits auf Datenträgern gespeichert sind oder ohnehin in Telekommunikationsnetzwerken transferiert werden, und neuen Daten, die erst durch Sensoren erfasst werden. Als Beispiel für ersteres ist die Beschlagnahme eines Datenträgers zu nennen, letzteres wäre etwa der Einsatz eines GPS Peilsenders, der kontinuierlich Positionsdaten in digitaler Form sendet. Zu differenzieren ist zudem zwischen offenen und verdeckten Ermittlungsmaßnahmen. Nach unserem Verfassungsverständnis wirken verdeckte, heimliche Ermittlungsmaßnahmen besonders schwer, da sie erst einmal ohne externe Kontrollmechanismen erfolgen. Deshalb sind sie materiellrechtlich auf hinreichend gewichtige Fallkonstellationen beschränkt und prozessual beispielsweise durch einen präventiven Richtervorbehalt oder Berichtspflichten abgesichert. Zuletzt existiert noch eine eher technisch anmutende Differenzierung zwischen allgemeinen Daten und Telekommunikationsdaten. Diese Unterscheidung ist aus grundrechtlicher Perspektive für die Frage wichtig, ob zusätzliche Schutzanforderungen der Kommunikationsfreiheit nach Art. 10 GG zu beachten sind. Zu einer Steigerung der Komplexität kommt es im Hinblick auf das europäische Recht, da hiernach zwischen Telekommunikation im engeren Sinn und Telemediendiensten unterschieden wird. Eine spannende, ungelöste Frage ist, ob man auch Telemediendienste mit einer Maßnahme nach § 100a StPO, die bekanntlich mit Telekommunikationsüberwachung überschrieben ist, erfassen kann. Die Eingriffsgrundlagen der StPO zeichnen die vorgenannten Differenzierungen nur unzureichend nach. Sie sind teils sehr spezifisch formuliert und schwer voneinander abzugrenzen. Sie weisen Regelungslücken auf, die in der praktischen Handhabung zu großer Rechtsunsicherheit führen.

3. Zugriff auf Daten(träger)

Es gibt verschiedene Möglichkeiten, durch einen offenen Zugriff Daten zu erheben. Der Provider kann um freiwillige Auskunft (§§ 161, 163 StPO) erbeten werden, wobei dies bei Anfragen im Ausland zu völkerrechtlichen Problemen führen kann. Eine weitere Zugriffsmöglichkeit besteht in der Herausgabepflicht nach § 95 StPO. Diese Norm kann gegenüber unverdächtigen Dritten als „decryption order" auch angewendet werden, um sich Daten in unverschlüsselter Form aushändigen zu lassen. Zudem ermöglicht die Online-Durchsuchung nach § 100b StPO einen Zugriff auf Daten, sofern die Maßnahmen im Inland erfolgen. Diese Norm wirft in verfassungsrechtlicher Hinsicht sowie in Bezug auf die technische Umsetzbarkeit viele Fragen auf. Praktisch bedeutsam sind Fragen des Anwendungsbereichs. So sind Laptops, Server und Smartphones taugliche Zielobjekt einer solchen Online-Durchsuchung, es könnten aber auch Smart-TVs oder Smart-Watches darüber überwacht werden. Ein weiteres Problem besteht in der Aktivierung von Sensoren. Diese kann nach der rechtswissenschaftlichen Literatur nicht auf § 100b StPO gestützt werden. Der klassische Weg der Sicherung digitaler Spuren führt aber über die Sicherstellung und Beschlagnahme. Es ist allgemein anerkannt, dass § 94 StPO auch Daten als beschlagnahmefähige Gegenstände erfasst. Hier ergeben sich in Bezug auf digitale Spuren fünf Problemkreise:

a) Beschlagnahme von „ruhender" Telekommunikation

Das erste Problem richtet sich auf die Beschlagnahme von Telekommunikationsdaten, insbesondere ruhender Telekommunikation. Spätestens seit einem Grundsatzbeschluss des *BVerfG* gelten die Vorschriften der Sicherstellung und Beschlagnahme gem. §§ 94 ff. StPO auch als taugliche Eingriffsgrundlage in Bezug auf die Telekommunikationsfreiheit nach Art. 10 GG. Das betrifft insbesondere die Frage, ob man ein E-Mail-Postfach, das sich auf den Datenspeichern eines inländischen Internet-Service-Providers befindet, auf diesem Wege ausforschen kann. Die klare höchstrichterliche Rechtsprechung besagt, dass dies als offene Maßnahme geschehen muss und der Betroffene unverzüglich zu benachrichtigen ist. Der *BGH* betont, dass ein Komplettzugriff auf ein E-Mail-Postfach aus Gründen der Verhältnismäßigkeit zu vermeiden ist. Deswegen besteht die technisch schwierig umzusetzende Anforderung, Filter- oder Suchkriterien anzuwenden. Bezüglich des verdeckten Zugriffs auf Telekommunikationsdaten, der bisher auf § 100a StPO gestützt wurde, ist fraglich, ob dies auch in Zukunft möglich sein wird, da der *EuGH* entschieden hat, dass es sich hierbei nicht um einen

Telekommunikationsdienst, sondern um einen Telemediendienst handelt.

b) Isolation des Beweismittels

Als Zweites stellt sich die Frage, was man mit einem sichergestellten oder beschlagnahmten informationstechnischen System alles machen darf. Ziel der Sicherstellung und Beschlagnahme ist es, die Integrität und Verfügbarkeit des Beweismittels für das weitere Strafverfahren zu gewährleisten. Durch eine Veränderung des Beweismittels – etwa durch das Weiterbetreiben eines beschlagnahmten Handys – wird diese Integrität verletzt. Deswegen muss man sich bemühen, das Beweismittel zu isolieren und darf es nicht weiter empfangsbereit halten und es darauf anlegen, dass es sich weiter verändert.

c) Überwindung von Verschlüsselungstechnologie

Ein aus Sicht der Strafverfolgungsbehörden gravierendes Problem ist, dass Daten vermehrt mit kryptographisch sicheren Methoden verschlüsselt werden. Ohne Kenntnis des Schlüssels kann der ursprüngliche Informationsgehalt nicht entnommen werden und der Beschuldigte darf nicht gezwungen werden, das Passwort zu nennen. Er genießt das verfassungs- und menschenrechtlich geschützte Recht, nicht an seiner eigenen Überführung mitwirken zu müssen. Grundsätzlich ist Verschlüsselungstechnologie sinnvoll und geboten, weswegen den Forderungen, den Einsatz von Verschlüsselungstechnologie zu beschränken oder staatliche Hintertüren einzubauen, eine Absage zu erteilen ist. Dies würde die Verschlüsselungstechnologie schwächen und Einfallstore für Angriffe Dritter bieten. Es gibt technische und organisatorische Mittel, um Verschlüsselungstechnologie in Strafverfahren zu überwinden. Informationstechnische Systeme können im laufenden, entschlüsselten Betrieb beschlagnahmt werden, (aufgefundene) Passwörter können probehalber eingetippt oder gespeicherte Passwörter über spezielle Rechtsgrundlagen angefragt werden. Eine gewisse Schwierigkeit existiert in Bezug auf biometrische Merkmale wie dem Fingerabdrucksensor zum Entsperren eines Mobiltelefons. Kann man einen Beschuldigten verpflichten, die Abnahme seines Fingerabdrucks zu diesem Zweck zu erdulden? Zum Teil wird dies auf § 81b StPO gestützt. Nach dieser Norm können Fingerabdrücke abgenommen werden, soweit es für den Zweck des Verfahrens notwendig ist. Allerdings handelt es sich der Überschrift zufolge um erkennungsdienstliche Maßnahmen. Die Entschlüsselung eines Smartphones ist ein tiefgreifender Eingriff, der eine Eingriffsgrundlage wie § 81a StPO erfordert. Jedoch passt auch diese Norm nicht genau. Schließlich dient § 100b StPO der Überwindung von Verschlüsselungstechnologie.

d) Zugriff auf entfernte Speichermedien (§ 110 Abs. 3 StPO)

Daten sind häufig nicht mehr lokal vorgehalten, sondern in Rechenzentren ausgelagert. Der Durchsuchungsbeschluss ist aber räumlich auf ein Durchsuchungsobjekt begrenzt und erfasst ausgelagerte Rechenzentren nicht. § 110 Abs. 3 StPO wurde geschaffen, um auch auf räumlich getrennte Speichermedien zugreifen zu können. Ein zentrales Problem dieser Norm besteht jedoch darin, dass sie nach vorherrschender Ansicht nur Zugriffe auf inländische Datenspeicher legitimieren kann, da ausländische Datenspeicher den Souveränitätsrechten anderer Staaten unterliegen. In der Praxis wird dieses Problem oftmals durch ein Nichtwissen um den Standort der Daten umgangen. Es stellen sich jedoch insbesondere im aktuellen europäischen Kontext die schwierigen Fragen: Welche Relevanz hat der Speicherort? Sind die Behörden desjenigen Staates, in dem solche Daten gespeichert sind, wenigstens zu informieren? Sollen sie ein Widerspruchsrecht haben, wenn Ermittler auf die Daten zugreifen?

e) „big data“

Ein weiteres Problem ist die Auswertung großer Datenmengen, sog. „big data“. Es ist keine Seltenheit, dass mehrere Terrabyte an Daten beschlagnahmt werden. Dies bedeutet sowohl für die Strafverfolgung als auch für die Strafverteidigung ein Ressourcenproblem. Mittlerweile gibt es verschiedene Ansätze, wie man unter gewissen rechtlichen und technischen Voraussetzungen Legal Tech und die sog. künstliche Intelligenz zur Lösung dieses Problems einsetzen könnte. Die zunehmende, massenhafte Speicherung von Daten wirft außerdem das Problem des digitalen Zufallsfundes auf sowie die Frage, wie Eingriffe weiter fokussiert werden können.

4. Von digitalen Spuren zu elektronischen Beweismitteln

Inwieweit passen die Beweismittel des Strengbeweisverfahrens nun auf digitale Spuren? Die Inaugenscheinnahme gestattet die sinnliche Wahrnehmung des Beweismittels: sehen, hören, riechen, schmecken, fühlen. Daten bedürfen jedoch einer Transformation bzw. Aufbereitung, um diese als Ausdruck oder durch Abspielen auf einem Bildschirm in Augenschein zu nehmen. Bei einem Urkundsbeweis wird ein Schriftstück verlesen und damit über die in der Urkunde enthaltene Gedankenerklärung Beweis erhoben. Seit dem 1.1.2018 kann man auch elektronische Dokumente wie eine verkörperte Urkunde verlesen, wobei der Begriff des elektronischen Dokuments allerdings ungeklärt ist. Der Zeugenbeweis bezieht sich auf Wahrnehmungen einer Person und damit auch nur indirekt auf digitale Spuren. Gleiches gilt für Sachverständige, die über ihr Gutachten berichten. Auch hier geht es um eine Transformation der ursprünglichen digitalen Spuren. Wann sind digitale Beweise nun statthaft? Das Gericht unterliegt nach § 244 Abs. 2 StPO einer Aufklärungspflicht, die jedoch darauf beschränkt ist, den Anklagevorwurf zur Überzeugung des Gerichts aufzuklären. Hiernach wird es in der gerichtlichen Praxis nicht selten entbehrlich sein, über digitale Spuren und daraus gewonnene Erkenntnisse umfassend Beweis zu erheben.

5. Würdigung digitaler Beweise

Das Gericht ist nicht an fallunabhängige Beweisregeln gebunden, vielmehr ist die Würdigung von Beweisen, gleich ob digital oder analog, frei. Um vor der Rechtsordnung

Bestand zu haben, muss die Würdigung lückenlos, logisch widerspruchsfrei und für Außenstehende hinreichend nachvollziehbar erfolgen. Dabei bietet der gern überschätzte Aussagegehalt eines digitalen Beweismittels genügend Fallstricke. Eine ausgedruckte E-Mail, die im Urkundsbeweis verlesen wird, besagt noch nichts über den Urheber. Der Mitschnitt einer TKÜ besagt für sich genommen noch nicht, welche Personen miteinander gesprochen haben. Auch das Auffinden eines USB-Sticks mit kinderpornografischen Bilddateien in einer Wohnung belegt noch nicht, dass es der Wohnungsinhaber war, der diese Bilder vorsätzlich besitzt. Für eine logisch widerspruchsfreie Beweiswürdigung sind fehlende Feststellungen durch weitere Beweise zu treffen. Außerdem muss versucht werden, Fehlerquellen bei der Erhebung, Auswertung und Analyse digitaler Spuren weitgehend zu unterbinden. Diese Zwischenschritte werden nicht durch das Gericht vorgenommen, sondern von Polizeibeamten und Informatikern sowie zum Teil durch externe Dienstleister. Es ist zu fragen, was die digitalforensischen, kunstgerechten Standards bei so einer Auswertung sind. Im Bereich von DNA-Analysen hat es Jahrzehnte gedauert, diese Standards zu entwickeln. Es ist zu hoffen, dass die Wissenschaft und Praxis nicht zu lange benötigt, um digitalforensische Standards in die gerichtliche Praxis zu bringen.

6. Q&A-Session

Die sich dem Vortrag anschließende Fragerunde drehte sich insbesondere um zwei Themenkreise. Zunächst wurde der Zugriff auf räumlich getrennte Speichermedien nach § 110 Abs. 3 StPO diskutiert. Diese unscheinbar wirkende Norm bietet ein Einfallstor für weltweite Durchsuchungen von Cloudspeichern. Als Ergebnis eines politischen Kompromisses kann man sie als hybride Norm bezeichnen, die einerseits eine offene Durchsuchungsmaßnahme erfordert, andererseits aber dritte Personen betreffen und somit (teil-)verdeckt sein kann. Beachtenswert ist zudem, dass die Norm häufig als Grundlage für Auswertungen von Datenträgern Monate nach der Sicherstellung dient. Dies ist im Hinblick auf die Ratio der Norm, einen drohenden Beweisverlust zu verhindern, fragwürdig. Daneben rückte die E-Evidence-Verordnung in den Fokus der Debatte. Hierdurch soll es innerhalb der Europäischen Union ermöglicht werden, Daten bei Internetdienstleisteranbietern aus der ganzen Welt unabhängig davon anzufordern, wo die Daten gespeichert sind, solange diese in Deutschland Dienste erbringen. Dies ist insbesondere vor dem Hintergrund problematisch, dass im Einzelfall nicht nur Souveränitätsrechte von EU-Staaten, sondern auch von Drittstaaten durch diese Maßnahmen betroffen wären.

II. Die sog. Blackbox-Problematik bei IT-Forensiktools (*Johannes Pollach,* M.Sc., ZCB)

Das Rednerpult übernahm als Nächstes der bei der Zentralstelle Cybercrime Bayern (ZCB) tätige IT-Forensiker *Johannes Pollach,* M.Sc. Er gewährte dem Publikum einen Einblick in seine Tätigkeit, machte es mit den Grundlagen der digitalen Forensik vertraut und rückte die Problematik der sogenannten Blackbox in das Bewusstsein der Zuhörer.

1. Grundlagen zur digitalen Forensik

Die digitale Forensik beschreibt den Vorgang, juristische Fragestellungen mit wissenschaftlichen Methoden der Informatik zu beantworten. Wird gefragt, ob ein Bild auf dem Computer vorhanden ist, lässt sich zum Beispiel über Hash-Sets technisch nachweisen, dass dieses Bild unter einem bestimmten Pfad auf dem Gerät vorhanden ist. Ähnlich wie bei anderen Wissenschaften gibt es verschiedene Anforderungen, die an die digitale Forensik gestellt werden. Hierzu gehören insbesondere Akzeptanz, Glaubwürdigkeit, Reproduzierbarkeit, Integrität und Dokumentation. Die angewandten Methoden müssen in der Fachwelt bekannt und akzeptiert sein. Sie müssen funktional und robust und die zustande gekommenen Ergebnisse nachvollziehbar sein. Wenn dritte Personen den Prozess wiederholen, sollten identische Ergebnisse herauskommen. Asservate sollten so wenig wie möglich verändert und notwendige Veränderungen gut dokumentiert werden. Die Dokumentation ist wichtig, damit nachfolgende Behörden oder andere Forensiker die Ergebnisse validieren und den Prozess überprüfen können.

a) Der forensische Prozess (SAP-Modell)

SAP bedeutet Secure, Analyse and Present – sichern, analysieren und darstellen. Den Beginn der Tätigkeit eines Forensikers bildet die Daten-Extraktion. Diese kann unter anderem durchgeführt werden, indem eine Festplatte mit Hilfe eines Writeblockers an einen Auswerterechner angeschlossen wird, wobei der Writeblocker einen Schreibzugriff auf die Festplatte unterbindet. Beim PC lässt sich dies durch das Ausbauen der Festplatte und einer Verbindung mit dem Writeblocker erreichen. Die Daten werden 1:1 kopiert und können später analysiert werden, ohne das Asservat zu verändern. Schwierig ist es bei Smartphones. Hier werden spezielle Geräte benötigt, weil Smartphones keine Festplatte besitzen. Die nächste Phase ist die Analyse der durch die Extraktion erlangten Daten. Die Daten werden in spezielle Programme übertragen, die diese automatisch aufbereiten und in geeigneter Weise darstellen. Ausgewertet werden insbesondere Google-Suchanfragen und Chatnachrichten. Der letzte Teil des forensischen Prozesses ist die Berichtsfunktionalität. In einem Untersuchungsbericht werden alle Veränderungen – am besten mit Zeitstempel – dokumentiert, die an einem Asservat durchgeführt wurden. Dies dient der Dokumentation und der Beantwortung späterer Rückfragen im Verfahren. Ein wichtiger Teil ist hierbei die Visualisierung. Für den Auftraggeber sollte leicht zu erkennen sein, was das Ergebnis der forensischen Untersuchung ist. Der Bericht sollte die Zusammenhänge der Asservate aufzeigen und deutlich machen, auf welchen Asservaten wichtige verfahrensrelevante Daten enthalten sind und welche hingegen irrelevant oder für das Verfahren nicht geeignet sind.

b) Sicherungsarten und Probleme

In der Forensik gibt es drei Sicherungsarten: physisch, logisch und Dateisystem. Die angestrebte Sicherungsart ist die physische, die 1:1-Kopie des Speichers. Hier werden alle Daten erhoben, inklusive geschützter und gelöschter Bereiche. Bei der logischen Sicherung werden nur Dateien gesichert, keine geschützten oder gelöschten Bereiche. Manchmal wenden Tools Tricks an, um allgemeine Informationen wie Anruflisten oder SMS aufzubereiten. Ein großes Problem ist jedoch, dass Anwendungen wie WhatsApp und andere Messenger nicht in logischen Sicherungen enthalten sind. Deswegen ist es wichtig, eine physikalische Sicherung anzufertigen. Die letzte und schlechteste Sicherungsart ist das Dateisystem. Hier werden alle Daten ausgewertet, auf die man über eine gewöhnliche USB-Verbindung zugreifen könnte.

Um die Blackbox-Problematik besser zu verstehen, sollte man zwischen den Sicherheitstechnologien von PCs und Smartphones unterscheiden. Zunächst lässt sich der Speicher des PCs in der Regel ausbauen und ist somit leicht zugreifbar, wohingegen der Speicher des Handys fest verlötet ist und durch Auslötung zerstört wird. Überdies sind USB-Schnittstellen beim Computer meist frei zugänglich. Beim Handy ist hingegen eine explizite Aktivierung der Dateifreigabe notwendig. Verschlüsselungen müssen beim PC explizit aktiviert werden –was in der Praxis selten geschieht. Beim Handy ist diese werkseitig aktiviert. Auch ist ein Angriff auf die Verschlüsselung bei PCs meist simpel, da man das Asservat an einen anderen Rechner anstecken und den Angriff auf die Verschlüsselung dort durchführen kann. Beim Handy wird die Verschlüsselung regelmäßig über ein integriertes Bauteil realisiert, weshalb der Angriff nur direkt auf dem Gerät möglich ist, was den Prozess verlängert. Zudem können beim Computer alternative Betriebssysteme geladen werden, was beim Handy standardmäßig nicht möglich ist. Durch Laden anderer Systeme kann man Sicherheitslücken im eigentlichen System ausnutzen und dadurch eine Datenextraktion durchführen. Auch beim Computer gibt es Sicherheitsmechanismen, sog. TPM-Chips. Allerdings sind diese oftmals nicht aktiv, wohingegen bei Handys der Hardware Keyscore als Sicherheitsmechanismus dient und meist aktiv ist und eingesetzt wird.

2. Aktuelle Probleme in der Forensik

Aufgrund dieser Umstände ist es bei PCs in der Regel einfach, eine physikalische Sicherung anzufertigen und auf die Daten zuzugreifen. Die Problematik liegt eher in der großen Anzahl an Anwendungen, die aufbereitet werden müssen. Zwar existieren hier auch Verschlüsselungen, jedoch können diese durch externe Ressourcen meist gut angegriffen werden. Im Smartphone-Bereich ist die Forensik aufgrund der Vielzahl an verwendeten Betriebssystemen und Herstellern, von denen jeder eigene Sicherheitsfeatures anbietet, schwierig. Für jeden Hersteller und teilweise jedes Gerät müssen Sicherheitslücken gefunden werden. Dies ist von Firmen erkannt worden. Mittlerweile bieten verschiedene Softwarehersteller eigene Lösungen an, um die Probleme der Varianz an Programmen und Sicherheitsfeatures bei den Endgeräten zu meistern und Forensikern Lösungen bereitzustellen. Bei diesem Prozess gibt es jedoch keine Dokumentation, wie die Extraktion erfolgt ist, welche Sicherheitslücken ausgenutzt wurden, ob es mögliche Probleme gab sowie ob Daten verändert wurden. Somit stellt sich die Frage, wie das Ergebnis überprüft werden kann.

Nachfolgend werden einige unter das Stichwort „Blackbox“ fallende gravierende Probleme dargestellt. Hierbei ist zu beachten, dass die Tools in der Forensik benötigt werden und ihre Daseinsberechtigung haben. Die geübte strenge Kritik dient dazu, der zunehmenden Intransparenz, Geheimhaltung und Abstraktion in der Forensik entgegenzuwirken und die Schaffung offener Standards zu erreichen.

3. Blackbox-Problematik 1: Phase Secure

Ein Problem in der Extraktionsphase besteht darin, dass in die Korrektheit des Prozesses vertraut wird. Beispielsweise wurde in einem vergangenen Fall trotz physikalischer Sicherung eines Smartphones und mehrmaliger Durchführung der Sicherung kein Beweismittel gefunden. Der Hersteller des Asservats hatte zwei Speicherchips verbaut und die Forensiksoftware hatte nur den ersten ausgelesen. Diese fehlende Dokumentation und Nachvollziehbarkeit von Prozessen führt an mehreren Stellen zu Problemen. So werden verschiedene Methoden der physikalischen Auslesung angeboten, ohne weitere Informationen, was diese genau machen. Extraktionsmethoden benötigen zudem teilweise mehrere (zum Teil bis zu 40) Versuche. Erfahrungen zeigen, dass das Smartphone für eine erfolgreiche Extraktion manchmal in einem bestimmten Zustand sein muss. Dies wird weder in der Fehlermeldung angezeigt, noch wird darauf hingewiesen, dass eine erfolgreiche Extraktion mehrere Versuche benötigen kann. Hierdurch entstehen die verschiedensten Tipps zur Durchführung einer Extraktion, ohne dass sie wissenschaftlich belegt sind. Unerfahrene Forensiker kennen die Problematiken häufig nicht und geben die Asservate aufgrund der Fehlermeldungen ab. Kritisch ist außerdem, dass bei den Tools keine Quellcode-Prüfung durch Dritte stattfindet. Überdies verschwinden manche Extraktions-Methoden in neueren Software-Versionen, ohne dass die Anwender hierüber informiert werden und aktuelle Geräte werden meistens nicht unterstützt. Bei neueren Geräten wird es aufgrund der Sicherheitsfeatures immer schwieriger, (physikalische) Datenextraktionen durchzuführen. Hierdurch werden auch Sicherheitslücken immer teurer und Unternehmen bieten zum Schutz ihrer Investitionen In-House Services an. Man kann die aktuellen Geräte gesperrt einschicken und für eine beträchtliche Summe entsperren oder eine Datenextraktion durchführen lassen. Dieser Prozess erzeugt enorme Kosten, ist absolut intransparent und ermöglicht keinerlei Kontrolle bezüglich der Asservate und Daten. Nachdem viele Behörden aus diesen Gründen In-House Services nicht nutzen konnten, haben die Hersteller neue Lösungen kreiert. Es gibt mittlerweile ein Produkt, dass den In-House-Dienst beim Kunden durchführen kann. Zum Schutz der Investition unterliegen

diese Produkte der maximalen Geheimhaltung, sog. NDA (non-disclosure-agreement). Dies hat sehr viele Nachteile für Forensiker, weil es einen Erfahrungsaustausch unmöglich macht. Für manche Behörden wird es hierdurch schwer, die Produkte anzuschaffen. Sie haben keine Kenntnis über deren Möglichkeiten und können die Investition nicht begründen.

4. Blackbox-Problematik 2: Phase Analyse

In dem Bereich der Datenanalyse ist die Transparenz keine große Problematik. Das Problem liegt vielmehr in der geringen Erkennungsrate und Unterstützung von Softwares. Aufgrund der Vielzahl von Anwendungen kommt es häufig vor, dass die auf dem Asservat installierten Anwendungen nicht von der Software unterstützt werden. Ein großer Vorteil der Analyse-Tools liegt jedoch darin, dass sie viele Informationen liefern und dargestellt wird, wie diese Informationen zustande gekommen sind. Ein Nachteil ist wiederum der Umstand, dass diese Programme viel händische Arbeit erfordern. Sie müssen zunächst manuell aufbereitet werden, um anschließend einen Prozess für die automatisierte Aufbereitung generieren zu können. Trotzdem sind die Anwendungen auch für erfahrene Forensiker sehr hilfreich, da sie die „Top-Anwendungen" wie Messenger-Dienste oder Browser unterstützen. Kritisch ist jedoch, dass manche Hersteller bei Problemen sehr intransparent agieren. Bei vielen Programmen gibt es keinen öffentlich zugänglichen Bugtracker; die Fehler sind meistens geheim, werden nicht bekanntgeben und behoben, ohne dass der Kunde informiert wird. So passiert es, dass in einer Version bestimmte Analysetechniken verwendet werden können und in der nächsten Version nicht mehr. Nirgends wird kommuniziert, dass die Funktionalität in dieser Version nicht mehr vorhanden ist. Dies hat dazu geführt, dass viele Forensiker alte Versionen aufheben und manchmal Analysen mit älteren Softwares durchführen. Da die Fehler nicht öffentlich dokumentiert werden, kann es passieren, dass die Version, mit der die Daten analysiert wurden, plötzlich verschwindet. Bei auftretenden Problemen werden Forensiker als Software-Tester oder Bugreporter missbraucht. Wochenlange Kommunikation und Aufforderungen zu verschiedenen Lösungsversuchen lassen bezweifeln, dass die Hersteller eigene Softwaretests zum Erkennen von Fehlern durchführen. Die Gefahr, solche Fehler zu übersehen, wird dadurch vergrößert, dass durch die automatisierte Aufarbeitung oftmals ein „Tunnelblick" entwickelt und eine händische Prüfung unterlassen wird. Ein großes Problem lässt sich außerdem in den Interpretationsspielräumen bei Begrifflichkeiten in den Anwendungen feststellen. Es werden keine Differenzierungen bei den Aufbereitungen getroffen. So haben zum Beispiel zwei Anwendungen verschiedene Teilnehmerzahlen einer WhatsApp-Gruppe geliefert, als festgestellt werden sollte, wer ein inkriminiertes Bild erhalten hatte. Bei genauerem Hinsehen wurde klar, dass ein Tool nur den Stand der Teilnehmer zum gefragten Zeitpunkt anzeigte, während beim anderen auch alle ehemaligen Teilnehmer gelistet wurden.

5. Blackbox-Problematik 3: Phase Present

Im Rahmen der Dokumentation gibt es insgesamt wenig Blackbox-Problematiken. Eine nennenswerte Schwierigkeit besteht darin, dass manche Tools automatische Berichte erstellen, die meist sehr generisch und nicht für die Verhandlung geeignet sind. Hier sollte Qualität statt Quantität geliefert werden. Es existieren keine Standards, weshalb die Berichte und Gutachten der Forensiker sich in Aufbau und Untersuchungstiefe unterscheiden. Darüber hinaus erstellen Forensiker aufgrund der Ansicht, dass weniger Inhalt im Bericht zu weniger Problemen führt, teilweise selbst Blackboxes. Verbesserungsbedarf besteht auch im Bereich des Wissenstransfers. Meist sind Schulungen in der Forensik als Produktschulungen ausgestaltet, bei denen erklärt wird, wie bestimmte Blackbox-Tools bedient werden. Wichtiger wären Methoden- und Grundlagenschulungen, bei denen Hintergründe und Prozesse erläutert werden. Unter Forensikern ist außerdem die negative Entwicklung zu beobachten, dass das Wissen, wie man Daten extrahieren oder aufbereiten kann, zunehmend geheim gehalten wird. Entgegen diesem Trend muss das Wissen transferiert werden, damit es wachsen kann und in der Zukunft Datenextraktionen durchgeführt werden können, die bisher nicht möglich waren.

6. Q&A-Session

In der sich dem Vortrag anschließenden Q&A-Session wurde eine weitere Dimension der Blackbox-Problematik thematisiert. Es stellt sich die Frage, wie viele Informationen über die verwendeten Tools der Strafverteidigung und dem Beschuldigten zur Verfügung gestellt werden müssen. Von Seiten der Strafverfolgung bestehen hier teilweise Bedenken, dass dieses Wissen leicht von Kriminellen verwendet werden könnte. Mittlerweile gibt es jedoch eine Vielzahl an antiforensischen Maßnahmen, so dass durch das Offenlegen der Methoden, insbesondere der Bekanntgabe der verwendeten Version, wohl keine schweren negativen Folgen zu befürchten sind. Bei kommerziellen Tools besteht allerdings das Problem, dass diese an Lizenzkosten gebunden sind und Dritten aus diesem Grund nicht zur Verfügung gestellt werden können. Darüber hinaus wurde debattiert, wie eine Transparenz für Forensiktools am besten reguliert werden könnte. Als eine wünschenswerte Möglichkeit erscheint es, dass die öffentliche Hand – etwa die ZITiS – selbst Forensiktools entwickelt.

III. Cybercrime aus Sicht der Strafverfolgung – Recht und Praxis (StA *Andreas Brück*, ZAC NRW)

Nach der Mittagspause referierte Staatsanwalt *Andreas Brück* über Cybercrime aus Sicht der Strafverfolgung. StA *Andreas Brück* ist bei der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) tätig. Zum Aufgabenbereich der ZAC gehört die Führung herausgehobener Ermittlungsverfahren im Bereich des Cybercrime, die Thematisierung von Grundsatzfragen (z.B. im Bereich von Ermittlungstechniken oder rechtlichen Einschätzungen) sowie die Aus- und Fortbildung von Justiz und Polizei.

1. Kriminalitätsfeld Cybercrime

Es stellt sich immer wieder die Frage, was unter „Cybercrime“ zu verstehen und wie bedeutend dieses Kriminalitätsfeld tatsächlich ist. Bei einem Blick auf die Zahlen wird schnell klar, dass Cybercrime längst keine Nische mehr ist. Prozentual gesehen liegt Cybercrime im Hinblick auf den hierdurch jährlich entstehenden Schaden mit konventionellen Deliktsfeldern wie Drogenhandel und Produktfälschung auf Augenhöhe. Statistiken nennen eine Schadenssumme von weltweit 445 Mrd. USD jährlich.

a) Tätertypologie

In den verschiedenen Cybercrime-Verfahren und -phänomenen erscheinen unterschiedliche „klassische“ Täter. Das Bild des Hackers, wie er teilweise in Film oder Fernsehen dargestellt wird, ist kaum mehr anzutreffen. Einzeltäter sind in der Szene fast völlig ausgestorben und wurden von Szenetätern ersetzt. Eine deutsche Cybercrime-Szene hat sich auf allen möglichen Plattformen organisiert. Diese Szene umfasst einen „harten Kern“ sowie eine große Anzahl an Mitläufern und Gelegenheitstätern. Die Szenetäter agieren typischerweise im Fraud-Bereich und begehen verschiedenste Straftaten wie Kreditkartenmissbrauch, Bestellbetrügereien oder einfache Hacking-Szenarien. Hiervon abzugrenzen sind die sogenannten Hacktivisten – Akivisten, die für eine bessere Welt hacken. Sie führen beispielsweise DDoS-Angriffe auf Chemieunternehmen durch, um ihren Unmut gegen Tierversuche kundzutun. Der größte Teil der Verfahren in der ZAC betrifft OK-Gruppierungen (Organisierte Kriminalität) und (Dritt-)Staatlich induzierte Kriminalität. Im Wesentlichen hat die Zentralstelle es mit professionalisiertem Vorgehen in organisierten Kriminalitätsstrukturen zu tun. Diese OK-Gruppierungen spezialisieren sich auf unterschiedliche Felder wie zum Beispiel Banking-Betrugsverfahren oder Angriffe auf Industrieunternehmen. Die (Dritt-)Staatlich induzierte Kriminalität ist die am schwersten zu fassende und zu bezeichnende. Hierunter fallen zum einen Szenarien der Wirtschaftsspionage. Zum anderen kann dies auch schlichte schädigende Ereignisse betreffen, wenn unklar ist, ob sie von einem Drittstaat oder einer OK-Gruppierung aus einem anderen Staat verübt wurden. Dies kann etwa der Fall sein, wenn Infrastrukturen gezielt und über längere Zeit angegriffen und unterwandert werden.
Cybercrime ist in der Form, wie wir sie heute sehen, ein hoch professionelles Geschäftsfeld mit hohen Schadenssummen. Im Rahmen dieser Professionalisierung ist ein Trend zur Kriminalität als Dienstleistung, sog. „Crime-as-a-service“, erkennbar. Im Gegensatz zum klassischen Bild des Hackers, der im Keller sitzt und allein eine Firma angreift, müssen Hacker heutzutage nicht mehr in der Lage sein, einen Hacking-Angriff selbst umzusetzen. Sie können Autoren von Schadsoftware ebenso wie die Dienstleistung für den Angriff kaufen und diesen mit dem entsprechenden (technischen) Support durchführen.

b) Werkzeuge der Strafverfolgungsbehörden

Wie kann die Justiz dagegen vorgehen? Die relevanten Normen zur Beschlagnahme und Sicherstellung (§§ 94, 98 StPO) stammen, wie im ersten Vortrag bereits erörtert, aus dem Jahr 1879. Mit diesen 150 Jahre alten Normen versuchen die Strafverfolgungsbehörden, weltweit Server zu beschlagnahmen und sicherzustellen, um an Daten und Beweismittel zu kommen. Oftmals ist die StPO nicht auf dem Stand, mit dem die Strafverfolger tatsächlich konfrontiert werden. Allerdings hat sich die StPO seit der Einführung der §§ 94 ff. StPO auch weiterentwickelt. So hat die Strafverfolgung als Reaktion auf die zunehmende Computerkriminalität neue Werkzeuge in Form der Quellen-TKÜ und der Online-Durchsuchung an die Hand bekommen. Mit der Quellen-TKÜ ist es mittlerweile möglich, mit technischen Mitteln in die IT des Beschuldigten einzudringen, um Informationen auszuleiten oder Telekommunikation zu überwachen. Bei der Online-Durchsuchung dürfen die Strafverfolger mit technischen Mitteln die IT-Geräte des Beschuldigten kompromittieren und infiltrieren, um daraus im Rahmen der Online-Durchsuchung Daten zu erheben. Dies war für die Ermittler wichtig, um zielgerichtet anstelle von massenhaften Erhebungen und Grundrechtseingriffen agieren zu können. Doch wie funktioniert die Online-Durchsuchung eigentlich? Ein Problem besteht in der praktischen Umsetzung. Nach heutiger Rechtslage kann bei Vorliegen einer Katalogtat auf die IT des Beschuldigten zugegriffen werden. Problematisch ist allerdings, dass bei der verdeckten Maßnahme regelmäßig ein körperlicher Zugriff auf die IT nicht stattfinden kann. Bei der Online-Durchsuchung nach § 100b StPO fehlt jedoch eine Betretungsbefugnis der Ermittler. Sie können nicht in eine Wohnung eindringen und auf ein Gerät zugreifen, um heimlich eine Infiltrierung zu ermöglichen. Somit wird die Infiltration über einen Trojaner, eine Ferninfiltrierung oder Ähnliches notwendig. Bei solchen Fernzugriffen hängt der Erfolg regelmäßig vom Verhalten des Beschuldigten ab. Soll eine Schadsoftware installiert werden, muss der Beschuldigte auf eine E-Mail, die man ihm sendet oder deren Anhang klicken. Praktisch ist die Online-Durchsuchung allein aufgrund dieser technischen Hemmnisse der konventionellen TKÜ bei weitem noch nicht gleichgestellt. Für die Zukunft stellt sich die Herausforderung, wie die gesetzlichen Anforderungen mit höchstmöglicher Effektivität umgesetzt werden können.

2. Die Phänomene

Die ZAC hat es im Rahmen ihrer Cybercrime-Bekämpfung mit verschiedenen Phänomenen zu tun, die unterschiedliche Herausforderungen mit sich bringen. Diese werden nachfolgend näher betrachtet.

a) CEO-Fraud

Ein für Cybercrime etwas untypisches Phänomen, in dem die ZAC viele Verfahren führt, ist der CEO-Fraud. In dieser Fallkonstellation weist ein vermeintlicher CEO ein Unternehmen an, eine Überweisung zu tätigen. Überweist der Mitarbeiter oder die Buchhaltung die Summe, entsteht dem Unternehmen ein Schaden in dieser Höhe. Warum ist die ZAC für solche Fälle, die im Kern ein schlichtes Betrugs-Szenario darstellen, zuständig? Ein näherer Blick in die Verfahren machte deutlich, dass die Täter mit großer Sachkunde aus dem Unternehmen ausgestattet waren. Die

Täter, die am Anfang telefonisch Kontakt aufgenommen hatten, wussten, dass der CEO auf Geschäftsreise ist und stellten sicher, dass der Anruf bei der richtigen Person zur richtigen Zeit ankommt. Die später übersendete E-Mail passte sowohl bezüglich der E-Mail-Adresse als auch der vermeintlichen schriftlichen Signatur bis hin zur Diktion genau in das Unternehmen (es war bewusst, wer geduzt und wer gesiezt wurde; wie der CEO tatsächlich die betroffene Person anrufen würde). Durch diese Umstände entstand die Hypothese, dass es sich um einen technischen Angriff handeln könnte. Sich anschließende Ermittlungen bestanden zunächst aus TKÜ-Maßnahmen, mit denen versucht wurde, die Telefonnummer zu identifizieren und zu überwachen. Hierdurch konnten die Strafverfolger parallel zu den Taten mithören, wie die Täter andere Geschädigten anriefen und konnten mit diesen Unternehmen Kontakt aufnehmen. Bei den Ermittlungen hat sich herausgestellt, dass der Kenntnisvorsprung tatsächlich ausgesprochen gut war, jedoch nicht durch einen technischen Hack erlangt wurde. Vielmehr wurden Informationen aus öffentlichen Medien, aus sozialen Medien, aus Internetseiten und allen möglichen anderen Quellen zusammengetragen. So wurde beispielsweise der für die Überweisung zuständige Buchhalter zwei Wochen vor der Tat vermeintlich vom CEO angerufen. Vorbereitend für die Tat wurde ihm für seine Mitarbeit gedankt und zum Geburtstag gratuliert, der über die sozialen Medien bekannt war. Dies diente dazu, dass der Buchhalter die Stimme der Täter kennenlernte und die Authentizität des späteren Anrufs nicht in Frage stellte. In einer anderen Situation lehnte die Buchhaltung die Überweisung mit der Begründung ab, dass nach Unternehmensgepflogenheiten Überweisungen nur bei Abzeichnung zweier Prokuristen getätigt werden. Die Täter fragten sodann das notwendige Formular bei dem Buchhalter an und sandten dies mit Unterschriften zweier Vorstandsmitglieder zurück. Diese Unterschriften erhielten sie aus dem Handelsregister durch eine dort abgeschlossene Premiummitgliedschaft. Zusammenfassend lässt sich beim CEO-Fraud feststellen, dass nicht nur das technische Hacken ein Problem sein kann. Vielmehr hat ein soziales Hacken die Täter in die Lage versetzt, durch Kommunikation und Information ein Vertrauen aufzubauen und dieses Vertrauen bei der Tatbegehung auszunutzen. Dies wirft die ein oder andere Frage auf, wie wir in der Öffentlichkeit mit Informationen umgehen und was wir tatsächlich von uns preisgeben wollen und uns dadurch verletzbar machen.

b) CEO-Fraud 2.0.

Die letzte Ausbaustufe des CEO-Fraud ist eine neue Betrugsmasche, die mit den Ursprungstaten nichts mehr zu tun hat. Hier wird mit einer Stimmimitation durch KI-Software gearbeitet, die in der Lage ist, die Stimme des Vorgesetzten perfekt zu imitieren. Dies erhöht den Vertrauensvorschuss erheblich. Die Schäden, die durch diese Masche weltweit entstanden sind, gingen in den hohen Millionen- bis Milliardenbereich. Bei der ZAC wurden ca. 150 Verfahren einer Tätergruppe zugeordnet, die einen Schaden von 150 Mio. USD verursachte. Die Täter konnten letztlich durch TKÜ-Maßnahmen und internationale Zusammenarbeit identifiziert werden.

c) Erpressung 2.0 – Beispiel „NotPetya"

Heutzutage erfolgt nahezu die Hälfte aller Erpressungen über das Internet. Das kann ein DDos-Angriff sein, bei dem eine Vielzahl von Computern aus einem Botnetz heraus auf ein Ziel zugreift, um dieses lahmzulegen und dann erpressen zu können. Es kann aber auch eine Ransomware sein, die verteilt wird, um auf dem Rechner zu Hause eine Verschlüsselung oder Sperre herbeizuführen. Diese bringt den Geschädigten zur Zahlung eines bestimmten Betrags – im Regelfall in Bitcoin. Die Ransomware in dieser Form ist schon seit einigen Jahren bekannt. Die ersten Vorläufer stammen aus den 80er/90er Jahren. Ab etwa 2011/2012 hat das Ganze eine neue Popularität gewonnen und an Masse und zuletzt auch an Qualität stark zugenommen. Früher gab es Angriffe auf Privathaushalte mit dem Ziel, eine Zahlung zu erlangen. Heute ist es ein „unternehmerisches Massengeschäft" und kritische Infrastrukturen sollen zu einer Zahlung für die Rekonstruktion bewegt werden. Hierbei handelt es sich um eine völlig neue Dimension, wie nachfolgendes Beispiel verdeutlicht.

Im Sommer 2017 wurde der Hackerangriff „NotPetya" verübt, der zu einem weltweiten Gesamtschaden von etwa 10 Mrd. USD führte. Dem lag folgendes Szenario zugrunde: An einem Tag gingen gehäuft Schadensmeldungen beim LKA und der ZAC ein, dass Unternehmenssysteme bundesweit in kürzester Zeit komplett verschlüsselt und arbeitsunfähig waren. Die ZAC NRW übernahm das Verfahren und begann am Folgetag mit operativen Maßnahmen wie der Beschlagnahme von Servern und E-Mail-Accounts. Von diesem weltweiten Angriff war in Deutschland lediglich eine kleinere Anzahl an Firmen betroffen. Die meisten und ersten Schadensfälle waren in der Ukraine zu vermelden. Nationale und internationale Ermittlungen ergaben, dass die Kompromittierungen ihren Ursprung in der Ukraine hatten. Ein Softwareprodukt, das im Unternehmensbereich notwendig genutzt wird, wurde durch die Täter manipuliert. Anstelle regulärer Updates wurde über die digitale Versorgungskette ein Verschlüsselungstrojaner eingeschleust. Die internationalen Ermittlungen dauern derzeit noch an. Bemerkenswert bei derartigen Supply-Chain-Angriffen ist, dass es auf Grund der Kompromittierung der unmittelbaren digitalen Versorgungskette nahezu unmöglich ist, wirksame Prävention zu betreiben.

d) Drittstaatlich induzierte Kriminalität, Wirtschaft und kritische Infrastrukturen

Der Hackerangriff „NotPetya" als Supply-Chain-Attack war nicht das Ende der Entwicklung. Zuletzt gab es beispielsweise einen IT-Angriff auf die Systeme der Düsseldorfer Uniklinik, bei dem in Rede stand, dass eine Person auf Grund ausgefallener Operationstermine gestorben sei. Solche Angriffe auf kritische Infrastrukturen oder Wirtschaftsangriffe stellen die Strafverfolger vor neue Herausforderungen bei der Verfahrensführung. Täterkreis dieses Bereichs sind meist organisierte Strukturen, die teilweise an der Schwelle zu einem dritten Staat oder einer staatlichen Organisation stehen. Neben den schnell zerstörenden Angriffen wie „NotPetya" sehen sich die Strafverfolger in

diesem Feld mit Angriffen anderer Art wie den sog. APT-Angriffen (Advanced Persistent Threat) konfrontiert. Hierbei handelt es sich um die teils monatelange oder jahrelange Unterwanderung des IT-Systems eines Unternehmens durch Schadsoftware, um zielgerichtet Informationen von besonderem Informationsgehalt ausleiten zu können. In diesem Bereich war es für die Ermittler lange Zeit am schwersten, das Vertrauen der Unternehmen gewinnen zu können, um überhaupt strafverfolgend tätig zu werden. In den letzten Jahren ist dies zunehmend besser gelungen. Der Fokus der Ermittler liegt auf der Identifizierung von Angriffswegen und der Qualität des Angriffs, um hieraus Rückschlüsse auf die Täter ziehen zu können.

e) Die sonstigen Felder

Weitere Tätigkeitsfelder der ZAC bestehen zum einen in der Bekämpfung des Darknet-Handels. Zum anderen betreibt die Zentralstelle seit mehreren Jahren ein Projekt gegen Hate-Speech. Es besteht eine enge Kooperation mit der Presse und den digitalen Medien, die eine schnelle Stellung von Anzeigen und Ermittlungen ermöglicht. Außerdem verfügt die ZAC über eine Task-Force zur Bekämpfung des sexuellen Missbrauchs und der Kinderpornografie in den digitalen Medien. Hier wurde im letzten Jahr die lang bestehende Hypothese widerlegt, dass der Kernbereich dieses Deliktsfeldes im Darknet und in geschlossenen Kreisen stattfindet. Vielmehr fanden die Ermittler massenhaft Spuren im Clearnet, in digitalen Medien und in Social Media. In diesem Kampf gegen Massendelinquenz dient bislang die digitale Anonymität als Schutzmantel. Ein Instrument wie die Vorratsdatenspeicherung würde den Ermittlern ihre Arbeit erleichtern, zumindest einen Teil der Masse dieser Täter überführen zu können. Zwar wird der Kampf von den Ermittlern derzeit relativ erfolgreich geführt, jedoch ist es ein schwieriger und aufwendiger, der die Abwägung zwischen Datenschutz und Kriminalitätsbekämpfung hinterfragen lässt.

3. Q&A-Session

In der sich dem Vortrag anschließenden Q&A-Session wurden zukünftige Cybercrime-Bedrohungen für Unternehmen erörtert. Eine Vorhersage der zukünftigen Cybercrime-Szenarien ist ebenso wenig möglich wie ein gänzlicher Schutz vor Angriffen. Empfehlenswert ist allerdings in jedem Fall die Schulung von Mitarbeitern, um das Risiko gängiger Angriffsverfahren zu minimieren. Häufig sitzt die größte Sicherheitslücke vor dem Computer. Darüber hinaus wurde debattiert, wie eine Vorratsdatenspeicherung im deutschen Recht im Hinblick darauf geregelt werden könnte, dass der EuGH die anlasslose Vorratsdatenspeicherung als mit europäischen Grundrechten nicht vereinbar erklärt und Einschränkungen gefordert hat. In diesem Zusammenhang wurde auch festgestellt, dass eine Harmonisierung der derzeit sehr unterschiedlichen Standards auf europäischer Ebene sinnvoll wäre. Thematisiert wurden zudem die neu eingeführten Ermittlungsbefugnisse zur Bekämpfung von Kinderpornographie nach § 110d StPO i.V.m. § 184b Abs. 5 S. 2 StGB, deren praktische Möglichkeiten derzeit noch ausgelotet werden.

IV. Problematische Standards digitaler Forensik und Dringlichkeit der Cyber-Strafverteidigung (RA *Dr. Uwe Ewald,* Berlin)

Nach Einblicken in das Tätigkeitsfeld der Strafverfolgung präsentierte RA *Dr. Uwe Ewald* aus Berlin seine Perspektive auf den Problemkreis „justizieller Umgang mit Cybercrime“. In seinem Vortrag stellte er die derzeit bestehenden Probleme bei der Cyber-Strafverteidigung vor und bot zugleich verschiedene Lösungsansätze an.

1. Kontext Digitalisierung und Strafverteidigung

Der Darstellung von Problemen und Lösungsvorschlägen im Rahmen von Cyber-Strafverteidigung wurden einige allgemeine Ausführungen zum Kontext von Digitalisierung und Strafverteidigung vorangestellt.

a) Kriminologisch-analytische Perspektive mit juristischer Referenz

Damit der Übergang von der analogen zur digitalen Informationsverarbeitung im Strafverfahren gelingt, muss das Erkenntnisverfahren als analytischer Informationsverarbeitungsprozess verstanden werden. Dies ist ein anderer Zugang als die rein juristische Perspektive. Aus diesem Grund bezieht der Vortrag eine kriminologisch-analytische Perspektive mit juristischer Referenz und keine juristisch-normative Perspektive. Am Ende des Erkenntnisverfahrens steht stets das normative Konstrukt, das Verbrechen. Auf dem Weg dorthin werden Beweismittel wie Zeugen, Experten, Sachverständige und Dokumente, aber auch die digitalen Beweismittel, in einem Diskurs der Strafjuristen als beweisrelevante Informationen verarbeitet. Der entscheidende Unterschied zwischen der bisherigen, traditionellen analogen Informationsverarbeitung und der Verarbeitung von digitalen Beweismitteln besteht darin, dass der Vorgang der Transformation von Daten in die juristische oder prozessuale Wahrheit hinsichtlich der digitalen Beweise anders nachzuprüfen und nachzuvollziehen ist als bei analogen Beweismitteln, bei denen eine sinnliche Wahrnehmung möglich ist. Die Auswertung digitaler Informationen als Beweise erfordert die Anwendung von Hard- und Software, eine Fähigkeit, die von Strafjuristen neu erlernt werden muss. In gewisser Weise geht es um eine neue Art von Lesen und Schreiben in der juristischen Arbeit. Bislang ist diese Herausforderung im Alltag der Strafverfahren kaum bewältigt, und der „digital gap“ in der Strafjustiz ist nicht zu übersehen. Es geht darum zu vermeiden, dass am Ende nicht einige Beteiligte am Strafverfahren – zugespitzt formuliert - mit Keilschrift agieren, während die anderen Hochleistungscomputer verwenden.

b) Ansichten zum Verhältnis von digitalen Beweisen und Strafverteidigung

Ewald geht dann auf Ansichten verschiedener Berufsgruppen zum Thema Digitalisierung und Strafverfahren ein. Auf den großen Konferenzen der **IT-Forensik**, wie der GPEC (General Police Equipment Exhibition & Con-

ference), der DIC (Digital Investigation Conference) sowie dem Europäischen Polizeikongress lassen sich folgende zentrale Positionen feststellen: Der Schwerpunkt der Beweise verschiebt sich von Zeugen und Dokumenten hin zu digitalen Beweisen, die Verarbeitung digitaler Beweise ist Expertensache und es besteht ein distanziertes Verhältnis zur Kompetenzerweiterung für die Strafverteidigung. Dies stellt ein Problem dar, da die Lösung ein interdisziplinäres Zusammenarbeiten erfordert. Es ist zu erwarten, dass eine rasante technische und wirtschaftliche Entwicklung im Bereich der forensischen Informationsverarbeitung und so der digitalen Beweise auf uns zukommt und die Zeit drängt, um sich aus juristischer Sicht klar zu werden, wie digitale Beweise für ein verlässliches Verfahren so behandelt werden, dass die Unabhängigkeit der Strafgerichte und die Grundsätze eines fairen Verfahrens gewahrt bleiben.

Die Ansicht der **Strafjustiz und Gesetzgebung** im Hinblick auf das Verhältnis von digitalen Beweisen und Strafverteidigung ist ebenfalls sehr interessant. Die Formulierung des Veranstalters, *Professor Safferling*, „Sensibilität in Gerichts- und Plenarsälen ist noch nicht besonders ausgeprägt", ist noch freundlich. Es ist beispielsweise seit Jahren bekannt, dass die Strafverteidiger ein Problem haben, die Kompetenz im Umgang mit digitalen Beweismitteln zu entwickeln und die hierfür aufgewendete Zeit vergütet zu bekommen. Trotz der jahrelangen Bekanntheit dieses Problems hat es in den Vorbereitungsrunden des RVG-Referentenentwurfs keine Rolle gespielt. Auch ist der ministeriale Umgang mit IT-Forensik-Wirtschaft zu kritisieren. Beim Kauf von IT-Forensik-Software bestimmen die Käufer – also die Strafermittler bzw. das Innenministerium – wie und wo die Tools eingesetzt werden sollen. Einstiegsvoraussetzung für den Einkauf solcher Software müsste es sein, dass auch für die Verteidigung kosten- bzw. lizenzfreie Tools geliefert werden, damit diese nicht abgehängt wird.

Gewisse Tendenzen zum **Selbstbild der Strafverteidiger** zeigen eigene Umfragen *Ewalds* im Rahmen seiner Seminare. Strafverteidiger haben ein eher ambivalentes Verhältnis zur Digitalisierung und dem eigenständigen Umgang mit digitalen Beweisen. Die Masse der Strafverteidiger erwirbt in diesem Bereich nicht selbst aktiv Kompetenzen. Dies wird auch an den Ausbildungskonzepten der Rechtsanwaltskammern deutlich, wo die Themen nicht systematisch, sondern eher zufällig und sporadisch vermittelt werden. Es ist zu hoffen, dass die „Digital Natives" unter den Strafverteidigern effektiver vorgehen und zukünftig mehr Interesse an den Themen zeigen werden. Die (nicht repräsentativen) Umfragen ergaben, dass derzeit nicht einmal 4 % der Verteidiger digitale Beweise eigenständig auswerten. Die größten Hindernisse für die „Waffengleichheit" der Strafverteidigung beim Umgang mit digitalen Beweismitteln im Strafverfahren sahen die Teilnehmenden insbesondere in der fehlenden Kompetenz in der Auswertung sowie in der unzureichenden Bezahlung.

c) Risiko-Effekte der Digitalisierung des Beweisverfahrens auf Strafverfahrensgrundsätze

Der sachgerechte Umgang mit digitalen Beweisen ist für die Wahrheitsfindung immens wichtig, da gewisse Risiko-Effekte der Digitalisierung auf die Strafverfahrensgrundsätze ausstrahlen. So ist in Bezug auf den Anklage- und Untersuchungsgrundsatz zu befürchten, dass die Abhängigkeit von digitalen Systemen in den Vorermittlungen steigen wird. Zudem besteht im Hinblick auf die freie richterliche Beweiswürdigung ein Risiko für die Unabhängigkeit und Eigenständigkeit, wenn Beweise nicht mehr richtig oder gar nicht verstanden werden. Bezüglich des Mündlichkeits- und des Öffentlichkeitsgrundsatzes stellt sich die Frage, was passiert, wenn Maschinensprache (der digitalen Beweise) in der juristischen Verarbeitung von Beweisen auf natürliche Sprache (des Strafverfahrens) trifft. Unter dem Stichwort „Unschuldsvermutung vs. Gefährderansatz", das insbesondere auch mit dem Einsatz von KI in der Verbrechensbekämpfung verbunden ist, kann das Risiko für das Prinzip der individuellen strafrechtlichen Verantwortlichkeit betrachtet werden. Überdies ist auch der Fair-Trial-Grundsatz bzw. die Waffengleichheit durch ein Risiko für die rechtstaatliche Balance zwischen den Verfahrensbeteiligten betroffen.

2. Lage der Dinge – beunruhigend problematisch

Inzwischen gibt es eine Reihe beunruhigender Vorfälle im Umgang mit digitalen Beweisen, die auch mit Blick auf das Versagen der Strafverteidigung diskutiert werden. International bekannt wurde der sog. dänische Funkzellen-Daten-Skandal, der die Frage nach der Glaubwürdigkeit von Funkzellen-Daten aufwarf. Bei der Transformation der Funkzellen-Daten der Provider auf polizeiliche Systeme kam es zu Verfälschungen von Daten. Dies führte zur Überprüfung von 10.700 Urteilen in Dänemark und der Freilassung von 32 Gefangenen. Das Beispiel zeigt, welche fatalen Auswirkungen die „digitale Kluft" bei der Verarbeitung von elektronischen Beweismitteln in der Strafjustiz haben kann, wenn die juristischen Entscheidungspersonen die digitalen Beweise nicht verstehen. Eine jüngste Auswertung dieses Vorfalls erfolgte in "The use of historical call data records as evidence in the criminal justice system - lessons learned from the Danish telecom scandal" von *Lene Wacher Lentz* und *Nina Sunde.*[3]

Ein zweiter herausragender Skandal ereignete sich in Großbritannien. Eine Besonderheit dieses Falles liegt darin, dass er im Bereich der „private prosecutions" und nicht der ordinären Strafverfolgung verortet ist. Zwischen den Jahren 2000-2019 wurden sog. Sub-Postmaster der britischen Post beschuldigt, Geld unterschlagen zu haben.

[3] *Wacher-Lentz/Sunde*, The use of historical call data records as evidence in the criminal justice system - lessons learned from the Danish telecom scandal, abrufbar unter: https://www.researchgate.net/publication/346025404 (zuletzt abgerufen am 20.1.2021).

Es ging um hunderte von Fällen und – am Ende infolge Justizversagens – zerstörte Existenzen. Bei einer späteren Untersuchung durch die CCRC (criminal cases review commission) wurden massive Fehlurteile festgestellt. Grund waren ungeprüfte digitale Beweise aus dem komplexen Computersystem namens „Horizon". Lesenswert zu diesem Thema ist der Artikel „The harm that judges do – misunderstanding computer evidence: Mr Castleton's story" von *Paul Marshall*[4] sowie „Written evidence" von *Stephen Mason*.[5] Letzterer liefert eine gute Übersicht zu den kritischen Punkten, durch die es zu der Situation in Großbritannien gekommen ist und die sich teilweise auch auf Deutschland übertragen lassen. Ein Problem liegt in der grundlegenden Neigung von Juristen, die Zuverlässigkeit von Computern und Programmen anzunehmen. Der Fall macht auch das Versagen der juristischen Profession mit Blick auf die eigene Fort- und Weiterbildung überdeutlich. Des Weiteren bedarf es auch in Bezug auf die Akteneinsicht übergreifender Regeln, weil die Gerichte in den einzelnen Ländern ihre Abläufe diesbezüglich derzeit sehr unterschiedlich gestalten. Aktuell sind wir auch in Deutschland noch ein Stück weit davon entfernt, zuverlässige Methoden der Verarbeitung digitaler Beweise anzuwenden. Doch wie ist nun weiter zu verfahren? Zwei Grundthesen sollen eine Lösungsperspektive bieten.

3. Teil 1 der Lösung: IT-forensische Standards

Die erste Grundthese ist folgende: *IT-forensische Standards bei der Produktion digitaler Beweise und deren unabhängige juristische Überprüfbarkeit durch die am Strafverfahren beteiligten Strafjuristen bannen das Digitalisierungsrisiko für die Justiz.* Auf europäischer Ebene laufen bereits Projekte, die sich mit der Frage beschäftigen, mit welchen Standards, Methoden und in welchen Prozessformen digitale Beweise erzeugt, bearbeitet und ausgetauscht werden sollten. Vier der führenden Projekte sind: eEvidence, meCodex, LOCARD und FORMOBILE. Als Mitglied des Ethics Advisory Boards hat *Ewald* einen direkten Einblick in das Projekt „FORMOBILE". Dieses Horizon 2020 Projekt wurde ins Leben gerufen, um neue Standards für die Verarbeitung von Mobiltelefondaten zu erarbeiten. Ziel ist es, diese Standards als ISO-Standards zu etablieren und damit eine umfassende Rückwirkung auf deren IT-forensische Umsetzung in den nationalen Strafverfahren zu erreichen. Die Standards stellen zugleich einen gewissen Leitfaden für Strafverteidiger dar, im Verfahren Fragen zu entwickeln, die auf die Überprüfung ihrer Einhaltung gerichtet sind. Geschaffen werden müssen Standards auf verschiedensten Ebenen wie etwa Ausbildungsstandards, Standards für Software-Tools (Auswahlkriterien, Test und Validierungssystem), analytisch-methodische Standards sowie ethisch-rechtliche Standards (z.B. Schutz des persönlichen Kernbereichs und Schutz von Vertrauensbeziehungen). Auch für die allgemeinen strafprozessuale Prinzipien (Unparteilichkeit, Nachprüfbarkeit, Wiederholbarkeit, Reproduzierbarkeit, Erforderlichkeit, Verwahrkette, Analyse-Standards, Standards für die Archivierung und Reports) gibt es derzeit kein einheitliches Format, das von den Forensikern beherzigt wird, um Routinen einüben zu können. Ähnlich wie in der empirischen Sozialforschung, müsste es auch hier eine klare Schrittfolge geben. Häufig sind die technischen Zusammenhänge zu komplex, um wiederum von Juristen verstanden zu werden. Aus diesem Grund bräuchte es forensisch-juristische Standards in einer Metasprache, die eine unabhängige (!) juristische Überprüfung digitaler Beweise durch Strafjuristen ermöglicht – vergleichbar der Flug-Check-Liste für Piloten, die – obwohl nicht im Besitz des Ingenieurswissens der Flugzeugbauer – eine mit den technischen Experten gemeinsam entwickelte Checkliste erhalten, anhand derer der Pilot eine Prüfung der Zuverlässigkeit des Fluggerätes unabhängig und eigenständig durchführen kann.

4. Teil 2 der Lösung: Unabhängige juristische Prüfung und Strafverteidigung

Die Entwicklung rein forensischer Standards ist also nicht ausreichend, vielmehr muss die Unabhängigkeit und Eigenständigkeit der Strafjustiz durch eine eigenständige juristische Prüfung der Zuverlässigkeit von digitalen Beweisen gewahrt werden. Dies ist mit den bisherigen Verfahrenswegen und Standards nicht möglich. Deshalb bedarf es juristischer Standards, die sich an die IT-Standards anschließen. Hierbei ist auch auf die besondere Rolle der Strafverteidigung einzugehen, die zur zweiten Grundthese führt: *Der Cyber-Strafverteidigung kommt wegen ihrer besonderen Stellung im Strafverfahren eine besondere Rolle bei der Überprüfung der Reliabilität und Validität sowie daraus folgender Einschätzung von Zuverlässigkeit und Beweiswert digitaler Beweise zu.* Sie ist die einzige Akteurin, die im parteilichen Interesse für den Angeklagten im legalen Rahmen am kompromisslosen Test der von der Anklage vorgebrachten digitalen Beweise interessiert ist. Diese besondere Rolle wird auch durch das Amtsermittlungsprinzip oder die Verpflichtung der Staatsanwaltschaft zur Objektivität nicht aufgehoben. Aus diesem Grund müssen die Kompetenzen der Verteidigung im Umgang mit digitalen Beweisen a) sowohl im Hinblick auf deren Überprüfung als auch b) in Bezug auf eine eigenständige Auswertung erweitert werden.

Im Rahmen des vorgestellten dänischen Funkzellen-Daten-Skandals wurden vier Aspekte aufgestellt, die dem Problembewusstsein der Juristen im Umgang mit solchen Daten dienen sollten. Erstens, es ist wichtig, das ursprüngliche Anwendungsszenario der dann als (potenzielle) Beweismittel verwendeten digitalen Daten und Informationen zu verstehen. Viele digitalen Daten sind nicht im Zuge der Strafverfolgung, sondern für ganz andere Zwecke erstellt worden. Diese Zwecke muss man begreifen, um potenziell zu erfassen, wo kritische Bereiche in diesen Daten und bei ihrer Verarbeitung entstehen könnten. Man kann nicht von vornherein davon ausgehen, dass diese Daten

[4] *Marshall*, Digital Evidence and Electronic Signature Law Review, 17 (2020), p. 25-48.

[5] *Mason*, Response to the Justice Committee call for evidence regarding private prosecutions and safeguards, abrufbar unter: https://committees.parliament.uk/writtenevidence/7839/pdf/ (zuletzt abgerufen am 20.1.2021)

„automatisch" zuverlässig sind, wenn es um Belange der Strafverfolgung geht. Zweitens, die potenziell kritischen Bereiche sollten dann anhand einer Liste bekannter Risiken, die von den IT-Forensikern mitgeteilt werden, verständlich gemacht werden. Schwachstellen sind in der Regel bekannt, wie die Softwarefirma für die Auswertung von Funkzellendaten „CellHawk" in einem Online-Vortrag über „6 Dinge die Staatsanwälte über Funkzellendaten wissen sollten" zu erkennen gibt. Drittens müssen Zuverlässigkeitskriterien für die juristische Prüfung und viertens rechtliche Konsequenzen bei Nichteinhaltung der Standards festgelegt werden. Hier ist eine rote Linie in der Gestalt erforderlich, dass ein Beweismittel als unzulässig zu gelten hat, wenn die Zuverlässigkeit der Auswertungsmethode nicht dargestellt wird. Eine Entwicklung technischer Standards und ihre „Übersetzung" in Checklisten für die gerichtliche Überprüfung erfordert eine gemeinsame interdisziplinäre Anstrengung von IT-Forensikexperten und Juristen. Es bedarf einer historisch neuen Metasprache für IT-forensisch-juristische Standards, bei denen Maschinensprache und natürliche Sprache aufeinandertreffen. Das FORMOBILE-Projekt ist die erste übergreifende Initiative, die einen systematischen interdisziplinären Ansatz verfolgt, in dessen Ergebnis der Ansatz für eine solche Checkliste erarbeitet werden soll. Hierzu müssen zunächst die Richtlinien und Standards für die polizeiliche IT-forensischen Ermittlungen allgemeinverständlich für Strafjuristen „übersetzt" werden. Fallbezogen sollte dann entlang dieser Leitlinien protokolliert werden, an welchen Stellen bestimmte Risiken auftreten konnten und wie diesen Risiken methodisch begegnet wurde. Außerdem müssen Ermittler, Staatsanwaltschaft, Gericht und Verteidigung zu diesen sich ständig entwickelnden Standards und ihrer Anwendung kontinuierlich geschult werden.

5. Q&A-Session

In der sich dem Vortrag anschließenden Q&A-Session wurde insbesondere der Umstand thematisiert, dass die Gewinnung digitalforensischer Daten häufig aufwendig ist und intransparente Tools verwendet werden. Hierdurch stellt sich die Frage, ob ein IT-fachfremder Richter dieses Problem und die Wertigkeit von Beweismitteln überhaupt plausibilisieren kann. Bereiche, die eine extreme technische Perspektive erfordern, bei denen die Juristen an ihre Grenzen kommen, werden sich wohl nicht vermeiden lassen. Allerdings betreffen diese zum einen nicht die Masse der Verfahren. Zum anderen muss auch in diesen Situationen den Juristen immer dabei geholfen werden, einschätzen zu können, ob die Arbeit des IT-Sachverständigen methodisch sauber durchgeführt wurde. Ein Urteilsvermögen des Richters muss immer hergestellt werden, sodass dieser nicht wie im dänischen Funkzellen-Daten-Skandal zum Statisten wird.

V. Schlusswort und Fazit

Die Vorträge und Diskussionsbeiträge des EC²CT 2020 machten deutlich, dass Cybercrime und IT-Forensik bei weitem keine Nischenthemen mehr sind, sondern in Wissenschaft und Praxis eine stetig größer werdende Bedeutung für (fast) alle Verfahrensbeteiligten aufweisen. Vor diesem Hintergrund ist es notwendig, IT-forensische Standards für die polizeiliche, staatsanwaltschaftliche und gerichtliche Praxis zu entwickeln und zu etablieren. Hierfür ist eine Vernetzung von Wissenschaft, Strafverfolgung, Strafverteidigung und Gesetzgebung notwendig. *Professor Safferling* und das ICLU-Team freuen sich, mit dem Erlanger Cybercrime Tag einen Beitrag zur Schaffung und Stärkung eines Netzwerks zwischen den verschiedenen Bereichen zu leisten und eine Möglichkeit für die Diskussion und den Austausch zu schaffen. Die interdisziplinäre Veranstaltungsreihe wird im Herbst 2021 fortgesetzt – ob in Präsenzform oder im virtuellen Raum, ist noch offen.