TAGUNGSBERICHT

Erlanger Cyber² Crime Tag 2021: Internationale Strafverfolgung von Cybercrime Delikten

*von Dr. Christian Rückert und Nicole Scheler**

Der Tagungsbericht enthält sprachlich bereinigte und teils vom Englischen ins Deutsche übersetzte Zusammenfassungen der Transkriptionen der Vorträge und Diskussionsbeiträge des Erlanger Cyber² Crime Tages 2021. Der Vortragsstil der einzelnen Beiträge wurde überwiegend beibehalten. Dementsprechend wurde generell auch auf Fußnoten verzichtet. Der Erlanger Cyber² Crime Tag 2021 und die Erstellung dieses Tagungsberichts wurden vom Bundesministerium des Innern und für Heimat gefördert.

Im Anschluss an die erste erfolgreiche Online-Veranstaltung im Jahr 2020 aus der Veranstaltungsreihe des Erlanger Cybercrime Tages, fand am 23.9.2021 der fünfte Erlanger Cyber² Crime Tag 2021 (EC²CT 2021) im virtuellen Format statt, in diesem Jahr auch mit zahlreichen Teilnehmer:innen aus dem Ausland. Grußworte kamen in diesem Jahr vom bayerischen Staatsminister der Justiz, *Georg Eisenreich*, der sich live aus der Schlossaula auf die heimischen Bildschirme schaltete. Mithilfe einer intuitiv bedienbaren und vielseitigen Tagungsplattform konnten *Prof. Dr. Christoph Safferling*, LL.M. (LSE) und sein Team der International Criminal Law Research Unit (ICLU) den Besucher:innen auch dieses Jahr wieder die Möglichkeit bieten, während der Q&A-Sessions im Anschluss an die Vorträge Fragen an die Referierenden zu stellen, in den Workshop-Räumen interaktiv mit diesen zu diskutieren und sich auch jederzeit untereinander auszutauschen.

Mit dem Thema „Internationale Strafverfolgung von Cybercrime Delikten“ widmete sich der vom Bundesinnenministerium geförderte EC²CT 2021 den schwierigen Fragen des nationalen und internationalen Rechts, die damit einhergehen und die es zu lösen gilt: Angefangen bei nationalen Vorschriften in Bezug auf grenzüberschreitende Sachverhalte, die Zusammenarbeit der verschiedenen ermittelnden nationalen und internationalen Strafverfolgungsbehörden untereinander und mit privaten Dienstleistenden, den bereits bestehenden und geplanten internationalen Abkommen, eine effektive internationale Strafverteidigung und der Grund- und Menschenrechtsschutz der weltweit von Ermittlungsmaßnahmen betroffenen Personen.

Bereits in der Begrüßungsrede des Veranstalters, *Prof. Dr. Christoph Safferling*, LL.M (LSE), wurde die Notwendigkeit transnationaler Zusammenarbeit im Bereich der Strafverfolgung von Cybercrime deutlich. Nach Art. 6 EMRK (der Beschleunigungsmaxime) hat jeder Mensch das Recht, dass in Bezug auf die gegen ihn erhobene Anklage innerhalb einer angemessenen Frist verhandelt wird. Der *Europäische Gerichtshof für Menschenrechte* hat etwa 30 % seiner Beanstandungen auf diese Vorschrift gestützt. Auch deutsche Gerichtsverfahren waren häufig betroffen: Von den 199 Verurteilungen, die seit 1959 gegen Deutschland ergangen sind, sind 102 auf Verfahrenslänge zurückzuführen (51 %). Die Verfahrenslänge in erstinstanzlichen Strafverfahren nimmt dabei immer weiter zu. Mittlerweile beträgt die durchschnittliche Verfahrenslänge 8 Monate, an Landgerichten sogar bis zu 20 Monate. Das liegt zunächst an den immer größer werdenden Datenmengen und an dem zunehmenden Auslandsbezug der Verfahren.[1] Eben diesen Auslandsbezug im Bereich der Cyberkriminalität und die damit einhergehenden Herausforderungen thematisierte der diesjährige EC²CT 2021.

I. International Darknet Investigations – Dark Web Monitor (englischer Vortrag ins Deutsche übersetzt) von *Dr. Mark van Staalduinen* (CFLW Cyber Strategies) und OStA *Thomas Goger* (ZCB)

Eröffnet wird die Vortragsrunde von *Dr. Mark van Staalduinen* und OStA *Thomas Goger*. Sie präsentieren den „Dark Web Monitor“[2] – eine Technologie, die Strafverfolgungsbehörden bei der täglichen Arbeit von Darknet-Ermittlungen unterstützen soll.

Die Idee, das Projekt des „Dark Web Monitors“ weiterzuentwickeln und auf die Bedarfe von Strafverfolgungsbehörden anzupassen, entstand durch eine Kollaboration der beiden Referenten und wurde seit Ende 2019 von TNO (einer niederländische Forschungsorganisation), CFLW Cyber Strategies (unter der Leitung von *Mark Staalduinen*) und der ZCB (stellvertretend durch *Thomas Goger*) geplant und umgesetzt.

* *Dr. Christian Rückert* ist Habilitand an der Friedrich-Alexander-Universität Erlangen-Nürnberg und Lehrstuhlvertreter an der Universität Mannheim; *Nicole Scheler* ist wissenschaftliche Mitarbeiterin an der Friedrich-Alexander-Universität Erlangen-Nürnberg.

1 https://www.drb.de/newsroom/presse-mediencenter/nachrichten-auf-einen-blick/nachricht/news/strafjustiz-am-limit-1 (zuletzt abgerufen am 12.5.2022).

2 https://cflw.com/dwm/

1. Ziel der Tool-Entwickler:innen

Ziel war es, ein Tool zu entwickeln, das die tägliche Arbeit von Strafverfolger:innen bei den schwierigen Ermittlungen im Darknet erleichtert. Strafverfolgungsbehörden und Geheimdienstorganisationen sind vor die große Herausforderung gestellt, die sich ständig ändernden Muster und Phänomene im (verschlüsselten) Dark Web im Blick zu behalten, um beurteilen zu können, welches Verhalten strafrechtlich relevant ist, welche neuen Technologien sich entwickeln, welche Dienste auf welchen Servern angeboten werden und welche neuen Untergrundorganisationen sich bilden. Da die Vorgehensweisen immer raffinierter werden, besteht ein großer Bedarf an verbesserten Überwachungsfunktionen für das Dark Web, um einen Vorteil gegenüber den Kriminellen zu erlangen. Der „Dark Web Monitor" unterstützt Organisationen in den Bereichen Strafverfolgung, Cybersicherheit und Finanzwesen bei verdächtigen Aktivitäten und ermöglicht es ihnen, verdächtige Infrastrukturen durch den Einsatz von Crawling-Mechanismen und fortschrittlicher Analysemethoden aufzuspüren und digitale Spuren zu untersuchen, um sie zu unterbrechen und zu verfolgen.

2. Anforderungen und Code of Conduct

Ein sehr wichtiges Anliegen der Beteiligten war es nicht nur die technischen Features an die Suchmaschine zu formulieren oder die Ausgabe des Datensatzes zu verbessern, sondern auch sog. nichtfunktionale Anforderungen aufzustellen, um die geltenden Rechtsrahmen einzuhalten. Es soll Transparenz geschaffen werden: Wer nutzt das Tool, wie werden die Datensätze verarbeitet und wie wird der Datenschutz umgesetzt? Neben den datenschutz- und anderen rechtlichen Anforderungen war und ist es ein wichtiges Ziel, bei der Entwicklung des Tools forensische Standards einzuhalten, d.h. Ergebnisse zu produzieren, die sowohl transparent als auch nachvollziehbar sind.

Für all diese Anforderungen und Fragen haben die Entwickler:innen einen Code of Conduct verfasst, der auch ständig aktualisiert und angepasst wird. So wollen die Entwickler:innen nicht zuletzt sicherstellen, dass das Tool in einem offenen und vertrauenswürdigen Umgang angewendet wird. Es soll klar sein, wer hinter dem Tool steht, wer es verwendet, wie es funktioniert und wie es angewendet werden soll.

3. Der „Dark Web Monitor" in der Anwendung

Anschließend führen die Referenten das Publikum durch die Anwendung des Tools und präsentieren erste gewonnene Erkenntnisse mithilfe des „Dark Web Monitors".

2013, als der erste Darkweb-Crawler entwickelt wurde, wurde bereits die Überwachung einer einzigen .onion-Adresse als Erfolg gefeiert. Allerdings ist es häufig so, dass die meisten .onion-Seiten nicht lange online sind und nach wenigen Wochen offline gehen. Manchmal schalten sie sich nach einiger Zeit wieder an, manchmal aber auch nicht („dynamisches Ökosystem"). Deshalb wurde schnell klar, dass es Ziel sein muss, so viele .onion-Adressen wie möglich zu überwachen. Mit dem „Dark Web Monitor" werden derzeit rund eine Million .onion-Adressen überwacht (wovon ca. 120.000 Seiten aktiv sind) und es war eine große Herausforderung, dabei einen guten Überblick zu bekommen und zu behalten.

Bei der Anwendung des „Dark Web Monitors" wird versucht, jede .onion-Adresse zu klassifizieren, um zu verstehen, ob und welches strafrechtlich relevante Verhalten auf der Seite beobachtet werden kann, bspw. welcher Service dort angeboten wird. Außerdem werden die jeweiligen Adressen dokumentiert und gespeichert: Die Links und Namen werden in der Datenbank hinterlegt, Screenshots der Seite und Angebote bewahrt und zudem bestimmte „Tags" vermerkt (z.B. „Ransomware"). Hinter der Datenerhebung und -sammlung steht eine durchdachte und ständig weiterentwickelte Taxonomie. Die gesammelten Inhalte können dann in einer übersichtlichen Ausgabemaske angezeigt und mit verschiedenen Filterfunktionen selektiert werden. Wenn man also Ermittlungen im Bereich „Ransomware" tätigt, kann man sich so alle Adressen anzeigen lassen, die mit „Ransomware" getaggt wurden – also bspw. welche Seiten mutmaßlich mit Ransomware handeln, welche Art von Daten bereits veröffentlicht wurden mittels Ransomware-Angriffen oder um einen Überblick zu bekommen welche Arten an Ransomware derzeit im Umlauf sind.

Mark van Staalduinen zeigte auch einige Beispiele und Details des Tools. So führt er die Zuschauer:innen über verschiedene Links der Ausgabemaske, zu Screenshots der verschiedenen Seiten, die der Dark Web Monitor derzeit überwacht. Einige dieser Seiten werben mit Geschäftsmodellen, die auf Schneeballsysteme schließen lassen. Andere Seiten bieten verschiedene Dienstleistungen (wie das Hacken von Paypal Accounts) und Produkte (wie Prepaidkarten, Drogen oder kinderpornografisches Material) an. Am Beispiel von „BITCARDS", die Prepaidkarten anbieten, hat *Dr. van Staalduinen* dem Publikum gezeigt, wie solche Seiten (typischerweise) aufgebaut sind und wie detailliert sie ihre Dienste und Produkte beschreiben.[3] Allein schon diese Darstellungen sind sehr wertvoll für die Strafverfolgungsbehörden, da sie viel über das Täterverhalten und den modus operandi verraten.

a) Der Dark Web Monitor als „Way-back-machine" für TOR

Zur Beobachtung des Status (online/offline) der .onion Seite (sehr dynamisches Ökosystem, vgl. oben), gibt es auch ein Feature, das alle 18 Stunden einen Zwischenstand der Seite speichert und dokumentiert. Er fertigt Screenshots an und greift alle erwähnten Kryptowährungsadressen, PGP-Keys oder E-Mail-Adressen auf. Vor allem für Darknet-Ermittlungen von Strafverfolgungsbehörden ist das eine sehr wertvolle Anwendung. Oft tauchen in einem Verfahren .onion Adressen auf, von denen 90 % zum Stand der Ermittlungen nicht mehr aktiv sind.

[3] Für mehr Informationen vgl. Tagungsbericht Erlanger Cybercrime Tag 2018: Darknet und Underground Economy: KriPoZ 2018, 247.

Bei diesen bestünde keine Möglichkeit mehr, auf die relevanten Inhalte zuzugreifen. Der Dark Web Monitor fungiert mithilfe des Zwischenspeichers jedoch als eine Art „Way-back-machine" für Tor, denn so können die Inhalte von inaktiven Seiten bis weit in die Vergangenheit zurück nachvollzogen werden.

Mithilfe dieser Funktion war es beispielsweise in einem Fall möglich, den Tatnachweis im Zusammenhang mit kinderpornografischen Schriften zu erbringen. Und das, obwohl der Angeklagte jegliche Vorwürfe abstritt, die im Speicher gefundenen Adressen lediglich zu .onion-Seiten führten, die bereits offline waren und ansonsten keine belastenden Beweise vorlagen. Dank der angefertigten Screenshots konnte nachvollzogen werden, was auf den ehemaligen .onion-Seiten gehostet wurde. Damit gelang die Führung des Tatnachweises und das Gericht konnte sich von der Schuld des Angeklagten überzeugen.

b) Verknüpfung von Duplikaten

Mithilfe der gesammelten Informationen über die verschiedenen .onion Seiten wird es auch möglich, „Duplikate" zu erkennen. Solche Duplikate sind nichts anderes als genau die gleichen Inhalte von denselben Urheber:innen – nur unter einer neuen Domain. Das wird häufig aus Gründen der Resilienz gemacht, um bei Angriffen oder technischen Störungen eine stabile und widerstandsfähige Infrastruktur zu gewährleisten. Durch die Verknüpfung dieser „zusammengehörenden Seiten" lassen sich Rückschlüsse auf die dahinterstehende Organisation bzw. Tatverdächtigen ziehen. Vor allem für Strafverfolgungsbehörden ist diese Übersicht sehr wertvoll, denn so erhöht man die Wahrscheinlichkeit, die gesamte Infrastruktur der strafrechtlich relevanten Inhalte vom Netz zu nehmen und nicht nur vereinzelte Seiten.

In diesem Zusammenhang berichtete *Thomas Goger* von der erfolgreichen Beschlagnahme von „Boys Town" durch die Frankfurter Strafverfolgungsbehörden. Der Erfolg bestand vor allem darin, dass es ihnen gelungen war, alle Seiten, die mit „BoysTown" im Zusammenhang standen, vom Netz zu nehmen. Zum Zeitpunkt der Beschlagnahme tauchte allerdings schon wieder eine neue Seite im Dark Web auf: „BoysTown2". Dieses Beispiel zeigt die Wichtigkeit des Features auf, sich die komplette Infrastruktur der im Zusammenhang stehenden Seiten anzeigen zu lassen und direkt sehen zu können, ob die Operation – alle verfahrensrelevanten Seiten offline zu nehmen – erfolgreich war bzw. welche neuen Duplikate im Dark Web gefunden werden konnten.

c) Verlinkungen der Onion Adressen untereinander

Ein anderes wertvolles Feature ist die Dokumentation darüber, welche Domains sich gegenseitig verlinken und empfehlen. Der Dark Web Monitor kann ein Ranking der meistverlinkten Seiten erstellen. So kann festgestellt werden, welche Seiten wahrscheinlich wichtiger bzw. prominenter sind als andere. Diese Differenzierung gibt Hinweise auf Ermittlungsansätze.

Im Fall von „Lenas Bioladen" konnten die Ermittler:innen sehen, wo dieser erwähnt bzw. empfohlen wurde, um sowohl einen Überblick über die Zusammenhänge und Infrastrukturen der verschiedenen .onion-Seiten zu bekommen, als auch Rückschlüsse auf die dahinterstehende Organisation ziehen zu können. So haben auch hier die erfolgreichen Ermittlungen zu einer Hauptverhandlung vor Gericht geführt.

d) Weitere Erkenntnisse durch die Anwendung des „Dark Web Monitors"

Erste Erkenntnisse der Anwendung des Tools weisen darauf hin, dass viele der Domains im Dark Web strafrechtlich relevanten Inhalt aufweisen. Ein Blick auf die ausgegebene Statistik zeigt, dass „Spitzenreiter" – nicht wie vermutet der Drogenhandel – sondern Dienstleistungen im Bereich der Finanzkriminalität sind. Schon allein diese Erkenntnis demonstriert, wie wichtig es ist, mit echten Datensätzen und Erkenntnissen der Forschung zu arbeiten und sich bei Ermittlungen nicht allein von Vermutungen leiten zu lassen.

Ein anderes Beispiel verdeutlicht, dass der Dark Web Monitor zwar nicht immer zu Ermittlungserfolgen verhelfen kann, aber in jedem Fall strategische Einblicke in das Dark Web bietet. Auf einer Seite wurden gefälschte bayerische Impfpässe angeboten. Die Ermittlungen waren allerdings recht schnell am Ende, weil die Seite direkt mit einem „Sicherstellungsbanner" (sog. Splashpage) versehen wurde, den sonst nur Strafverfolgungsbehörden für den Erfolg einer beschlagnahmten Seite verwenden. Die Ermittler:innen vermuten, dass das von der dahinterstehenden Organisation selbst vorgenommen wurde, um sich noch am Anfang der Ermittlungen schnell aus der Affäre zu ziehen, ohne Vertrauenswürdigkeit gegenüber der Kund:innen einbüßen zu müssen. So konnte der Dark Web Monitor also nicht dabei helfen Ermittlungen zum Erfolg zu verhelfen, allerdings machte er die Behörden auf neues Täterverhalten aufmerksam, das verhindert werden muss.

e) Anwendungen über das TOR Netz hinaus

Nachdem Strafverfolgungsbehörden schon einige Ermittlungserfolge im Bereich des TOR Netzes feiern konnten (Silk Road, Silk World 2, BoysTown, Hansamarket etc.), liegt die Annahme nicht fern, dass sich die Täter:innen nach anderen Darknet-Technologien umsehen wie bspw. i2P oder ZERONet. Wissenschaftler:innen überprüften das mithilfe des Dark Web Monitor und konnten zwar kriminelle Aktivitäten und Handelsplattformen feststellen, allerdings handelt es sich immer noch um eine Nische. Bisher kann (noch) nicht davon gesprochen werden, dass sich die kriminellen Verhaltensweisen vom TOR Netz auf i2p oder ZeroNet verlagern. Weiter gibt es Anhaltspunkte, dass die Täter:innen auf Messenger-Dienste wie Telegram ausweichen, um dort Deals abzuwickeln. Diese gewonnenen Erkenntnisse zeigen, dass die Anwendung des Darb Web Monitor nicht nur für spezifische Ermittlungen hilfreich ist, sondern eben auch um strategische Einblicke in das Dark Web als Ganzes zu bekommen.

3. Q&A-Session

In der sich dem Vortrag anschließenden Q&A-Session wurde insbesondere nochmals darauf eingegangen, dass es sich um öffentlich zugängliche Daten handelt, die vom Dark Web Monitor gesammelt werden (wie auf den Seiten verwendete E-Mail-Adressen und Bitcoin-Adressen). Diese bieten vor allem den Vorteil, dass sie verlinkt werden und Zusammenhänge und Infrastrukturen aufzeigen können. Die Erkenntnisse, die mithilfe des Dark Web Monitor erlangt werden, und als Beweis in die Hauptverhandlung eingeführt werden sollen (wie die Screenshots in dem Beispielfall) werden in den meisten Fällen durch Sachverständige eingebracht.

Dass andere Darknet-Technologien (noch) nicht wirklich genutzt werden, liegt vor allem daran, dass TOR im Vergleich zu alternativen Technologien sehr einfach zu bedienen ist. Was aber wohl nicht unterschätzt werden darf, ist die Verlagerung der kriminellen Geschäfte auf Messenger-Dienste wie Telegram.

Um zu verhindern, dass Kriminelle den Dark Web Monitor missbrauchen, haben die Entwickler:innen Sicherheitsmechanismen vorgesehen. So wird beispielsweise überprüft, welche E-Mail-Adresse angegeben wird, welcher Organisation man angehört und zu welchen Zwecken das Tool angewendet werden soll.

II. Kritische Reflexionen zur E-Evidence-VO und zur Reform der Europol-VO von Rechtsanwältin *Dr. Margarete Gräfin von Galen* (Galen Rechtsanwälte)

Bei beiden Verordnungskonzepten handelt es sich um Verordnungsvorschläge der europäischen Kommission, die sich noch im Gesetzgebungsverfahren befinden. In ihrem Vortrag konzentriert sich die Referentin vor allem auf das Thema des Zugriffs durch Strafverfolgungsbehörden auf Daten und Informationen, die bei Privaten gespeichert sind.

1. Reform der EEA durch die E-Evidence-Verordnung

Die aktuell geltende Rechtslage grenzüberschreitender Ermittlungen bestimmt sich nach der Europäischen Ermittlungsanordnung (EEA)[4]. Die Kommission sieht allerdings die Befugnisse und Möglichkeiten der EEA als nicht ausreichend an und will diese mit den beiden Verordnungsvorschlägen erweitern. Der Vorschlag der europäischen Kommission für eine Verordnung des europäischen Parlaments und des Rates über die europäische Herausgabeanordnung und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, sog. E-Evidence-VO, wurde 2018 eingeführt[5]. Zusammengefasst geht es inhaltlich darum, schnell und effektiv auf elektronische Beweismittel, die in der EU gespeichert sind (bei Privatpersonen, bei Dienstanbietenden sowie privaten Unternehmen), zugreifen zu können. Und das möglichst ohne Zwischenschaltung von Gerichten oder (weiteren) staatlichen Stellen.

a) Drei verschiedene Vorschläge und der Trilog

Neben dem Vorschlag der Kommission gibt es eine sog. Ausrichtung des Rates vom 30.11.2018[6] und den Bericht des europäischen Parlaments vom 11.12.2020[7]. Sie wandeln den ursprünglichen Vorschlag der Kommission an verschiedenen Stellen ab. Mit diesen drei Varianten hat am 10.2.2021 der Trilog zwischen Kommission, dem Rat und dem Parlament begonnen. Der Knackpunkt liegt wohl im Unterschied zwischen dem Rats- und dem Parlamentsvorschlag, bspw. die Frage, inwieweit der Vollstreckungsstaat (dort wo die Ermittlungsmaßnahme umgesetzt werden soll) eingebunden werden soll. Bevor es um die Differenzen zwischen dem Rats- und dem Parlaments-Entwurf gehen soll, führt die Referentin die Zuhörer:innen durch die grundlegenden Punkte der E-Evidence-VO.

b) Grundlegendes zur E-Evidence-VO

Die E-Evidence-VO kennt die Herausgabeanordnung und die Sicherungsanordnung. Die Herausgabeanordnung meint, dass der Mitgliedstaat A (Anordnungsstaat) für sein Ermittlungsverfahren notwendige elektronische Beweismittel aus dem Mitgliedstaat B (Vollstreckungsstaat) direkt von einem in B ansässigen privaten Diensteanbieter herausverlangen darf. Unterhalb der Herausgabeanordnung gibt es die Sicherungsanordnung. Sie betrifft die (vorläufige) Sicherung der Daten, um ihren Verlust zu vermeiden.

c) Einzelheiten des Vorschlags des Rates

Voraussetzung für eine Herausgabeanordnung ist, dass sie in einem vergleichbaren Fall auch im Vollstreckungsstaat zulässig wäre. Außerdem muss sie notwendig und verhältnismäßig sein. Ob diese Generalklausel in den Einzelfällen Anwendung findet, ist der Referentin zweifelhaft. Die betroffenen Personen, egal ob Beschuldigter oder Dritte, dürfen nicht informiert werden.

Der Vorschlag unterscheidet dabei zwischen Teilnehmerdaten (am eingriffsschwächsten), Zugangsdaten, Transaktionsdaten und Inhaltsdaten (am eingriffsintensivsten). Je nachdem um welche Daten es sich handelt, variieren auch die Voraussetzungen eines Herausgabeverlangens. Bei weniger sensiblen Daten (wie bspw. Teilnehmerdaten) ist eine behördliche Entscheidung, die von der Staatsanwaltschaft validiert wurde, ausreichend – bei sensibleren Daten (wie Inhaltsdaten) muss die Entscheidung gerichtlich

[4] Richtlinie 2014/41/EU Des Europäischen Parlaments und des Rates vom 3.4.2014 über die Europäische Ermittlungsanordnung in Strafsachen, online abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014L0041&from=DE (zuletzt abgerufen am 12.5.2022).

[5] Online abrufbar unter: https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0003.02/DOC_1&format=PDF (zuletzt abgerufen am 12.5.2022).

[6] Online abrufbar unter: https://db.eurocrim.org/db/de/doc/3117.pdf (zuletzt abgerufen am 12.5.2022).

[7] Online abrufbar unter: https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_DE.pdf (zuletzt abgerufen am 12.5.2022).

validiert sein. Der Entwurf sieht keine Möglichkeit vor, Graubereiche noch einmal überprüfen zu lassen.

Zu wenig behandelt wird auch das Thema der Herausgabe von „bevorrechtigten" Daten. Das sind solche Daten, die nicht aus dem Verfügungsbereich der berechtigten Person (Stichwort: Zeugnisverweigerungsrecht) oder des Staates (Stichwort: nationale Sicherheit) gelangen sollten. So findet beispielhaft überhaupt keine Kontrolle oder Differenzierung bezüglich der Datenkategorie statt, wenn die betroffene Person ihren Wohnsitz im Anordnungsstaat hat. Wenn die betroffene Person dagegen ihren Wohnsitz nicht im Anordnungsstaat hat, wird zunächst unterschieden zwischen Transaktions- und Inhaltsdaten und weiter wird bestimmt, wann die Anordnungsbehörde die Vollstreckungsbehörde kontaktieren muss. Wenn es sich um Transaktionsdaten handelt und die Anordnungsbehörde berechtigten Grund zur Annahme hat, dass entsprechende bevorrechtigte Daten darunter sind, kann sie zur weiteren Klärung Kontakt mit der Vollstreckungsbehörde aufnehmen. Ob aber die Staatsanwaltschaft des Anordnungsstaates, die schließlich ein sehr starkes Herausgabeinteresse an diesen Daten hat, bei Zweifeln tatsächlich Kontakt zur Vollstreckungsbehörde aufnimmt, geschweige denn ganz von einem Herausgabeverlangen absieht, ist höchst fraglich. Stellt sich schließlich heraus, dass es sich auch um bevorrechtigte Daten handelt, die herausgegeben werden sollen, richten sich die weiteren Schritte nach den Vorgaben des nationalen Rechts des Anordnungsstaates. Wenn die Daten beispielsweise im Vollstreckungsstaat bevorrechtigt wären, im Anordnungsstaat jedoch nicht, würde die Herausgabeanordnung trotzdem ergehen. Handelt es sich dagegen um Inhaltsdaten, wird die Vollstreckungsbehörde immer kontaktiert, egal ob die Anordnungsbehörde Bedenken bzgl. bevorrechtigter Daten hat oder nicht. Es ist dann Aufgabe der Vollstreckungsbehörde die Anordnungsbehörde gegebenenfalls über bevorrechtigte Daten zu unterrichten. Wie die Vollstreckungsbehörde allerdings an diese Informationen gelangen soll, ist auch noch weitestgehend ungeklärt. Sie kann sich zwar an den Dienstanbieter wenden, dieser ist aber nicht zur Auskunft verpflichtet.

Dass es keine „Rechtsbeziehung" zwischen Dienstanbietenden und der zuständigen Stelle im Vollstreckungsstaat gibt, stellt aus Sicht der Referentin ein weiteres Problem dar. Konsequenterweise gibt es auch keine offizielle Unterstützung für die Dienstanbieter durch die Vollstreckungsbehörde. Sie müssen als Adressaten selbstständig entscheiden, wie sie der Herausgabeanordnung nachkommen. D.h. sie müssen innerhalb einer sehr kurzen Frist (von 10 Tagen bis hin zu 6 Stunden) liefern oder im Ausnahmefall unverzüglich Informationen über Hindernisse mitteilen und die Daten sichern. Kommen die Dienstanbieter der Herausgabeanordnung nicht nach, drohen ihnen erhebliche Sanktionen (bis zu zwei Prozent des weltweiten Jahresumsatzes des Unternehmens). Weigern sich die Dienstanbieter, obwohl es keine Hinderungsgründe gibt, tritt die Vollstreckungsbehörde in Aktion und kann tatsächlich vollstrecken.

Dem geschuldet ist auch der Umstand, dass sich die anschließende Frage der Verwertung der (möglicherweise rechtswidrig) erlangten Daten erst verhältnismäßig spät in einem Strafverfahren ergibt – faktisch erst wenn diese schon in das Strafverfahren „geflossen" sind. Die Gefahr, dass ein Verwertungsverbot erst sehr spät geltend gemacht werden kann, wird noch deutlicher, wenn man sich vor Augen führt, dass die herausgegebenen Daten unter bestimmten Voraussetzungen auch in anderen Verfahren verwendet werden und an Mitgliedstaaten sowie an Drittstaaten weitergeleitet werden dürfen.

Auch sind die Rechtsbehelfe, die der Verordnungsentwurf vorsieht, sehr eingeschränkt: Dienstanbietern stehen keine Rechtsbehelfe im Vollstreckungsstaat zur Verfügung. Auch Dritte haben nur einen Rechtsbehelf vor dem Gericht des Anordnungsstaates. Nachdem diese aber nicht über die Maßnahmen informiert werden, bleibt offen, wie und wann sie diese überhaupt geltend machen können. Für die beschuldigte Person besteht die Möglichkeit, zu den üblichen nationalen Rechtsbehelfen während des Strafverfahrens zu greifen. Vor allem in diesem Zusammenhang wird die Gefahr deutlich, die mit der Zersplitterung in nationales Recht einhergeht. So kann es am Ende sein, dass es zwar ein einheitliches Instrument der Herausgabeanordnung gibt, aber gleichzeitig ein zersplittertes – also uneinheitliches – System der Rechtsbehelfe.

d) Einzelheiten des Entwurfs des europäischen Parlaments

Einen Punkt, den das Parlament eingefügt haben möchte, ist bspw., dass auch der Beschuldigte das Recht haben soll, eine europäische Herausgabeanordnung zu beantragen (Waffengleichheit). Auch will es andere Datenbegriffe und -kategorien verwenden, die dem europäischen Recht bereits bekannt sind: Teilnehmerdaten, Verkehrsdaten und Inhaltsdaten. Ganz allgemein zieht das Parlament klarere und höhere Hürden. Es konkretisiert u.a. den sehr offen gehaltenen Verhältnismäßigkeitsgrundsatz mit der Formulierung, dass ausreichend Grund zu der Annahme bestehen muss, dass eine Straftat begangen wurde, die schwerwiegend genug ist.

Ein weiterer wichtiger Unterschied besteht darin, dass die Person, deren Daten angefordert werden, informiert werden soll. Die herausgegebenen Daten sollen nur für das eigene Verfahren verwendet werden dürfen. Außerdem gibt es Regelungen zur Löschungspflicht. Daneben ist eine Regelung vorgesehen, dass rechtswidrig erlangte Informationen nicht vor Gericht verwendet werden dürfen, diese Entscheidung wird also nicht mehr dem nationalen Recht überlassen. Das Parlament hat außerdem von den schwerwiegenden Sanktionen gegen die Dienstanbieter Abstand genommen. Zuletzt soll es für alle Beteiligten Rechtsbehelfe vor den Gerichten sowohl des Anordnungs- als auch des Vollstreckungsstaates geben.

Eine wesentliche Änderung, die das Parlament vornehmen möchte, ist, dass jede Anordnung an den Dienstanbieter und an die Vollstreckungsbehörde gerichtet werden

muss. Dem Parlament ist wichtig, dass die Vollstreckungsbehörde in jedem Fall eingebunden wird und auch verschiedene Ablehnungsmöglichkeiten zur Verfügung hat.

2. Verordnungsvorschlag für eine Änderung von Europol

Die Tendenz, dass der Zugriff direkt auf Private erfolgen darf, setzt sich auch in den Änderungen der Europol-Verordnung fort.[8] Neben verschiedenen anderen Reformvorschlägen beziehen sich verschiedene Punkte nämlich auch auf die Zusammenarbeit von Europol und privaten Parteien. So heißt es in Art. 26 Abs. 2 des Verordnungsvorschlags zur Änderung der Verordnung (EU) 2016/794, dass Europol personenbezogene Daten direkt von Privaten entgegennehmen kann, um die betreffenden nationalen Ermittlungsbehörden (nach Abs. 1 lit. a) zu ermitteln.

Durch die unklare Formulierung liegt die Gefahr allerdings nicht fern, dass Europol darin eine Möglichkeit sieht und den Austausch von Daten eben nicht nur zur Feststellung der Zuständigkeit und Gerichtsbarkeit nutzt, sondern auch um Strafverfahren in den Mitgliedstaaten zu initiieren (was von Art. 88 AEUV nicht mehr gedeckt wäre). Ebenfalls kritisiert worden ist, dass damit ein großes Risiko geschaffen wird, dass bevorrechtigte Daten ausgehändigt und grundlegende gerichtliche Schutzmechanismen umgangen werden. Auch werden datenschutzrechtliche Vorgaben nicht eingehalten: Art. 6 DSGVO bietet aus Sicht der Referentin keine ausreichende Rechtsgrundlage für die Übermittlung von Daten durch Private an Europol. Deutschland hat in § 24 BDSG geregelt, dass eine Weitergabe möglich ist, wenn sie zur Strafverfolgung nötig ist. Nach Art. 26 des Verordnungsvorschlags ist der Datenaustausch allerdings nicht für die Strafverfolgung, sondern zur Feststellung der Zuständigkeiten gedacht. Wenn Private jetzt der Forderung von Europol nachkommen, allerdings ein Verstoß gegen die DSGVO vorliegt, drohen ihnen sehr hohe Strafen (bis zu 20 Mio. Euro oder 4% des weltweiten Jahresumsatzes).

3. Fazit

Ohne Frage ist die Forderung nach Beschleunigung der Ermittlungen von grenzüberschreitenden Sachverhalten gerechtfertigt. Dass sie allerdings sorgfältig unter Auslassung der rechtsstaatlich erforderlichen Garantien umgesetzt werden soll, erscheint der Referentin nicht gerechtfertigt. Die Referentin schlägt vor, mit der eingriffsschwächeren Sicherungsanordnungen zu agieren und die Schnelligkeit und Effektivität der internationalen Strafverfolgung mit Geld und Personal voranzutreiben. Die Lösung kann jedenfalls keine Verordnung sein, die Schutzmechanismen einfach ausblendet, weil sie das Verfahren verzögern würden.

III. Internationale Zusammenarbeit bei der Bekämpfung von Cybercrime – Täter, Partner und Vorgehensweisen vom Leitenden Kriminaldirektor *Heiko Löhr* (BKA)

Nach der Mittagspause ist der Leitende Kriminaldirektor *Heiko Löhr* vom BKA auf der virtuellen Hauptbühne zu sehen. Mit seinem Vortrag „Internationale Zusammenarbeit bei der Bekämpfung von Cybercrime – Täter, Partner und Vorgehensweise“ gibt er dem Publikum Einblicke in die aktuelle polizeiliche Arbeit.

1. Big Game Hunting und Ransomware

Ein maßgeblicher Punkt, der die aktuelle Lage im Bereich Cybercrime kennzeichnet, ist das „Big Game Hunting“. Das soll zum Ausdruck bringen, dass sich die Täter:innen vermehrt auf große Opfer und Unternehmen, aber auch auf öffentliche Einrichtungen als Angriffsziele konzentrieren. Ein gutes Beispiel ist in diesem Zusammenhang der massive Anstieg von Ransomware. Denn auch hier liegt ein verstärkter Fokus auf das „Big Game“, d.h. auf der Verschlüsselung von zahlungskräftigen großen Unternehmen und öffentlichen Einrichtungen in der Erwartung, dass diese aufgrund ihrer Eigenschaft als Kritische-Infrastruktur oder als wirtschaftlich potentes Ziel eine entsprechende Zahlungsbereitschaft zeigen werden. Die durchschnittliche Höhe von Lösegeldforderungen hat sich gegenüber den Jahren 2019/2020 sogar verdreifacht. Auch heute existieren unterschiedliche Arten von Ransomware. Neben der Verschlüsselung von IT-Systemen, gibt es die sog. Wiper-Ransomware, bei der die angegriffene Infrastruktur dauerhaft zerstört wird, unabhängig davon, ob gezahlt wird. Die bekanntesten Varianten sind derzeit Ryuk, Doppelpaymer und Conti.[9]

2. Der Vierfache Angriff

Herr *Löhr* schildert anschließend, wie sich ein typischer Ransomware-Angriff darstellt. Die Täter:innen infiltrieren zunächst die betroffenen IT-Systeme, entweder indem Schwachstellen ausgenutzt werden, Fishing-Mails versendet werden, oder – das ist ein klarer Trend – die Täter:innen sich gestohlene Zugangsdaten kaufen. Durch die Infiltration des IT-Systems können sie sich nun Zugang zu dem System verschaffen. Daran schließt sich eine Phase des Auskundschaftens an. Das Lösegeld wird festgelegt. Schließlich kommt es zum „Action-Day“. An dem erfolgt eine – auch für den Betroffenen wahrnehmbare – Verschlüsselung der Daten und die entsprechende Erpressung mit digitalem Lösegeld.

Standardmäßig werden diese Angriffe als sog. Double Extortion (zweifache Erpressung) ausgeführt. D.h. neben der Erpressung mit Lösegeld, damit die verschlüsselten Daten wieder entschlüsselt werden, wird zudem damit Lösegeld abgepresst, dass die durch den Angriff erlangten Daten nicht auf entsprechenden Leak-Seiten veröffent-

[8] Online abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0796&from=DE (zuletzt abgerufen am 12.5.2022).

[9] Ein interessantes Infoportal in diesem Zusammenhang ist „No more Ransom“.

licht werden, womit die Reputation des Unternehmens geschädigt würde. Mittlerweile gibt es außerdem die „Tripple-Extortion", d.h. zu der Ransomware Erpressung durch Verschlüsselung und Veröffentlichung ist die Durchführung von DDoS-Attacken hinzugetreten. Diese sind sog. Überlastungsangriffe, die die Webseiten der Unternehmen „lahm legen". Auch diese werden stets mit eigenständigen Lösegeldforderungen ausgeführt. Neuester Trend ist die vierfache, die „Quadruple Extortion". Mithilfe der Daten und Kundenbeziehungen, die durch das Auskundschaften des betroffenen Unternehmens gewonnenen wurden, wird gedroht, Kontakt zu den Kunden aufzubauen, um auch dort einen Ransomware-Angriff durchzuführen, wenn kein entsprechendes Geld gezahlt wird.

3. Die neun Säulen der Dienstleistungsindustrie

Die Dimension dieser Angriffe lässt den Schluss zu, dass in vielen Fällen nicht nur eine Person alle Tathandlungen und Prozessschritte selbst vornimmt. Stattdessen gibt es Arbeitsteilung und Spezialisierung, die über die ganze Welt verteilt ist, wobei man sowohl IT-Fachleute, Cybercrime-Service-Provider und OK-Gruppierungen findet – aber eben auch den „digitalen Jedermann", der sich ohne jegliche Kenntnisse eine Komplettlösung kaufen kann. In anderen Worten: Es ist eine kriminelle Dienstleistungsindustrie.

Das kriminelle Serviceangebot in der Underground Economy kann auf mindestens neun Dienstleistungssektoren zurückgeführt werden: 1) Es gibt die Malware-Programmierung, 2) die Stärkung der Malware gegen Erkennung und Deaktivierung durch die betroffenen Unternehmen oder Anti-Viren-Scanner, und 3) das Testen der Malware auf Anti-Viren-Software-Resistenz – erst wenn die gängigen Anti-Viren-Softwaren nicht anschlagen, kann die Software mit einem kriminellen TÜV-Siegel versehen und 4) vertrieben werden. Daneben gibt es 5) einen Sektor, der Handelsplattformen für kompromittierte Zugangsdaten oder Zahlungsdaten anbietet, um Systeme infiltrieren zu können (s.o.). Ein sehr großer Sektor sind 6) die sog. Foren, in denen Expertisen ausgetauscht, Aufgaben verteilt, und Modi Operandi besprochen werden können. Weiter gibt es 7) die Malware-Auslieferung, bildlich gesprochen: Die digitalen Paketdienste, die die Malware zum betreffenden Unternehmen bringen und dort hineinschleusen. Wenn das geschehen ist, geht es 8) darum, das Geld, das erwirtschaftet worden ist, zu sichern. Letztendlich gibt es da auch 9) den Dienstleistungssektor, der sich mit dem „Cashout" beschäftigt und die Gewinne z.B. über Strohmänner an die Tatbeteiligten weiterleitet.

4. Aufgabe des BKA

Nach den geschilderten Herausforderungen im Bereich der Cyberkriminalität geht Herr *Löhr* auf die Rolle des BKA ein. Ein Bereich ist die internationale Zusammenarbeit (§ 3 BKA-Gesetz). Das BKA vermittelt für die Bundesländer nach außen in die Welt und umgekehrt nach innen. Das BKA führt auch eigene Ermittlungen durch (§ 4 BKA-Gesetz). Es hat eine originäre unmittelbare Zuständigkeit bei bestimmten Cyberangriffen auf Behörden des Bundes oder „kritische Infrastrukturen" gemäß Bundesrecht. Daneben ermittelt das BKA aber auch im Rahmen der sog. Auftragszuständigkeit, d.h. auf Antrag der Länder. Das BKA ist auch zuständig für das Thema der Früherkennung und Strategie. Es beobachtet, wo sich neue Verhaltensweise auftun. Sie sind auch „Tool- und Solutionprovider" für die deutsche Polizei, wodurch verhindert werden soll, dass sich jede Polizeidienststelle eigene Tools baut, sondern dass die Werkzeuge zentral (in internationalen Kooperationen) entwickelt und zur Verfügung gestellt werden. Und schließlich (als wichtigsten Punkt) betreibt das BKA Kooperationen, denn in keinem anderen Phänomenbereich wie im Bereich Cybercrime ist das von gleicher immenser Bedeutung. Die Strafverfolgung ist in besonderer Weise auf die Zusammenarbeit mit der IT-Sicherheitswirtschaft, mit den betroffenen Unternehmen und potentiell betroffenen Opferunternehmen angewiesen.

5. Die „Werkzeugkiste" des BKA

Anschließend präsentierte Herr *Löhr* den Zuhörer:innen einige Tools aus der Werkzeugkiste, die dem BKA bei der internationalen Bekämpfung von Cyberkriminalität helfen: Zum einen hat das BKA ein weltweites Netzwerk aus sog. BKA-Verbindungsbeamten. Diese sind zwar nicht spezialisiert auf das Thema „Cyber", sie sind aber der erste Anknüpfungspunkt zu Dienststellen im Ausland, zu denen bis dato noch kein direkter Kontakt bestand. Daneben gibt es Europol auf europäischer Ebene, die die Strafverfolgungsmaßnahmen in den Nationalstaaten auf unterschiedliche Weise wie bspw. durch Informationsaustausch oder weitere europäische Kooperationsrahmen unterstützen können. Dort angesiedelt sind auch das EC3 (das europäische Zentrum zur Bekämpfung von Cybercrime) und J-Cat (Joint Cybercrime Action Taskforce), die bei der Initiierung und Unterstützung grenzübergreifender Ermittlungen gegen „Cybercrime-Keyplayer" eine große Rolle spielen. So konnte J-Cat bspw. schon knapp 80 internationale Exekutiveinsätze und Verfahren unterstützen. Es existieren aber auch EU-Förderprogramme, mit denen ganz konkret operative Maßnahmen finanziert, aber auch Präventionsarbeit und die Aus- und Fortbildung in Mitgliedstaaten unterstützt werden können, wie bspw. EMPACT. Sobald es den europäischen Rahmen verlässt, kann auf Interpol zurückgegriffen werden. Neben diesen supranationalen Einrichtungen, in denen das BKA als Ansprechpartner für die deutsche Polizei fungiert, gibt es auch eine Reihe bilateraler Kooperationen mit Cybercrimedienststellen. Ein weiterer Trend, der beobachtet werden kann, ist der Zusammenschluss zwischen Strafverfolgungsbehörden und Wirtschaftsunternehmen. Ein weiteres effektives Werkzeug sind die 24/7-Netzwerke – v.a., wenn es ganz schnell gehen muss. Eines der wichtigsten Netzwerke ist das auf der Basis der Budapester Konvention und dient der Beschleunigung des Vorabsicherungsverfahrens in bestimmten Fällen (die Bitte die Daten in einem vorläufigen Status zu sichern und einzufrieren bis das offizielle Rechtshilfeersuchen greift).

6. Fazit

Der internationalen Cybercrime-Bekämpfung stehen im Werkzeugkasten ein System von Verbindungsbeamten im Ausland zur Verfügung, das auf einer Reihe von bilateralen Premiumpartnerschaften gründet, sowie sehr engen Kooperationen, sowohl im Bereich der Entwicklung als auch der Strafverfolgung im engeren Sinne, ein weitverzweigtes 24/7-Netzwerk der Cybercrime-Dienststellen und die supranationalen Polizeieinrichtungen Europol (insb. J-Cat) und Interpol. So ein spezialisiertes Verbindungsbeamtenzentrum und Netzwerk an Kooperationen gibt es bisher für keinen anderen Phänomenbereich, hat aber aufgrund der Erfolgsgeschichte durchaus Potential auf andere Felder „abzufärben".

7. Q&A

In der anschließenden Q&A-Session wurde noch einmal hervorgehoben, dass es nicht nur eine Spezialisierung auf die verschiedenen Dienstleistungssektoren auf Täter:innen-Seite gibt, sondern auch unter den Polizeibehörden, die diese Bereiche durchaus auch separat verfolgen, wenn die entsprechenden Voraussetzungen für präventive oder repressive Maßnahmen erfüllt sind. Die Möglichkeit mittels „Hackbacks" auf die Infrastrukturen der Angreifer:innen zuzugreifen endet an der Landesgrenze für die deutsche Polizei. Eine große Herausforderung bei der Kooperation mit den (geschädigten) Unternehmen ist die Abstimmung der Maßnahmen und die Terminierung, denn diese fürchten einen Reputations- bzw. Geschäftsschaden und möchten die Kundeninteressen schützen. Die Polizeibehörden müssen dahingehend sensibilisiert werden, um eine verbesserte Maßnahmenplanung durchzuführen, sodass sich die Unternehmen öffnen und häufiger auf die Strafverfolgung zugehen. Für die erfolgreiche Bekämpfung von Cybercrime geht es sowohl darum, ein internationales Netzwerk aufzubauen und sich externes Knowhow in die Dienststellen zu holen (bspw. durch die Zusammenarbeit mit der IT Sicherheitswirtschaft) als auch darum, das eigene Skillset der Beamt:innen auszubauen.

IV. Knowledge Management and Obstacles to International Cybercrime Investigations (englischer Vortrag ins Deutsche übersetzt) von *Prof. Dr. Marie-Helen Maras*, John Jay College, NY, USA

Als letzte Referentin des Veranstaltungstages richtete sich *Prof. Dr. Marie-Helen Maras* vom John Jay College live aus New York an die heimischen Bildschirme. Sie teilt ihre Sicht bzgl. der internationalen Zusammenarbeit mit den Zuschauer:innen. Dabei geht sie auf verschiedene Faktoren ein, die solche Kooperationen überhaupt erst möglich machen und belegt das mit einigen Erfolgsbeispielen. Sie nennt aber auch Hindernisse, die einer internationalen Zusammenarbeit im Bereich der Cyberkriminalität entgegenstehen. Der Schlüssel, den sie zur Überwindung sieht, ist Wissensmanagement.

1. Harmonisierung der Vorschriften

Ein wichtiger Schritt für die internationale Zusammenarbeit ist die Rechtsharmonisierung – also eine einheitliche und strukturierte Antwort auf Cyberkriminalität. Einige Länder verfügen über Gesetze, die speziell auf die Bekämpfung der Cyberkriminalität ausgerichtet sind, andere (bspw. Japan und China) haben ihre einschlägigen Bestimmungen im Strafgesetzbuch geändert, um die Cyberkriminalität anzusprechen. Weitere Länder haben bestehende Gesetze, die eigentlich für die Offline-Kriminalität gedacht sind, genutzt, um bestimmte Arten von Cyberkriminalität anzugehen, ohne den bestehenden Wortlaut zu ändern. Hinsichtlich der verfahrensrechtlichen Bestimmungen stellt die Cyberkriminalität neben dem Beweisrecht vor allem auch die internationale Zusammenarbeit, die Rechtshilfe, die Auslieferung und die Verpflichtungen der Diensteanbieter vor große Herausforderungen. Grund dafür ist, dass die Normen, wie die Beweisregeln, nicht universell standardisiert sind. Im Bereich der Cyberkriminalität braucht es aber unbedingt ähnliche Beweisregeln und Strafverfahren, da diese Form der Kriminalität Grenzen überschreitet und sich auf digitale Geräte und Systeme überall auf der Welt mit Internetanschluss auswirkt. Die Harmonisierung von Gesetzen und ihrer Durchsetzung sind für die internationale Zusammenarbeit von entscheidender Bedeutung, da sie dabei helfen können, Orte, die sich durch schwache Strafverfolgung auszeichnen (sog. sichere Häfen), zu beseitigen. Ganz allgemein führt eine Harmonisierung auch zu einer Erleichterung der Zusammenarbeit und zu einer effektiveren Verfolgung von Cyberkriminellen und deren Auslieferung.

a) Bilaterale und multilaterale Abkommen

Ein Instrument für die Harmonisierung und den Informationsaustausch sind die regionalen und nationalen Konventionen, Abkommen und Verträge in Bezug auf Cybercrime. Sie zielen darauf ab, die nationalen Gesetze zu harmonisieren, die Ermittlungstechniken im Bereich der Computerkriminalität zu verbessern und die internationale Zusammenarbeit zu intensivieren. Beispiele sind die Budapest Konvention (the Council of Europe´s Convention on Cybercrime of 2001)[10], das Abkommen der Gemeinschaft Unabhängiger Staaten über die Zusammenarbeit bei der Bekämpfung von Straftaten im Zusammenhang mit Computerinformationen von 2001, die "League of Arab States" und ihre Konvention über die Bekämpfung von Straftaten im Bereich der Informationstechnologie von 2010[11], das Abkommen der Shanghaier Organisation für Kooperation über die Zusammenarbeit auf dem Gebiet der internationalen Informationssicherheit von 2010[12], den Entwurf des Übereinkommens der Afrikanischen Union über die Schaffung eines Rechtsrahmens für

[10] Online abrufbar unter: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (zuletzt abgerufen am 12.5.2022).

[11] Online abrufbar unter: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf (zuletzt abgerufen am 12.5.2022).

[12] Online abrufbar unter: http://eng.sectsco.org/news/20210913/778271.html (zuletzt abgerufen am 12.5.2022).

die Cybersicherheit in Afrika von 2012[13], und das Übereinkommen der Afrikanischen Union über Cybersicherheit und den Schutz personenbezogener Daten von 2014[14].

b) Rechtshilfeabkommen

Daneben gibt es auch Rechtshilfeabkommen, die als Mechanismus für den Informationsaustausch dienen und die internationale Zusammenarbeit erleichtern. Da es bei Rechtshilfeersuchen allerdings keine zeitlichen Anforderungen gibt, kann es sein, dass sie den Ermittlungsprozess verlangsamen und eine rechtzeitige Reaktion verhindern, die erforderlich ist, um digitale Beweise zu beschaffen. Zeit ist in Cybercrime-Ermittlungen ein ausschlaggebendes Kriterium. Es braucht daher unbedingt eine rechtzeitige Beantwortung von Anfragen.

c) Informeller Austausch

Um diesen Prozess des Informationsaustausches zu beschleunigen und die Zusammenarbeit zu erleichtern, werden häufig auch informelle Mechanismen genutzt. So gibt es beispielsweise zwischen dem öffentlichen Sektor, den Strafverfolgungsbehörden und dem privaten Sektor informelle Informationsaustauschnetze (bspw. der US Cyber Security and Information Sharing Act von 2015). In einigen Ländern gibt es allerdings rechtliche Beschränkungen, die die Behörden daran hindern bzw. einschränken, über informelle Kanäle Unterstützung zu leisten. Sobald also ein strafrechtliches Ziel und die Erlangung von Beweismitteln verfolgt werden, muss die informelle Zusammenarbeit formalisiert werden, so dass die erlangten Beweise vor dem einzelstaatlichen Gericht zulässig sind.

d) Einrichtung offizieller gemeinsamer Ermittlungsgruppen

Eine weitere Möglichkeit zur Erleichterung der internationalen Zusammenarbeit ist die Einrichtung offizieller gemeinsamer Ermittlungsmaßnahmen. Es gibt einige rechtliche und praktische Fragen im Zusammenhang mit gemeinsamen Ermittlungen im Bereich der Cyberkriminalität: Beispielsweise müssen die unterschiedlichen Regeln für Beweismittel und Strafverfahren in den Ländern, die an den gemeinsamen Ermittlungen beteiligt sind, berücksichtigt werden. Damit gemeinsame Ermittlungen erfolgreich sein können, muss eine Vereinbarung darüber getroffen werden, wer die Ermittlungen leitet, welche Rolle die einzelnen Personen bei den gemeinsamen Ermittlungen spielen, welche Verantwortlichkeiten bestehen und wie die gemeinsamen Ermittlungen überwacht werden sollen. Außerdem muss geregelt sein, wie Konflikte zwischen den konkurrierenden Interessen der an den gemeinsamen Ermittlungen beteiligten Länder gelöst werden können.

2. Beispiele für eine erfolgreiche internationale (formelle und informelle) Zusammenarbeit

Prof. Maras erwähnt als Erfolgsgeschichte der internationalen Zusammenarbeit die Zerschlagung der „Emotet-Malware", die etwa 1,6 Millionen Computer weltweit infizierte und insbesondere kritische Infrastrukturen angriff, durch die Kooperation mehrerer Länder (USA, Kanada, Frankreich, Deutschland, Niederlande, Litauen, Schweden und Ukraine) unter der Führung von Europol und Eurojust. Auch die Beschlagnahme von INFRAUD ist ein bekanntes Beispiel für eine gelungene internationale Zusammenarbeit, die u.a. von den USA, dem Vereinigten Königreich, Australien, Frankreich, Italien, Kosovo und Serbien gegen die Organisation geführt wurden. Ein weiteres sehr bekanntes Beispiel für eine erfolgreiche gemeinsame Ermittlung im Bereich der internationalen Cyberkriminalität sind die gemeinsamen Ermittlungen gegen Alphabay und Hansa Market zwischen dem FBI, der US Drug Enforcement Administration, Europol und der niederländischen Polizei. Weitere erfolgreiche Operationen waren DisrupTor und Wallstreet Market. Es konnten auch schon erfolgreiche gemeinsame Ermittlungen gegen Verkäufer:innen proprietärer Geräte, die zur Erleichterung krimineller Handlungen eingesetzt werden, durchgeführt werden. Ein gutes Beispiel hierfür ist EncroChat. EncroChat war ein international erhältliches Mobilgerät, das ein verschlüsseltes Netzwerk bot und bei dem die Kamera, das Mikrofon, das GPS sowie der USB-Anschluss entfernt wurden. Also alles, was zur Überwachung der Nutzer:innen verwendet werden konnte. An den Ermittlungen beteiligt waren französische und niederländische Strafverfolgungs- und Justizbehörden sowie Europol und Eurojust. Die Informationen, die aus den EncroChat-Ermittlungen gewonnen wurden, konnten und werden immer noch in zahlreichen laufenden strafrechtlichen Ermittlungen zu Mord, Drogenhandel und anderen Verbrechen verwendet werden.

3. Schwierigkeiten bei internationalen Ermittlungen im Bereich der Cyberkriminalität

Es gibt also einige Faktoren, die zu erfolgreichen internationalen Ermittlungen im Bereich der Cyberkriminalität führen. Daneben gibt es aber auch einige Hindernisse, die einer erfolgreichen internationalen Bekämpfung von Cyber-Kriminalität entgegenstehen. Technologien zur Verbesserung der Privatsphäre und Anonymitätsnetzwerke wie TOR erschweren die internationale Ermittlung, denn so wird eine Identifizierung von Cyberkriminellen und ihren Geräten oft unmöglich. Auch der Einsatz von mit Malware infizierten Zombie-Computern, Botnetzen oder digitalen Geräten, die von Fernzugriffswerkzeugen gesteuert werden, hemmt eine Zuordnung. Weitere Hindernisse für internationale Ermittlungen im Bereich der Cyberkriminalität sind zeitliche Aspekte. Neben der Schwierigkeit der Terminfindung unter den weltweit verteilten Strafverfolgungsbehörden, kann die Beantwortung von Ersuchen

[13] Online abrufbar unter: https://ccdcoe.org/uploads/2018/11/AU-120901-DraftCSConvention.pdf (zuletzt abgerufen am 12.5.2022).

[14] Online abrufbar unter: https://issafrica.org/ctafrica/uploads/AU%20Convention%20on%20Cyber%20Security%20and%20Personal%20Data%20Protection.pdf (zuletzt abgerufen am 12.5.2022).

nach Informationen oder Beweisen Monate oder sogar Jahre dauern. Einen weiteren Zeitfaktor stellt die Übersetzung der beschafften Dokumente aus den verschiedenen Ländern dar; daneben kostet es das ersuchende Land auch viel Geld. Dies ist vor allem in Entwicklungsländern problematisch, die nicht über die notwendigen Mittel verfügen.

4. Kapazitätenausbau und Wissensmanagement

Der Aufbau von Kapazitäten sowie die Zusammenarbeit und Koordinierung von Ermittlungsbemühungen sind von entscheidender Bedeutung für erfolgreiche Ermittlungen. Die meisten Strafverfolgungsbehörden (als erste Ansprechstelle) benötigen erhebliche Investitionen in personelle, finanzielle und technische Ressourcen sowie aktuelle Informationen über Fälle von Cyberkriminalität, Schulungen und Technologien, um Cyberkriminalität wirksam untersuchen zu können. Aktuell fehlt es Ländern auf der ganzen Welt an qualifizierten und ausgebildeten Fachkräften, die über Grundkenntnisse im Bereich Cyberkriminalität und digitale Forensik verfügen, sowie finanzierten Schulungsprogrammen. Es sollten Initiativen ergriffen werden, um die Ausbildung von nicht spezialisierten Strafverfolgungsbeamten im Bereich der Cyberkriminalität zu verbessern. Eine dieser Initiativen könnte darin bestehen, Schulungen zu Internetkriminalität und digitaler Forensik in den Lehrplan der Polizeiakademien aufzunehmen.

An dieser Stelle kann auch das Wissensmanagement helfen. Es zielt darauf ab, Wissen und Wissensquellen denjenigen zur Verfügung zu stellen, die es suchen und benötigen. Wissensmanagement ist kein linearer Prozess. Man kann es sich als einen kontinuierlichen Zyklus vorstellen, der mit der Ermittlung und Formulierung des Wissensbedarfs beginnt. In einem nächsten Schritt geht es darum, vorhandenes Wissen zu ermitteln und zu bewerten, Wissenslücken zu eruieren, Prozesse und Praktiken zu entwickeln, um die Wissenslücken zu schließen, diese Prozesse und Praktiken umzusetzen und schließlich die umgesetzten Prozesse und Praktiken zu bewerten, um festzustellen, ob die Wissenslücken geschlossen wurden. Falls nicht, beginnt der Prozess von vorne. Dieses Wissen wird schließlich in Content-Management-Systemen verwaltet und auf einer Website oder in einer durchsuchbaren Datenbank zur Verfügung gestellt. Ein Beispiel dafür ist das „Sherlock-Portal".

5. Fazit

Der Erlangener Cybercrime Tag ist schon ein Schritt in die richtige Richtung und eine Form des Wissensaustauschs. Es sind jedoch weitere Anstrengungen erforderlich, um das Wissen über Ermittlungen im Bereich der Cyberkriminalität zu verwalten und auszutauschen. Die derzeitigen Herausforderungen für die Zusammenarbeit bei internationalen Ermittlungen im Bereich der Cyberkriminalität können wirklich nur mit einem vielschichtigen Ansatz überwunden werden, der sich mit Hindernissen und Defiziten bei den nationalen Kapazitäten, mit den begrenzten personellen, finanziellen und technischen Ressourcen für die Durchführung von Ermittlungen, mit den Unterschieden in der Qualität der Ausbildung von Ermittler:innen im Bereich der Cyberkriminalität und Spezialist:innen für digitale Forensik befasst und der schließlich die derzeitigen begrenzten Wissensmanagementsysteme in diesem Bereich überwindet.

6. Q&A

In der sich dem Vortrag anschließenden Q&A-Session wird noch einmal die Wichtigkeit der Berücksichtigung von nationalen materiell-rechtlichen und vor allem prozess-rechtlichen Vorschriften bei der internationalen Strafverfolgung von Cybercrime anhand der EnchroChat-Fälle verdeutlicht, um entscheiden zu können, ob die dadurch gewonnenen Beweismittel vor einem nationalen Gericht zugelassen werden dürfen oder nicht. In Deutschland sind sich die meisten Gerichte einig, dass die Beweismittel, die durch die EnchroChat-Ermittlungen erlangt wurden, zulässig sein sollen. Im Gegensatz zu Deutschland gibt es in den USA eine große akademische Teilhabe in politischen und gesetzgeberischen Entscheidungen. Auf der internationalen Ebene fehlt es hier aber noch an entsprechenden Institutionen.

V. Grußworte des Präsidiums der FAU und des Staatsministers *Eisenreich* (MdL, Bayerisches Staatsministerium der Justiz)

Die Vorträge der Referent:innen wurden abgerundet durch Grußworte des Präsidiums der FAU und des bayerischen Staatsministers der Justiz, *Georg Eisenreich*.

Zunächst berichtet *Prof. Joachim Hornegger*, Präsident der FAU, stellvertretend für die Universität, dass die FAU die innovationsstärkste Universität Deutschlands ist und weltweit Platz vierzehn belegt. Diesen Erfolg verdankt die Universität u.a. der tatkräftigen Unterstützung von innovativen Köpfen, wie des Veranstalters *Prof. Safferling*, und solchen Events wie dem EC²CT 2021. Für Innovation und Informationsaustausch steht auch die Kooperation zwischen der FAU und der ZCB (Zentralstelle Cybercrime Bayern). Auch mithilfe des interdisziplinären Graduiertenkollegs „GRK 2475 Cyberkriminalität und Forensische Informatik" an der FAU wird ein innovatives Feld erschlossen.

Anschließend übernahm Staatsminister *Eisenreich* das Mikrofon und bedankt sich für die Einladung, vor allem weil das Thema Cyberkriminalität das bayerische Justizministerium sehr beschäftigt. Die Cyberkriminalität ist auf dem Vormarsch, sie wird professioneller und immer vernetzter. Das Internet darf dabei kein rechtsfreier und kein rechtsverfolgungsfreier Raum sein. Der Staat muss hinschauen und das Recht durchsetzen. Dafür gibt es Ansätze auf verschiedenen Ebenen: Zunächst müssen die Strafverfolgungsstrukturen optimiert werden. Es braucht Spezialist:innen. Als bestes Beispiel dient die Entwicklung der ZCB, welche mit zwei Staatsanwält:innen begonnen hat und jetzt eine Stärke von achtzehn Staatsan-

wält:innen mit IT Expert:innen aufweist. Auf einer zweiten Ebene braucht es Austausch und Zusammenarbeit zwischen den vielen Behörden, die involviert sind – sowohl auf bundes-, europäischer und internationaler Ebene. Als dritten Schritt brauchen Ermittler:innen in der digitalen Welt weitergehende Befugnisse, um effektiv ermitteln zu können. Dieser Schritt ist jedoch nach wie vor sehr umstritten, wie das Thema der Verkehrsdatenspeicherung zeigt. Zuletzt müssen die Polizei- und Justizbehörden technisch auf dem neuesten Stand sein. Ein Beispiel hierfür ist die Investition und Unterstützung des Tools „Dark Web Monitor". Darüber hinaus ist eine Vernetzung und der Austausch zwischen Behörden und der Wissenschaft von entscheidender Bedeutung – dafür steht sowohl der EC²CT 2021 als auch die Kooperation zwischen der FAU und der ZCB. Nur so ist es möglich, Impulse zu setzen, Rechtsfragen zu diskutieren und neue beobachtete Phänomene zu erforschen.

Zum Abschluss bedankt er sich bei den Teilnehmer:innen, die sich dem Kampf gegen Cybercrime verschrieben haben und übergibt die Bühne wieder *Prof. Safferling* und den Referent:innen für eine abschließende Diskussionsrunde.

VI. Abschlussdiskussion, Schlusswort und Fazit

Die vom Veranstalter *Prof. Christoph Safferling* geleitete Abschlussdiskussion fasste noch einmal die gewonnenen Erkenntnisse und wichtigsten Punkte des heutigen Tages zusammen.

Aus Sicht der Strafverfolgung im Kampf gegen die Cyberkriminalität lässt sich zusammenfassend sagen: „Wir sind auf dem richtigen Weg, aber definitiv noch nicht da." Um dieses Ziel zu erreichen, braucht es eine starke Zusammenarbeit untereinander, mit der Regierung, mit dem privaten Dienstleistungssektor, den geschädigten Unternehmen und mit der Wissenschaft. Je enger und besser zusammengearbeitet wird, desto effektiver kann den Herausforderungen der internationalen Bekämpfung von Cyberkriminalität begegnet werden. Diese vielseitigen Kooperationen sind ein Alleinstellungsmerkmal des Kriminalitätsfeldes der Cyberkriminalität.

Ein Punkt, der die Zusammenarbeit erleichtern würde, wäre die Harmonisierung des Strafrechts. Aber das Prinzip der gegenseitigen Anerkennung, auf dem eine Harmonisierung beruht, ist vor allem für das Strafrecht problematisch. Das Verständnis von Grundrechten und Strafrechtspflege divergiert teilweise zu sehr. Die Wahrung der Schutzstandards der Menschenrechte und Grundrechte der Betroffenen muss aber stets berücksichtigt werden. Nichtsdestotrotz sind international durchführbare Maßnahmen und eine funktionierende Zusammenarbeit unerlässlich für eine effektive internationale Strafverfolgung. Die einzelnen nationalen Systeme sind auf diese Situation noch nicht richtig eingestellt. Ein Vorschlag, um das zu beheben ist es die Ressourcen, v.a. Geld für Personal und Technik zu erhöhen und einem nationalen „Klein-Klein" aktiv entgegenzuwirken.

Die Zahlen und Trends der Entwicklung von Cyberkriminalität lassen auf den ersten Blick wenig Raum für Hoffnung. Man darf jedoch nicht übersehen, dass die Bekämpfung des Kriminalitätsfeldes Cybercrime ein strategischer Schwerpunkt in der Strafverfolgung geworden ist. Die Bearbeitung der Delikte wird deutlich gestärkt und die nationale und internationale Zusammenarbeit wird enger denn je. Es kann ein erheblicher personeller Aufwuchs verzeichnet werden, ebenso eine verstärkte Kooperation mit der IT-Sicherheitswirtschaft. Es wird viel Zeit und Aufwand in Vernetzung investiert, um der internationalen Dimension der Cyberkriminalität schnell und effektiv begegnen zu können. Es wird noch einmal betont, dass der Informationsaustausch und die dadurch gewonnene Expertise weitergegeben werden muss. Es müssen noch mehr Individuen und Länder in die Kooperationen und Diskussionen mit einbezogen werden.

Die Vorträge und Diskussionsbeiträge des EC²CT 2021 machten deutlich, wie wichtig die interdisziplinäre Zusammenarbeit und der Informationsaustausch ist. Aus diesem Grund bedarf es solcher Diskussionen, wie sie im Rahmen des EC²CT 2021 geführt wurden, um die aktuellen Schwächen und Stärken der internationalen Strafverfolgung von Cyberkriminalität auszutarieren und mögliche Ansätze und Ideen auszutauschen. Vor diesem Hintergrund freuen sich *Prof. Safferling* und sein Team der International Criminal Law Research Unit über eine gelungene Tagung und blicken der Fortsetzung der Veranstaltungsreihe „Erlanger Cybercrime Tag" im Herbst 2022 mit dem Thema „KI in der Strafverfolgung" entgegen (hoffentlich wieder in Präsenzform).