Professionelle Cyberkriminalität

Jakob Ebbinghaus, Lukas Staffler

1. Einleitung

„Cyberbedrohungen sind zu einem integralen Bestandteil der Bedrohungslandschaft in der Schweiz aber auch international geworden“[1] – so fasste der im November 2024 erschiene Lagebericht des Schweizerischen Bundesamts für Cybersicherheit (BACS) die gegenwärtigen Entwicklungen zur Cybersicherheit zusammen und berichtete zum ersten Halbjahr 2024 von nahezu einer Verdopplung der Meldungen zu sicherheitsrelevanten Vorfällen zur Vergleichsperiode im Vorjahr. Dies zeigt exemplarisch, dass Wirtschaft und Gesellschaft mit einem cyberkriminellen Phänomen konfrontiert wird, das nicht nur Unternehmen, sondern auch Privatpersonen und letztlich sogar staatliche Strukturen bedroht.[2]

Das Phänomen Cyberkriminalität ist dabei sehr dynamisch[3] und die bisherige Erfahrung legt nahe, dass es sich bei diesem Phänomen nicht einfach um die Begehung von Straftaten mit digitalen Mitteln in Anlehnung an analoge Kriminalität handelt. Vielmehr ist anzunehmen, dass es ein neuartiges, komplexes und zum Teil grundlegend andersartiges Kriminalitätsphänomen darstellt,[4] das die Mittel des nationalen (Straf-)Rechts in bisher nicht gekanntem Ausmaß herausfordert. Nach der hier vertretenen Auffassung handelt sich um eine neue Form der Wirtschaftskriminalität[5],

1 BACS, Cybersicherheit Lage in der Schweiz und international, Halbjahresbericht 2024/I vom 07.11.2024.

2 Instruktiv *Hofmann*, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, 2024, 151 ff.; etwa zum Ransomware-Angriff auf Costa Rica, vgl. Couretas Cyber Operations, 2024, S. 1.

3 Empfehlenswert *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, 41 ff. (insb. 79 ff., 98 ff.).

4 Exemplarisch *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, 185 ff.; zusammenfassend *Staffler*, ZWF 2025, 172 ff.

5 Dabei ist sogleich darauf hinzuweisen, dass Cybercrime nicht nur aus wirtschaftlicher Motivation, sondern auch aus politisch, ideologischer oder terroristischer Motivation begangen wird: *Hofmann*, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, 2024, 151. Wirtschaftskriminalität ist nicht legaldefiniert, als Orientierungspunkt kann

die allerdings mit den bisherigen Erfahrungen von kriminellen Machenschaften durch legale Unternehmen (wie etwa Untreue oder Betrug) nur noch wenig gemein hat. Vielmehr zeichnen sich diese Phänomene durch einen hohen Grad an Professionalisierung und Arbeitsteilung aus.[6] Es sind Strukturen, die in ihrer Dynamik und internationalen Verflechtung noch wenig erforscht sind. Gleichzeitig treffen die neuen Kriminalitätsphänomene auf Wirtschaft und Gesellschaft, die zwar eine hohe Affinität zur Digitalisierung aufweisen, aber noch nicht ausreichend für die damit verbundenen Risiken sensibilisiert sind.

Vor diesem Hintergrund besteht das Ziel dieses Beitrags darin, jüngere Entwicklungen aus dem Bereich Cybercrime dahingehend zu reflektieren, inwiefern klassische Straftatbestände wie der Tatbestand der kriminellen Vereinigung im deutschen Strafrecht diese noch erfassen kann. Es wird geprüft, ob die bestehenden rechtlichen und gesellschaftlichen Ansätze einer Anpassung bedürfen, um diesen Herausforderungen effektiv begegnen zu können.

2. Phänomenologie von Ransomware

Um die einleitend beschriebenen Tendenzen näher zu ergründen, wird im Folgenden Ransomware im Hinblick auf Struktur, Funktionsweise und gesellschaftlichen Auswirkungen analysiert. Ransomware entstammt der digitalen Sphäre, ist gegenwärtig überaus praxisrelevant und veranschaulicht exemplarisch, wie organisierte Cyberkriminalität nicht nur technologische Schwachstellen ausnutzt, sondern auch auf psychologische Manipulation und soziale Dynamiken setzen, um ihre Ziele zu erreichen. Zudem folgt das Phänomen einem sehr strukturierten, arbeitsteiligen Vorgehen und basiert auf der gezielten Ausnutzung menschlicher und technischer Anfälligkeiten.

---

§ 74c I 1 GVG herangezogen werden; eine anerkannte Definition existiert für das deutsche Strafrecht nicht (vgl. *Dannecker/Bülte* Wabnitz/Janovsky/Schmitt, Handbuch Wirtschafts und Steuerstrafrecht, 2025 § 1 Rn. 5), oftmals wird darauf abgestellt, dass die besonderen Umstände des Wirtschaftsverkehr ausgenutzt werden, wie der Missbrauch des für das Funktionieren der Wirtschaft erforderlichen Vertrauens. Ransomware-Angriffe werden für Gewöhnlich nicht hierunter gefasst, obwohl bei den Phishing Angriffen ein solcher Vertrauensmissbrauch, Ausnutzen von Gepflogenheiten im Geschäftsverkehr, typisch ist.

6 *Hofmann*, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, 2024, 142.

2.1. Begriff

Der Begriff „Ransomware" setzt sich aus den englischen Wörtern „*ransom*" (Lösegeld) und „*software*" zusammen. Die Wortbildung folgt einem in der Informationstechnologie üblichen Muster, bei dem der Wortteil „*-ware*" für verschiedene Arten von Software verwendet wird, wie beispielsweise bei „*malware*" (bösartige Software) oder „*adware*" (werbefinanzierte Software). Die Kombination dieser Begriffe zu „Ransomware" beschreibt somit eine Schadsoftware, die darauf abzielt, den Zugriff auf Daten oder Systeme zu blockieren, um vom Opfer Lösegeld zu erpressen.[7]

In den letzten Jahren gab es eine Reihe prominenter Ransomware-Angriffe, die die Aufmerksamkeit auf diese Art von Cybercrime und ihr Ausmaß gelenkt haben.[8] Exemplarisch ist der WannaCry-Angriff aus dem Jahr 2017 zu nennen, der weltweit hunderttausende Computersysteme in mehr als 150 Ländern betraf. WannaCry nutzte eine Schwachstelle im Windows-Betriebssystem aus, die ursprünglich von der NSA entdeckt und später von einer Hackergruppe veröffentlicht wurde. Der Angriff führte zu massiven Störungen in staatlichen Einrichtungen und privaten Unternehmen.[9] Ein anderes berühmtes Beispiel ist der Colonial Pipeline-Angriff im Jahr 2021, bei dem ein wichtiges Pipeline-Netzwerk in den USA lahmgelegt wurde, was zu erheblichen Treibstoffengpässen führte. Die Angreifer, die die Ransomware „DarkSide" verwendeten, erpressten ein Lösegeld in Millionenhöhe, das von den Behörden teilweise zurückverfolgt werden konnte.[10]

2.2. Funktionsweise

Die Funktionsweise von Ransomware basiert auf einer Kombination von Verschlüsselungstechnologien, Techniken zur sozialen Manipulation und Mechanismen zur finanziellen Erpressung. Die Bedrohung durch Ransomware besteht im Wesentlichen darin, dass Daten auf einem infizierten System verschlüsselt werden, so dass der betroffene Nutzer den Zugriff auf diese Daten oder das gesamte System verliert.

---

7 Statt vieler s. *Meyer/Biermann*, MMR 2022, 940.

8 Vgl. *Anderl/Tlapak*, in: Anderl (Hrsg.), #Cybercrime Handbuch für die Praxis, 2023, 3 f., 5.

9 *Dickmann*, Cyberversicherung, 2025, Rn. 59.

10 US DoJ Dep.Attorney General Monaco Comprehensive Cyber Review July 2022 S.2,10,11; *Dickmann*, Cyberversicherung, 2025, Rn. 64.

2.2.1. Infiltration

Zunächst wird Ransomware über verschiedene Methoden verbreitet, die sich je nach Zielgruppe und Technik unterscheiden.[11] Besonders häufig werden E-Mails als Angriffskanal genutzt, wobei die Angreifenden Phishing-Kampagnen einsetzen, um die Nutzer zur Interaktion mit der Schadsoftware zu verleiten. Diese E-Mails sind dann so gestaltet, dass sie von vertrauenswürdigen Absendern wie etwa Banken, Behörden oder bekannten Unternehmen zu stammen scheinen.

Im Kontext von Phishing kann zwischen klassischen Massenangriffen und zielgerichteteren Techniken unterschieden werden: Sogenanntes Spear Phishing zielt auf bestimmte Personen oder Organisationen ab und nutzt individuell angepasste Inhalte, z.B. auf Basis öffentlich zugänglicher Informationen aus sozialen Netzwerken oder Unternehmenswebseiten.[12] Im Gegensatz dazu verfolgt sog. Dynamite Phishing einen hybriden Ansatz: Es beginnt mit einer breit gestreuten, generischen E-Mail-Kampagne, die auf eine erste Reaktion abzielt. Reagieren, wie beabsichtigt, einzelne Nutzer darauf, wird der Angriff gezielt vertieft und personalisiert – eine Eskalation, die typischerweise die Auslieferung der eigentlichen Ransomware bezweckt.[13] Darüber hinaus können auch infizierte Webseiten[14] oder kompromittierte Werbeanzeigen als Verbreitungswege dienen, die Nutzerinnen und Nutzer beim Besuch der entsprechenden Seiten automatisch mit der Schadsoftware infizieren.

Ferner spielt das Ausnutzen von Sicherheitslücken in Betriebssystemen oder Software spielt eine wichtige Rolle. Häufig wird Ransomware über sog. Exploit-Kits verbreitet, die gezielt Schwachstellen, insb. sogenannte „*zero-day-exploits*",[15] in nicht aktualisierten Systemen ausnutzen.

---

11 *Anderl/Tlapak*, in: Anderl (Hrsg.), #Cybercrime Handbuch für die Praxis, 2023, 4 f.

12 *Bär* in Wabnitz/Janovsky/Schmitt (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, 6. Aufl. 2025, § 15 Rn. 32.

13 Heise Online, Dynamit-Phishing: Emotet perfektioniert seine Angriffe weiter, 12.4.2019, abrufbar unter https://www.heise.de/security/meldung/Dynamit-Phishing-Emotet-perfektioniert-seine-Angriffe-weiter-4398626.html (abgerufen am 06.04.2025).

14 Vgl. jüngst https://www.bleepingcomputer.com/news/security/fbi-warnings-are-true-fake-file-converters-do-push-malware/ (abgerufen am 23.03.2025): online PDF-Konverter als Einfallstor.

15 Wobei mit zero day Exploits nicht Schwachstellen gemeint sind, die noch nicht geschlossen sind, wie z.B. *Brodowski/Schmid/Scholzen/Zoller* NStZ 2023, 385, 386

2.2.2. Verschlüsselung

Sobald unbemerkter Zugriff auf das infizierte System möglich ist, beginnt die Ransomware (oder die Angreifer) damit, Dateistrukturen zu analysieren und gezielt Dateien auszuwählen, die verschlüsselt werden sollen. Erfahrungsgemäß werden häufig Dateien mit bestimmten Dateierweiterungen wie .docx, .jpg oder .xlsx bevorzugt, da diese in der Regel für den Benutzer von großer Bedeutung sind. Die Verschlüsselung selbst erfolgt mit oftmals selbstentwickelten kryptografischen Verfahren, die sicherstellen sollen, dass die verschlüsselten Daten ohne den richtigen Schlüssel nicht wiederhergestellt werden können.[16]

2.2.3. Lösegelderpressung

Nachdem die Ransomware ihre Aufgabe erfüllt hat, beginnt die Phase der Lösegeldforderung. In einer auffälligen Nachricht wird das Opfer darüber informiert, dass dessen Daten verschlüsselt wurden und die einzige Möglichkeit, sie wiederherzustellen, in der Zahlung eines Lösegelds besteht.[17] Diese Mitteilungen sind oft detailliert und enthalten Anweisungen, wie die Zahlung zu erfolgen hat. Bei gewissen Opfern erfolgt ein Kontakt oft zusätzlich auch über einen verschlüsselten Chatdienst, um weiter Druck auf das Opfer auszuüben.

Um bestmögliche Anonymität in der Zahlungsabwicklung zu gewährleisten, verlangen die Angreifer erfahrungsgemäß die Zahlung in Kryptowährungen wie Bitcoin oder Monero, da diese aufgrund ihres dezentralen Charakters schwerer nachzuverfolgen sind. Transaktionen von Kryptowährungen werden typischerweise auf einer Blockchain, einer Art öffentlich einsehbarem Register, eingetragen, sodass eine durchgeführte Transaktion grundsätzlich nicht rückgängig gemacht werden kann. Zwar ist eine anonyme Nutzung möglich,[18] allerdings können die einzelnen Transaktionen

---

meinen, sondern vielmehr den Schweregrad beschreibt: Schwachstellen, die so gefährlich sind, dass nur null Tage Zeit bleibt, um diese zu schließen.

16 Vgl. allgemein zur Kryptografie im Internet: https://www.quantamagazine.org/how-public-key-cryptography-really-works-20241115/ (abgerufen am 27.03.2025).

17 *Anderl/Tlapak*, in: Anderl (Hrsg.), #Cybercrime Handbuch für die Praxis, 2023, 11 f.

18 *Brenneis*, APuZ 2017, 29, 33 f.; wobei nach einem Hack durchaus auch eine Änderung möglich ist, vorausgesetzt genügend Inhaber stimmen dem „Fork", also der Änderung im Protokoll zu, vgl. https://www.heise.de/news/Nach-dem-DAO-Hack-Ethereum-glueckt-der-harte-Fork-3273618.html (27.3.25).

nachverfolgt werden (Blockchainanalysis), daher ist eine Identifizierung bei Auszahlung grundsätzlich möglich.[19]

Um genau diese Rückverfolgbarkeit zu erschweren, nutzen Täter bisweilen sogenannte Kryptowährungs-Mixer (auch *Tumbler* genannt).[20] Diese Dienste sammeln Transaktionen unterschiedlicher Nutzer, vermischen die ein- und ausgehenden Beträge über viele Zwischenkonten und senden schließlich den Zielbetrag an eine neue Adresse – in stark fragmentierter und kaum rekonstruierbarer Form. Durch dieses „Waschen" der Kette verschwimmt die Spur des Geldflusses. In Kombination mit länderübergreifenden Transfers – insbesondere, wenn die Täter in nicht-kooperative Staaten wie Russland oder China agieren – steht die Strafverfolgung daher vor erheblichen praktischen Herausforderungen.[21]

2.2.4. Zwischenfazit

Zusammenfassend lässt sich sagen, dass Ransomware-Angriffe einem klaren und strukturierten Ablauf folgen, der sich in mehrere Phasen unterteilen lässt.

- In der ersten Phase der Infiltration soll die Ransomware unbemerkt auf dem Zielsystem installiert werden. Dies geschieht entweder durch betrügerisches Verhalten – wie Phishing oder Social Engineering – oder durch technisches Eindringen – beispielsweise über Sicherheitslücken mittels Exploit Kits.
- In der zweiten Phase, in der die Angreifer bereits Zugriff auf das System haben, werden die Daten verschlüsselt. Sobald der Vorgang abgeschlossen ist, kann der Nutzer nicht mehr auf das System oder die Dateien zugreifen.
- Die dritte Phase umfasst oft die Lösegeldverhandlungen. Die Angreifer fordern das Opfer in einer expliziten Nachricht auf, ein Lösegeld zu zahlen, um die verschlüsselten Daten wieder freizugeben. Die Nachricht enthält oft detaillierte Anweisungen für die Zahlung, die meist in Kryptowährungen erfolgt, um eine Rückverfolgung zu erschweren.

19 https://www.newyorker.com/business/currency/how-a-young-couple-failed-to-launder-billions-of-dollars-in-stolen-bitcoin (abgerufen am 23.12.2022).

20 *Fromberger/Haffke/Zimmermann*, BKR 2019, 377, 178 f.; *Maume/Haffke*, in; Maume/Maute, Rechtshandbuch Kryptowerte, 2020, § 15 Rn. 27.

21 https://www.newyorker.com/business/currency/how-a-young-couple-failed-to-launder-billions-of-dollars-in-stolen-bitcoin (abgerufen am 23.12.2022).

Die Verhandlungen werden durch klare Fristen und Drohungen wie die vollständige Löschung der Daten, eine Veröffentlichung privater Daten im Darknet oder eine Erhöhung des Lösegelds bei nicht rechtzeitiger Zahlung verstärkt.[22]

2.3. Ransomware-as-a-Service (RaaS)

Die Struktur eines Ransomware-Angriffs macht deutlich, dass arbeitsteiliges Vorgehen möglich ist, das verschiedene Kompetenzen kombiniert. Ein erfolgreicher Angriff erfordert betrügerisches Verhalten, technisches Know-how und geschickte Verhandlungsstrategien bei der Lösegeldforderung. Diese Komplexität hat in den letzten Jahren die Entstehung eines kriminellen Ökosystems rund um Ransomware begünstigt. Im Schutz der Anonymität des sogenannten Darknets, erfahrungsgemäß aber auch auf Telegram, bieten spezialisierte Akteure und Dienstleister nahezu alle Aspekte eines Ransomware-Angriffs als modulare Dienstleistungen an – ein Modell, das unter dem Begriff „Ransomware as a Service" (kurz: RaaS) bekannt geworden ist.

2.3.1. Ransomware-Ökosystem

In diesem kriminellen Ökosystem haben mehrere Akteure unterschiedliche Rollen, sodass es möglich ist, in modularer Weise über RaaS ein komplettes Angriffsszenario zu organisieren.

Sogenannte Initial Access Broker bieten oft Zugang zu geschützten Systemen, indem sie Sicherheitslücken ausnutzen oder Schwachstellen in Netzwerken identifizieren.[23] Ihre Dienste bilden häufig die Grundlage für einen Ransomware-Angriff, indem sie anderen kriminellen Akteuren den direkten Zugriff auf die Systeme ihrer Opfer ermöglichen. Daneben gibt es Dienstleister, die sich ausschließlich auf die Bereitstellung und Weiterentwicklung von Verschlüsselungssoftware konzentrieren. Diese Dienstleister bieten maßgeschneiderte Verschlüsselungslösungen an, die es den Angreifern erleichtern, die Daten effektiv zu blockieren und die Opfer zur Zahlung des Lösegeldes zu zwingen. Ferner hinaus gibt es spezialisierte Anbieter, die sich um die technische Abwicklung der Lösegeldforderungen küm-

22 *Anderl/Tlapak*, in: Anderl (Hrsg.), #Cybercrime Handbuch für die Praxis, 2023, 3.
23 *Hofmann*, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, 2024, 152.

mern, einschließlich der Bereitstellung sicherer Kommunikationskanäle für die Verhandlungen und der Generierung von Entschlüsselungsschlüsseln nach erfolgter Zahlung.

Das kriminelle Ökosystem umfasst auch unterstützende Dienste, die nicht unmittelbar mit der Durchführung von Angriffen in Verbindung stehen, aber deren Erfolg entscheidend beeinflussen. Ein Beispiel sind die oben genannten Tumbler bzw. Mixer-Dienste, die als Geldwäschedienste dafür sorgen, dass Lösegeldzahlungen, die meist in Kryptowährungen erfolgen, später anonymisiert und in legale Finanzströme überführt werden können. Darüber hinaus gibt es (Darknet-)Plattformen, die als Jobbörsen fungieren und auf denen verschiedene kriminelle Dienstleistungen angeboten werden. Auf diesen Marktplätzen werden Angebote von Akteuren gebündelt, die unterschiedliche Dienstleistungen wie das Schreiben von Schadsoftware, die Verbreitung von Phishing-Kampagnen oder die Bereitstellung von Exploit-Kits anbieten.

All das zeigt, dass „RaaS" die Einstiegshürden für technisch weniger versierte Kriminelle erheblich senkt, da diese auf die Expertise anderer „krimineller Stakeholder" zurückgreifen können. Dies beschleunigt die Verbreitung des kriminellen Geschäftsmodells „Ransomware" zusätzlich.

2.3.2. Ransomware-Serverstrukturen

Das technische Rückgrat eines Ransomware-Angriffs ist erfahrungsgemäß die Infrastruktur sogenannter Command-and-Control-Server (C2-Server). Diese Server fungieren als Schaltstellen, über die infizierte Systeme gesteuert, Verschlüsselungsvorgänge initiiert und exfiltrierte Daten weitergeleitet werden. C2-Server ermöglichen Echtzeitkommunikation zwischen Angreifer und Schadsoftware, koordinieren die Verschlüsselung der Zielsysteme und dienen der Befehlsübermittlung sowie dem Empfang gestohlener Daten. Ransomware-as-a-Service besteht also nicht nur aus Softwaremodulen und kriminellen Dienstleistern, sondern bedarf einer physischen Server-Infrastruktur.

Während viele dieser Server bewusst in Staaten mit geringer internationaler Kooperation platziert wurden, zeigen medienwirksame Erfolge der Strafverfolgungsbehörden aus jüngster Zeit, dass sich ein erheblicher Teil dieser Infrastruktur auch in Europa befand. Dies eröffnete den Behörden neue Handlungsspielräume: Durch gezielte „Takedown"-Aktionen im Rah-

men der Operationen wie „Endgame“[24] oder „Synergia“[25] konnten zentrale Serverstandorte abgeschaltet und damit laufende Ransomware-Kampagnen effektiv unterbrochen werden.

2.4. Häufigkeit

Ransomware-Angriffe haben in den vergangenen Jahren weltweit erheblich zugenommen.[26] Die Angriffsarten- und Abläufe werden von privaten Sicherheitsdienstleistern erfasst und in entsprechenden Berichten zur Verfügung gestellt.[27] Für die Darstellung wurden viele Tatsachenschilderungen von solchen Berichten privater Sicherheitsunternehmen übernommen. Aus wissenschaftlicher Vorsicht ist dabei zu berücksichtigen, dass derartige Dienstleister aus wirtschaftlicher Sicht natürlich motiviert sind, gegenwärtige IT-Gefahren entsprechend darzustellen, weshalb die folgenden Angaben stets mit Vorsicht zu genießen sind.[28] Die Autoren dieses Beitrags sind dennoch vorsichtig zuversichtlich, dass es sich bei den zitierten Aussagen um seriöse Quellen handelt.

Aus dem Sophos-Jahresbericht für das Jahr 2024 ist zu entnehmen, dass 59 % der befragten Unternehmen erfolgreichen Ransomware-Angriffen ausgesetzt waren, bei denen die Angreifer in das System eindringen konnten und eine Datenverschlüsselung erfolgreich durchführten.[29] Frankreich wies mit 74 % die weltweit höchste Ransomware-Angriffsrate auf, dicht gefolgt von Südafrika (69 %) und Italien (68 %). Am unteren Ende

24 Europol Pressemeldung zu Operation „Endgame“, abrufbar unter https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem (06.04.2025).

25 Interpol Pressemeldung zu Operation „Synergia II“, abrufbar unter https://www.interpol.int/News-and-Events/News/2024/INTERPOL-cyber-operation-takes-down-22-000-malicious-IP-addresses (06.04.2025).

26 Statt vieler s. *Sohr/Kemmerich*, in: Kipker (Hrsg.), Cybersecurity, 2. Aufl. 2023, Kap. 3 Rz 177.

27 Etwa Sophos, The State of Ransomware 2024, abrufbar unter https://www.sophos.com/en-us/content/state-of-ransomware (08.01.2025).

28 Illustrativ (wenn auch nicht unbedingt exemplarisch): *Khatchadourian*, A Cybersecurity Firm's Sharp Rise and Stunning Collapse, NewYorker, 28.10.2019, Ed. 4.1.2019.

29 Laut Sophos wurden rund 5.000 IT- und Cybersicherheitsverantwortliche von Unternehmen mit einer Größe von 100 bis 5.000 Mitarbeitenden befragt; die Befragung selbst wurde von der Agentur „Vanson Bourne“ zwischen Januar und Februar 2024 durchgeführt: https://news.sophos.com/en-us/2024/05/14/the-role-of-law-enforcement-in-remediating-ransomware-attacks/ (06.04.2025).

der Skala lagen Brasilien (44 %), Japan (51 %) und Australien (54 %) mit vergleichsweise niedrigen Angriffsraten. Während die Zahl der Angriffe in neun Ländern im Vergleich zu 2023 zurückging, stieg sie in fünf europäischen Ländern an, darunter Österreich, Frankreich, Deutschland, Italien und das Vereinigte Königreich.[30]

Ferner betrafen Ransomware-Angriffe verschiedene Branchen (mit wenigen Ausnahmen) relativ gleichmäßig, wobei die Angriffshäufigkeit in 11 der 15 untersuchten Branchen zwischen 60 % und 68 % lag. Eine Ausnahme bilden der Sektor Staat/Lokalverwaltung, in dem nur 34 % der Organisationen betroffen waren, und der Einzelhandel mit 45 %, in dem ebenfalls weniger als die Hälfte der Befragten Angriffe meldeten. Die höchste Angriffsrate verzeichnete hingegen die Zentral-/Bundesregierung mit 68 %. Der Gesundheitssektor erlebte einen Anstieg der Angriffe auf 67 %, in der IT-, Telekommunikations- und Technologiebranche stieg die Rate auf 55 %.[31]

Offenbar werden Lösegeldzahlungen bei Ransomware-Angriffen von Unternehmen häufig erwogen und tatsächlich geleistet. Bei den 1.097 Befragten, deren Organisation das geforderte Lösegeld gezahlt hat, stieg sowohl der Median als auch der Mittelwert deutlich an: Der Median stieg auf 2 Millionen US-Dollar (im Vergleich zu 400.000 US-Dollar aus dem Vorjahr), der Durchschnittswert von Lösegeldzahlungen lag bei rund 3,9 Millionen US-Dollar.[32] Andere Quellen hingegen berichten, dass 2024 die Zahlungen von Lösegeld nach Ransomware-Angriffen gefallen seien.[33]

3. Case-Study: Conti Leak

Nachdem überblicksweise Funktionsweisen und Mechanismen des Phänomens Ransomware dargestellt wurden, liegt der Fokus nun auf den Tätergruppen, die hinter diesen kriminellen Aktivitäten stehen. Ein differenziertes Verständnis der Strukturen, Motivationen und Vorgehensweisen dieser Gruppen ist essentiell, um effektive Gegenstrategien zu entwickeln und die Mechanismen der Cyberkriminalität in ihrer Gesamtheit zu durchdringen.

30 Sophos, The State of Ransomware, 2024, 4.
31 Sophos, The State of Ransomware, 2024, 6.
32 Sophos, The State of Ransomware, 2024, 18.
33 https://www.bleepingcomputer.com/news/security/ransomware-payments-fell-by-35-percent-in-2024-totalling-813-550-000/ (abgerufen am 25.03.2025), in Berufung auf Chainalysis.

Die Analyse erfordert dabei den Rückgriff auf (einigermaßen) verlässliche Studien und Datenquellen, um hochspekulative Annahmen zu vermeiden und empirisch fundierte Aussagen treffen zu können.

Hierfür bietet sich insbesondere der sogenannte Conti-Leak an, der detaillierte Einblicke in die interne Organisation und Arbeitsweise einer der weltweit aktivsten Ransomware-Gruppen namens „Conti" ermöglicht[34] Die Conti-Gruppe, eine der weltweit aktivsten und aggressivsten Ransomware-Organisationen, rückte Anfang 2022 ins Zentrum der Aufmerksamkeit, als interne Daten an die Öffentlichkeit gelangten.[35] Diese Leaks umfassten mehr als 60.000 interne Chatprotokolle, den vollständigen Quellcode der Ransomware sowie Schulungsmaterialien und Tutorials. Die Veröffentlichung der Daten erfolgte vor dem Hintergrund geopolitischer Spannungen: Nachdem die Conti-Gruppe im Zusammenhang mit dem Ukraine-Konflikt ihre Unterstützung für die russische Regierung zum Ausdruck gebracht hatte,[36] reagierte ein Insider, der mutmaßlich pro-ukrainisch eingestellt war, mit der Veröffentlichung der internen Informationen. Diese undichte Stelle bot der Öffentlichkeit und den Strafverfolgungsbehörden einen bislang beispiellosen Einblick in interne Abläufe eines Ransomware-„Konzerns".

3.1. Organisationsstruktur

Entgegen der Vorstellung von Cyberkriminellen als lose agierenden Einzelakteuren zeigt sich, dass Conti als streng hierarchisch strukturierte Organisation agierte, die in vielerlei Hinsicht den Abläufen eines klassischen Unternehmens glich.[37]

---

34 Instruktiv *Paternoster/Nazzari/Jofre/Uberti*, Inside the Leak: Exploring the Structure of the Conti Ransomware Group, Global Crime 1–24/2025, abrufbar unter https://doi.org/10.1080/17440572.2025.2473350 (06.04.2025).

35 Im Mai 2025 wurde die berüchtigte Ransomware-Gruppe LockBit kompromittiert und interne Daten mit Informationen zu Opfern veröffentlicht; diesbezüglich lagen jedoch zum Zeitpunkt der Manuskriptabgabe keine verlässlichen Informationen vor, weshalb hier nur auf den Conti Leak eingegangen wird.

36 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 26.04.2025).

37 Inzwischen ist im Bereich der Ransomware zunehmend ein Modell mit dezentralen Strukturen zu beobachten: Viele Gruppen operieren heute im Rahmen sogenannter Affiliate- oder Franchise-Modelle, bei denen eigenständige Partner – teils mit vertraglich geregelter Gewinnbeteiligung – für die initiale Infektion und teilweise auch für die Lösegeldverhandlungen verantwortlich sind; vgl. *Baker*, Ransomware as a Service (RaaS) explained how it works & examples vom 30.01.2023, abrufbar unter https://w

Herz der Conti-Organisation war eine klare Hierarchie, die Entscheidungsfindung und Arbeitsteilung effizient strukturierte. An der Spitze standen Führungskräfte, die strategische Entscheidungen trafen, wie etwa die Auswahl von Angriffszielen, die Festlegung von Lösegeldforderungen und die Priorisierung technischer Entwicklungen. Diese Anführer waren auch für die Verwaltung der finanziellen Ressourcen zuständig und koordinierten die Verteilung der Gewinne innerhalb der Gruppe. Unterhalb dieser Führungsebene gab es spezialisierte Teams, die jeweils für bestimmte Aufgabenbereiche zuständig waren. Diese Teams arbeiteten weitgehend autonom, aber unter der Aufsicht ihrer jeweiligen Vorgesetzten, die die Umsetzung der Gruppenstrategie sicherstellten. Auffallend ist die detaillierte Dokumentation und Berichterstattung innerhalb der Organisation, um Transparenz und Effizienz zu maximieren.

Die Organisation arbeitete nach einem Modell arbeitsteiliger Strukturen, das sich durch klare Zuständigkeiten und hohe Professionalität auszeichnete. Technische Experten innerhalb der Gruppe widmeten sich der Entwicklung und Weiterentwicklung der Conti-Schadsoftware. Sie waren für die Anpassung an neue Sicherheitsmaßnahmen und die Integration aktueller Exploits verantwortlich, damit die Schadsoftware immer auf dem neuesten Stand war und ihre maximale Wirkung entfalten konnte. Parallel dazu agierten Spezialisten, die sich auf das Eindringen in fremde Netzwerke und Systeme konzentrierten. Diese setzten eine Vielzahl von Techniken ein, darunter gezielte Phishing-Kampagnen und den Einsatz von Exploit-Kits, um Sicherheitslücken auszunutzen. Gelegentlich wurden auch Zugangsdaten von Drittanbietern im Darknet beschafft, wodurch die Gruppe ihre Angriffsfläche vergrößerte und zusätzliche Ressourcen nutzen konnte.

Ein weiterer wichtiger Bereich innerhalb der Organisation betraf die Kommunikation mit den Opfern. Mitarbeiter, die sich auf Verhandlungsstrategien spezialisiert hatten, übernahmen den Kontakt und führten Lösegeldforderungen gezielt durch. Sie bedienten sich manipulativer Taktiken, um Druck auszuüben und die Opfer zur Zahlung zu bewegen. Dabei folgten sie strikten Vorgaben des internen „Playbooks", die auf eine Maximierung der Erfolgsaussichten abzielten. Eine andere „Abteilung" von Experten entwickelten Strategien zur Geldwäsche, insbesondere im Umgang mit Kryptowährungen, die häufig bei Lösegeldzahlungen verlangt wurden. Mithilfe der bereits oben erwähnten Mixer-Diensten und komplexen Transak-

ww.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ (06.04.2025).

tionsketten wurde sichergestellt, dass die finanziellen Erträge nur schwer zurückverfolgt werden konnten und letztlich in legale Finanzströme einflossen.

3.2. Onboarding

Die durch den Conti-Leak bekannt gewordenen Schulungsmaterialien zeigen auch die systematische Herangehensweise der Ransomware-Gruppe Conti bei der Schulung ihrer Mitglieder.[38] Ein zentraler Bestandteil des Schulungsprogramms war die Einführung in fortgeschrittene Penetrationstechniken. Neue Mitglieder erhielten detaillierte Handbücher, in denen Schritt für Schritt erklärt wurde, wie man in fremde Netzwerke eindringt, sich Administratorrechte verschafft und persistente Zugänge schafft. Diese Anleitungen beinhalteten auch die Konfiguration von Tools wie AnyDesk für den Fernzugriff und Rclone für die Datenexfiltration, um die Effektivität der Angriffe zu maximieren. Besonderes Augenmerk wurde auf die Verwendung spezieller Software gelegt.

Die Schulungsunterlagen enthielten detaillierte Anweisungen zur Installation und Verwendung von Cobalt Strike, einem bekannten Werkzeug für Penetrationstests, das von der Gruppe für böswillige Zwecke angepasst wurde. Darüber hinaus wurden Techniken wie Kerberoast zur Kompromittierung von Anmeldedaten in Netzwerken sowie Methoden zur Deaktivierung von Sicherheitsmechanismen wie Windows Defender vermittelt, um die Entdeckung der Schadsoftware zu verhindern. Die Schulungsunterlagen gingen über technische Aspekte hinaus und behandelten auch operative Taktiken. Die Mitglieder wurden in Social Engineering geschult, um menschliche Schwächen auszunutzen, sowie in der effektiven Nutzung des Darknets, um zusätzliche Ressourcen zu beschaffen oder erbeutete Daten zu verkaufen.

Diese umfassende Ausbildung stellte sicher, dass die Mitglieder nicht nur über das technische Know-how, sondern auch über das notwendige taktische Verständnis verfügten, um erfolgreiche Angriffe durchzuführen. Die Professionalität des Schulungsprogramms spiegelte sich in der Qualität und Tiefe der zur Verfügung gestellten Materialien wider: Die Unterlagen waren klar strukturiert, praxisorientiert und wurden regelmäßig aktualisiert, um der sich verändernden Sicherheitslandschaft Rechnung zu tragen.

38 Ausführlich dargestellt durch esentire https://www.esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru (06.04.2025).

3.3. Kommunikation

Die im Conti-Leak veröffentlichten internen Chat-Protokolle geben einen detaillierten Einblick in die Kommunikations- und Entscheidungsprozesse des Conti-„Konzerns".[39] Die Kommunikation innerhalb der Conti-Gruppe erfolgte hauptsächlich über verschlüsselte Messenger-Dienste, was Sicherheit und Anonymität gewährleisten sollte. Die Protokolle zeigen, dass regelmäßig über den Fortschritt der Angriffe, technische Probleme und finanzielle Angelegenheiten berichtet wurde. Besonders auffällig ist die direkte und teilweise rigide Kommunikation zwischen den verschiedenen Hierarchieebenen. Entscheidungen und Anweisungen wurden klar formuliert und die Ausführenden hatten wenig Spielraum, von diesen Vorgaben abzuweichen. Dies betraf insbesondere die Auswahl der Angriffsziele, die Festlegung der Höhe der Lösegeldforderungen und das technische Ressourcenmanagement.

Trotz (oder gerade wegen) dieser zentralisierten Struktur und der klaren Kommunikation zeigen die Lecks auch interne Spannungen und Konflikte. Ein häufiger Streitpunkt war die Verteilung der Gewinne. Einige Mitglieder äußerten ihre Unzufriedenheit über ungleiche Zahlungen und forderten eine gerechtere Verteilung. Diese Konflikte wurden zum Teil offen in den Chats ausgetragen, wobei das „Management" oft rigoros eingriff, um die Disziplin aufrechtzuerhalten. Ein weiterer Konfliktpunkt betraf die Sicherheitsvorkehrungen. Einige Mitglieder beschwerten sich über die ständige Überwachung oder die Notwendigkeit, ihre Identität zu verbergen, was die Arbeit erschwerte. Diese Beschwerden wurden jedoch selten berücksichtigt, da die Sicherheit der Organisation oberste Priorität hatte.

3.4. Darknet Ökonomie

Die im Conti-Leak enthaltenen Informationen geben nicht nur Einblick in die interne Organisation der Gruppe, sondern auch in das kriminelle Ökosystem des Darknets selbst, in dem sie operierte. Besonders aufschlussreich sind die Strategien, mit denen die Conti-Gruppe über diese Plattformen neue Mitglieder rekrutierte und ihre Strukturen ausbaute.

39 Ausführlich bei Rapid7 unter https://www.rapid7.com/blog/post/2022/03/01/conti-ransomware-group-internal-chats-leaked-over-russia-ukraine-conflict (06.04.2025) sowie Flashpoint unter https://flashpoint.io/blog/history-of-conti-ransomware/ (06.04.2025).

Über spezialisierte Foren und Marktplätze wurden gezielt Spezialisten mit bestimmten technischen oder operativen Fähigkeiten angesprochen. Die Gruppe nutzte die Anonymität dieser Plattformen, um potenzielle Mitglieder anzuwerben, ohne ihre eigene Identität oder ihren Standort preiszugeben. Die von Conti veröffentlichten Stellenangebote waren häufig detailliert und ähnelten Ausschreibungen legaler Unternehmen. Gesucht wurden etwa Entwickler mit Erfahrung in Verschlüsselungstechnologien, Penetrationstester und Experten für Social Engineering. Um das Interesse potenzieller Bewerber zu wecken, wurden attraktive Vergütungen und flexible Arbeitsbedingungen hervorgehoben. Ein typisches Merkmal dieser Ausschreibungen war die Betonung der "Unabhängigkeit" der Mitarbeiter, die häufig als Freelancer arbeiteten und somit nicht fest in die Organisationsstruktur eingebunden waren. Gleichzeitig unterstrich Conti die eigene Professionalität und die langfristigen Möglichkeiten einer Zusammenarbeit, was insbesondere für technikaffine und risikobereite Akteure attraktiv war.[40]

Die Rekrutierungsprozesse der Conti-Gruppe waren ebenso strukturiert wie die betrieblichen Abläufe. Interessenten mussten ihre Fähigkeiten als „Freelancer“ häufig in praktischen Tests unter Beweis stellen. Dabei konnte es sich um die erfolgreiche Durchführung eines Penetrationstests oder die Entwicklung eines spezifischen Softwaretools handeln. Solche Tests dienten nicht nur der Überprüfung der technischen Fähigkeiten, sondern auch als Sicherheitsmechanismus, um zu gewährleisten, dass die Bewerber keine verdeckten Ermittler waren. Neben den technischen Fähigkeiten legte die Gruppe großen Wert auf Loyalität und Diskretion. Die Kandidaten wurden in den ersten Phasen ihrer Tätigkeit intensiv überwacht, und ihre Kommunikation mit anderen Mitgliedern war streng reglementiert. Damit sollten potenzielle Sicherheitsrisiken minimiert und der innere Zusammenhalt der Gruppe gewahrt werden. Nach der Rekrutierung der bewährten Freelancer wurden diese durch ein strukturiertes Onboarding-Programm in die Organisation integriert. Dieses beinhaltete nicht nur Schulungen, wie sie im Leak ausführlich beschrieben sind, sondern auch die schrittweise Einführung in operative Aufgaben. Neue Mitglieder wurden zunächst mit niedrigschwelligen Aufgaben betraut, bevor sie in zentrale Projekte eingebunden wurden. Diese Methodik ermöglichte es der Gruppe, Fähigkeiten

40 *Paternoster/Nazzari/Jofre/Uberti*, Inside the Leak: Exploring the Structure of the Conti Ransomware Group, Global Crime 1–24/2025, abrufbar unter https://doi.org/10.1080/17440572.2025.2473350 (06.04.2025).

und Loyalität der neuen Mitglieder zu testen und ihnen gleichzeitig die Möglichkeit zu geben, sich mit den internen Abläufen vertraut zu machen.[41]

4. Ransomware-Gruppierungen als kriminelle Vereinigungen

Im Folgenden soll die Frage ergründet werden, ob Ransomware-Gruppierungen als kriminelle Vereinigung strafrechtlich belangt werden und welche Herausforderungen sich bei der Rechtsanwendung stellen könnten.

4.1. Einleitende Bemerkungen

Das deutsche Strafrecht kennt für Zusammenschlüsse mehrerer Personen, neben den verschiedenen Beteiligungsmöglichkeiten, zwei Formen: die Bande und die kriminelle Vereinigung.

Die Mitgliedschaft in einer Bande ist ein Tatbestandsmerkmal, aber kein eigener Straftatbestand, sodass die Mitgliedschaft in einer Bande nicht als solches strafbar ist. Vielmehr ist diese in erster Linie strafschärfend, wobei es auch Auswirkungen im Bereich der Nebenfolgen und Zwangsmaßnahmen im Ermittlungsverfahren gibt.[42]

Die kriminelle Vereinigung ist demgegenüber ein eigenständiger Tatbestand. Strafbar macht sich, wer sie gründet, als Mitglied teilnimmt, sie unterstützt (oder für Mitglieder wirbt). Die Konsequenz ist, dass auch eigentlich sozialadäquates Verhalten, wie etwa die Serverwartung, vom Tatbestand erfasst ist, sofern der entsprechende Vorsatz vorliegt.[43] Historisch hat die Norm ihren Ursprung im (preußischen) Staatsschutzrecht, erfasste also in erster Linie staatsfeindliche politische Verbindungen wie die SPD Ende des 19. Jahrhunderts.[44] Wir werden sehen, dass auch die heute geltende Norm diese Entstehungsgeschichte nicht gänzlich abgeschüttelt hat. Ob

41 Check Point Research unter https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/ (06.04.2025).

42 vgl *Ebbinghaus* HRRS 2023/10 S.318 f.

43 Vgl. MüKoStGB/*Schäfer/Anstötz* § 129 Rn. 88; SK-StGB/*Stein/Greco* § 129 Rn. 52,47, 48; LK-StGB/*Krauß* § 129 Rn. 100, 101, 103; BGH NJW 2016, 657, 660.

44 Strafbar waren Verbindungen, die unrechtmäßig die Gesetzesvollziehung/Verwaltung behinderten. Da dies auf die SPD nicht zutraf, bedurfte es des Sozialistengesetzes, auf deren Umgehung SPD (/-nahe Verbindungen) gerichtet waren, um § 129 RStGB anwenden zu können.

Ransomware-Gruppierungen hierunter fallen können, soll Gegenstand des folgenden Abschnitts sein. Der Schwerpunkt wird dabei auf russischsprachigen Gruppierungen liegen, bei denen die Anwendung des § 129 StGB vor den größten Herausforderungen steht.

Eine Vereinigung, wie sie in § 129 II StGB legaldefiniert ist, besteht aus einem personalen, zeitlichen, organisatorischen und einem voluntativen Element.[45] Der Zusammenschluss setzt eine gewisse Organisationsstruktur sowie eine in gewissem Umfang vorhandene instrumentelle Vorausplanung und Koordinierung voraus. Die Vereinigung ist kriminell, wenn ihr Zweck oder ihre Tätigkeit auf die Begehung von Straftaten gerichtet ist.

Als zusätzliche, ungeschriebene Einschränkung des Tatbestandes wird ferner verlangt, dass es sich bei den Straftaten um solche von einigem Gewicht handeln müsse.[46] Teilweise wird dies in § 129 III Nr.2 StGB verortet.[47] Dies soll insbesondere Bagatellkriminalität ausschließen, aber schon die Begehung von Diebstählen im großen Stil wurde als ausreichend angesehen.[48] Daher ist es naheliegend, dass Erpressungen im großen Stil, Ausspähen von Daten, Datenhehlerei, Computersabotage[49] diese Anforderungen erfüllen. Dies gilt auch dann, wenn in dem Bereitstellen der Ransomware und der Infrastruktur lediglich eine Beihilfe gesehen wird, da die Affiliates bei der Opferauswahl und Infiltration der IT Systeme nicht selten eigenständig vorgehen.

Falls es sich bei den Ransomware-Gruppen um eine kriminelle Vereinigung iSd § 129 StGB (idR iVm § 129b StGB, da ausländisch) handelt, so ist nicht nur Mitgliedschaft strafbar, sondern auch deren Unterstützung. Dies hätte allerdings zur Folge, dass die Zahlung von „Lösegeld" zumindest

45 BGH, Urteil vom 3. Dezember 2009 – 3 StR 277/09 –, BGHSt 54, 216–236 Rn. 23; *Brodowski/Schmid/Scholzen/Zoller*, NStZ 2023, 385, 388; SK-StGB/*Stein/Greco* § 129 StGB Rn. 7.

46 BGH, Urteil vom 22.2.1995 – 3 StR 583/94-, BGHSt 41, 47–57; LK-StGB/*Krauß* § 129 StGB Rn. 54; SK-StGB/*Stein/Greco* § 129 StGB Rn. 27.

47 *Kuhli/Papenfuß*, KriPoZ 2023, 71,75, sie können sich dabei zwar auf den Willen des Gesetzgebers berufen, welcher mit dieser Einschränkung Sachbeschädigungen aus dem Anwendungsbereich des § 129 StGB heraushalten wollte, die Rspr. & hM sieht es jedoch als ein ungeschriebenes Tatbestandsmerkmal an.

48 BGHSt 57,14.

49 Vgl hierzu BGH ZWH 2022, 22, hier schien es sich um ein Affiliate gehandelt zu haben, § 129 StGB wurde nicht angesprochen, obwohl mehr als drei Personen beteiligt waren; vgl. auch *Eisele* in: Hilgendorf/Kudlich/Valerius (Hrsg.), Handbuch des Strafrechts, 2022, § 63 Rn. 142–145; *Vogelgesang/Möllers*, jM 2016, 381, 383ff.

den Tatbestand des § 129 StGB erfüllt[50] und eine Strafbarkeit des Ransomware-Opfers, das eine Zahlung an die Gruppe tätigt, allenfalls über Rechtfertigungsgründe (insb. Nötigungsnotstand) zu vermeiden wäre[51].

4.2. Organisatorisches Element

An das organisatorische Element werden keine großen Anforderungen gestellt, die Rechtsprechung bejaht dies bereits bei einem Zusammenschluss, der nur in den sozialen Netzwerken existiert, auch dann, wenn dieser „in gewisser Weise unverbindlich ist" und keine besonders ausgestalteten Regeln kennt, solange nur ein koordiniertes Zusammenwirken zur Erreichung des gemeinsamen Ziels vorliegt.[52]

Für einen Teil der Lehre ist das organisatorische Element das maßgebliche Kriterium, um die Bande von der kriminellen Vereinigung abzugrenzen.[53] Nach dieser Auffassung zeichnet sich eine Bande durch deutlich rudimentärere Strukturen aus als eine kriminelle Vereinigung, auch auf die persönliche Bereicherung der Beteiligten gerichteten Zusammenschlüsse könnten so als kriminelle Vereinigung erfasst werden. Dabei wird je-

50 A.A. *Makepeace* StV 2022, 754, 755–756 meinte, dass es dem Zahler idR nicht bewusst sein dürfte, welche Gruppierung genau unterstützt werden würde, daher läge der objektive Tatbestand schon nicht vor, dabei werden die Anforderungen an den objektiven Tatbestand hinsichtlich des Unterstützens einer kriminellen Vereinigung in nicht mehr vertretbarer Weise angehoben, sodass im Ergebnis nur noch die Unterstützung einer bereits gerichtlich als solcher festgestellten kriminellen Vereinigung erfasst wäre, *Makepeace* lehnt auch den Vorsatz dahingehend ab, da ein bloß allgemeines Wissen, dass eine kriminelle Vereinigung hinter der Erpressung stehe nicht ausreiche (aaO S. 756); aber auch LK-StGB/*Krauß* § 129 Rn. 149 verlangen nur, dass sich der Vorsatz darauf bezieht, dass die Unterstützung gerade der betreffenden kriminellen Vereinigung zugute kommt, m.a.W.: wird Lösegeld gezahlt, ist es nicht ersichtlich, wieso sich das Opfer nicht bewusst sein sollte, dass diese Lösegeldzahlung dem Adressaten der Zahlung (Erpresser) auch zugute kommt, damit auch der (ggf. dahinter stehenden) kriminellen Vereinigung; vgl. auch SK-StGB/*Stein/Greco* § 129 StGB Rn. 46: Unterstützen Aufrechterhaltung oder Erhöhung des spezifischen Gefährdungspotentials, keine qualifizierte Vorsatzform (aaO Rn. 52).

51 Unserer Ansicht nach ist die Lösung über den Nötigungsnotstand vorzugswürdig (so auch SK-StGB/*Stein/Greco* § 129 Rn. 53 für Schutzgeldzahlungen allgemein; vgl. *Dittrich/Erdogan*, ZWH 2022, 13, 17; so auch *Brodowski/Schmid/Scholzen/Zoller*, NStZ 2023, 385, 388,389, welche auch auf § 129 VI StGB verweisen; ein Anfangsverdacht scheint uns in diesem Kontext aber eher fernliegend, siehe Lösegeldzahlungen bei Cyberangriffen .

52 *Ebbinghaus*, HRRS 10/2023, 318, 320, Fn. 21 m.w.N.

53 *Sinn/Iden/Pörtner*, ZIS 2021 435, 446,447.

doch der Tatbestand in verfassungsrechtlich nicht hinnehmbare Weise verschleift: denn das übergeordnete gemeinsame Interesse, welches der Gesetzgeber in die Legaldefinition in Abs.2 aufgenommen hat, würde in dem Tatbestandsmerkmal der Bezweckung von Straftaten aufgehen. Das übergeordnete Interesse ist es, was ein notwendiges Merkmal für eine Vereinigung ist, die Bezweckung von Straftaten ist es, was der Vereinigung den kriminellen Charakter verleiht.

In der Praxis ergibt sich dabei die Herausforderung, dass Ransomware-Gruppen nicht homogen arbeiten, sondern sich bisweilen zwischen Kerngruppe und Affiliate differenzieren lässt. So setzen gerade russische Ransomware-Gruppierungen häufig auf ein RaaS Modell (s.o.), bei dem es eine Kern-Gruppierung gibt, die Software, Server zur Verfügung stellt, sowie oft auch eine Marke bereitstellt, unter der operiert wird. Die sogenannten Affiliates sind diejenigen, die die Angriffe überwiegend durchführen, teilweise bedienen sie sich auch sogenannter Access-Broker, die ein anvisiertes IT-System bereits infiltriert haben, sodass nur noch die Schadsoftware hochgeladen werden muss. Es ist nicht unüblich, dass ein Affiliate mehrere Anbieter (/Kern-Gruppierungen) nutzen, mehrere Angriffe gleichzeitig durchführen.[54]

Es scheint, als wären die Affiliates nicht in dem erforderlichen Maße in die Kerngruppierung integriert, um von eine umfassende Vereinigung anzunehmen. Denn teilweise agieren die Affiliates in den Dark-Net Foren auch unter eigenem Namen[55]. Sofern also die Kerngruppierung eine kriminelle Vereinigung darstellt, kann die Nutzung von Ransomware durch Affiliates eine Unterstützung der Kerngruppierung darstellen, somit von § 129 I S.2 StGB erfasst werden. Denkbar ist auch, dass es sich bei manchen Affiliates um eigenständige kriminelle Vereinigungen handelt, basierend auf den öffentlich zugänglichen Informationen spricht viel dafür, Affiliates und Kern-Gruppierung zumindest nicht als eine (gemeinsame) kriminelle Vereinigung anzusehen.

---

54 https://analyst1.com/ransomware-diaries-volume-2/ (abgerufen am 27.08.2023); vgl. auch https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/ (abgerufen am 06.04.2025), wonach es hohe Fluktuation bei den ‚Mitglieder' niedrigen Ranges bei Conti gegeben hat, es erscheint daher fraglich, diese als Mitglieder einzustufen, die kriminelle Vereinigung iSd § 129 StGB könnte daher auf höherrangige Mitglieder beschränkt geblieben sein.

55 zB ‚National Hazard Agency' als Name, unter dem ein Affiliate von LockBit auftrat, unbekannt, ob ein oder mehrere Mitglieder hatte, vgl. https://analyst1.com/ransomware-diaries-volume-3-lockbits-secrets/ (abgerufen am 27.08.2023).

4.3. Übergeordnetes gemeinsames Interesse

Problematisch ist das Element des sog. übergeordneten gemeinsamen Interesses, insbesondere bei wirtschaftskriminellen bzw. auf finanziellen Gewinn ausgerichteten Zusammenschlüssen.[56] Über dieses gemeinsame Interesse erfolgt die Abgrenzung zum bloß strafschärfenden Tatbestandsmerkmal der Bande.[57] Das gemeinsame Interesse darf sich nicht auf die Begehung von Straftaten beschränken (da es sich hierbei um ein anderes konstitutives Merkmal der kriminellen Vereinigung handelt, dass auch vom Vorsatz umfasst sein muss, auch würde andernfalls ein Gleichlauf mit der Bande erfolgen), auch ein (reines) Handeln um eines persönlichen Vorteils willen genügt nach ständiger Rechtsprechung nicht.[58] Im wirtschaftskriminellen Kontext im engeren Sinne (bspw Vorwürfe gegen ehemaligen Vorstand der Wirecard-AG), gibt es große Probleme, da die Strukturen regelmäßig auch legalen Zwecken dienen.[59] Zumindest dieses Problem besteht aber bei den Ransomware-Gruppierungen nicht.

4.3.1. Russische Ransomware-Gruppierungen

Bei Ransomware-Gruppen, die auch politisch Ziele verfolgen dürfte die Bejahung einer kriminellen Vereinigung leichtfallen, zumindest bezüglich der Kerngruppe. Russische Ransomware-Gruppierungen sind wohl überwiegend nicht in den staatlichen Sicherheitsapparat integriert, werden aber von diesem geduldet, solange sich die Tätigkeit auf Opfer außerhalb der russischen Föderationen beschränkt.[60] Die Beschränkung auf das Ausland scheint somit weniger politischen Zielen zu dienen, als vielmehr der Selbst-

56 BGH 3 StR 21/231, Rn.21 juris; BGH, Beschluss vom 9. Februar 2021 – AK 3 und 4/21 –, juris Rn.24.

57 BGH, Urteil vom 2. Juni 2021 – 3 StR 21/21 –, juris Rn.20; BGH, Beschluss vom 2. Juni 2021 – 3 StR 61/21 –, juris Rn.7, st.Rspr.

58 BGH 3 StR 21/231, juris; BGH NJW 2021, 2813, 2815f. BT-Drucks. 18/11275 S. 11; LK/*Krauß* § 129 Rn. 40 f.; SK-StGB/*Stein/Greco* § 129 Rn. 15; *Montenegro*, GA 2019, 489, 502.

59 SK-StGB/*Stein/Greco* § 129 Rn.4,19.

60 Überwiegend das westliche Ausland, aber auch in der südlichen Hemisphäre, zB Brasilien, vgl. *Couretas*, Cyber Operations, 2024, S.1 ff.

erhaltung, dem Schutz vor Strafverfolgung oder zu viel Aufmerksamkeit und Zwangsrekrutierung durch FSB/SVR/GRU.[61]

Es scheint deshalb fraglich, ob die Unterstützungserklärung zugunsten der russischen Regierung für den Überfall auf die Ukraine durch Conti wirklich Ausdruck einer politischen Einstellung oder Zielsetzung ist, da viele der Affiliates, die für das RaaS Geschäft elementar sind, in der Ukraine saßen und entsprechend verärgert waren.[62] Da zeitgleich mit der Invasion der FSB kurzzeitig ein Interesse an Ransomware-Gruppen zeigte,[63] lässt sich dies eher als eine Schutzmaßnahme vor staatlicher Repression deuten. LockBit, eine konkurrierende Ransomware-Gruppe, erklärte etwa kurz nach dem russischen Einmarsch, dass sie unpolitisch sein, ihnen ginge es nur ums Geld: „*We are only interested in money for our harmless and usefull work*"[64].

Die mittlerweile an Bedeutung verlorene EvilCorp, eine andere Ransomware-Gruppe, hat demgegenüber enge Verbindungen zu staatlichen Hackern[65] – hier erscheint es naheliegend, dass nicht nur wirtschaftliche Interessen verfolgt werden. Folglich ist bei Gruppierungen wie EvilCorp, die Verbindungen zu Nachrichtendiensten haben und auch politisch motiviert agieren,[66] die Bejahung einer kriminellen Vereinigung im Ausland naheliegend.

61 Vgl. hierzu jüngst: https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-s-internal-chat-logs-leak-online/ (abgerufen am 23.03.2025): BlackBasta hat zuvor russische Banken ins Visier genommen, daraufhin wurden wohl interne Chats geleakt.

62 Vgl. https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023).

63 Vgl https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/ (abgerufen am 06.04.2025).

64 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023) Diese Formulierung zeigt die zynische Selbstdarstellung als Post-Pen-tester, also als Programmierer, die Sicherheitslücken aufzeigten und dafür belohnt werden wollen, ein derart abwegiger Vorwand, der durch die Tätigkeit widerlegt ist und keiner näheren Erörterung bedarf.

65 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.23), vgl auch National State Ransomware S. 16f.

66 *Couretas*, Cyber Operations, 2024, S. 86.

4.3.1.1. Das Problem „LockBit"

In Fällen wie bei LockBit,[67] bei denen die Gewinnerzielungsabsicht der Beteiligten im Vordergrund zu stehen *scheint*, ist der typologische Vereinigungsbegriff der Rechtsprechung[68] von Bedeutung: Im Rahmen der Gesetzesreform 2017 hat der Gesetzgeber klargestellt, dass die Anforderungen an das organisatorische Element bei der kriminellen Vereinigung abgesenkt werden sollen.[69] Jedoch kann das gemeinsam verfolgte Interesse der Vereinigung aus objektiven Merkmalen hergeleitet werden, eine stark ausgeprägte Organisationsstruktur spricht dafür, dass nicht nur die persönliche Bereicherung der einzelnen im Vordergrund stehe.[70] So sah der BGH Indizien für ein übergeordnetes gemeinsames Interesse im Bestehen eines Prozesses der einheitlichen Willensbildung, internen Sanktionierung von Verstößen gegen gemeinschaftlich Regeln, eine Gemeinschaftskasse oder der Beanspruchung staatlicher Autorität und Einflussnahme auf Medien,[71] alles Elemente, die sich, wie dargelegt, auch bei Ransomware-Gruppierungen bejahen lassen.[72] In der Callcenter-Entscheidung hat der BGH aufgrund stark ausgeprägter Organisationsstrukturen das Bestehen einer kriminellen Vereinigung für naheliegend gehalten, sodass der Fall an eine Staatsschutzkammer zur weiteren Tatsachenfeststellung überwiesen wurde.[73] Die erste Hawala Entscheidung des BGH[74] wurde z.T. so verstanden, dass als gemeinsames Interesse auch der Selbsterhalt der Organisation in Betracht kommt,

67 Trotz der Stellungnahme Contis nach dem Überfall auf die Ukraine, spricht unserer Meinung viel dafür, dass dies auch auf Conti zutrifft, vgl. https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/ (abgerufen am 06.04.2025).

68 BGH NJW 2021, 2813 ff.; *Ebbinghaus*, HRRS 1/2023,16, 19 f.; SK-StGB/*Stein/Greco* §129 StGB Rn. 27.

69 BT DS 18/11275 S.10; wie aus § 98 I Nr. 6 StPO hervorgeht, weißt auch eine Bande ein organisatorisches Element auf, vgl. *Ebbinghaus* HRRS 1/2023 16, 18f.

70 BGH NJW 2021, 2813, 2814f. st.Rspr., BGHSt 44, 68; BGHSt 54, 216; BGH 2 StR 353/18 Rn.33, juris.

71 Vgl. BGH NJW 2021 2813, 2816; BeckOK-StGB/*Kulhanek* (1.8.24) § 129 Rn.32.

72 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023): Von Dritten moderierte Dark-Net-Foren mit eigenen Streitschlichtungsverfahren, Nutzer-(=Affiliates) Bewertung etc.

73 BGH NJW 2021, 2813.

74 BGH NStZ 2022, 35.

sofern bestimmte Voraussetzungen gegeben sind (in erster Linie eine gut ausgeprägte Struktur).[75]

Doch wäre dies ein Zirkelschluss: Die Vereinigung bestünde, weil die Beteiligten als gemeinsames Interesse bezwecken, das Bestehen der Vereinigung zu gewährleisten. Für die Frage nach dem gemeinsam verfolgten Interesse kommt es aber darauf an, *warum* der Zusammenschluss erhalten werden soll. Auch wenn der BGH derart (miss-) verstanden wird, dass diese Selbsterhaltung ausreiche[76], kann dies nicht überzeugen. Es ist daher begrüßenswert, dass der BGH ein Jahr später, in der zweiten Hawala Entscheidung, hiervon etwas abgerückt ist.[77] Insofern ist auch hier nach dem „Warum" zu fragen, eine Frage, die unter Verweis auf den Selbsterhalt nicht beantwortet wird. Es ist zu klären, warum der Erhalt des Zusammenschlusses angestrebt wird, denn dies ist das gemeinsam verfolgte Interesse, welches Voraussetzung für die Einstufung als Vereinigung iSd § 129 II StGB ist.

Eine ausgeprägte Organisationsstruktur ist also ein starkes Indiz für ein übergeordnetes gemeinsames Interesse. Diese Indizwirkung kann aber widerlegt werden, wenn sich die ausgeprägte Organisationsstruktur anderweitig erklären lässt. Erfordern die von dem Zusammenschluss zu begehenden Vermögensstraftaten etwa eine besonders ausgeprägte Organisationsstruktur, kann diese dadurch erklärt werden, dass so die persönliche Bereicherung der Beteiligten gewährleistet werden soll. Die Indizwirkung der ausgeprägten Struktur für ein übergeordnetes gemeinsames Interesse kann so in dem konkreten Fall auch widerlegt werden. Nur solche, über dieses Maß hinausgehende Strukturen sind ein starkes Indiz, dass es ein übergeordnetes gemeinsames Interesse gibt, da ihre Existenz nicht anders zu erklären ist.

---

75 So zB BeckOK-StGB/*Kulhanek* (1.8.24) § 129 Rn. 32; *Nestler/Schiffner,* Anm. zu BGH NStZ 2022, 35, 38.

76 Nach *Ebbinghaus* differenziert der BGH zwischen der Vereinigung, die das Hawala System betreibt und dem Hawala System selbst. Somit sei der gemeinsam verfolgte Zweck nicht der Selbsterhalt der Vereinigung, sondern der Erhalt des (davon zu unterscheidendem) Hawala-Netzwerks. Auch nach diesem Verständnis bleibt die Entscheidung kritikwürdig, da der BGH es versäumt, die Frage zu beantworten, warum das Hawala System erhalten bleiben solle: reine Gewinnerzielungsabsicht oder ein darüberhinausgehendes Interesse, vgl. *Ebbinghaus* HRRS 1/2023 16, 19, insb. Fn. 42 m.w.N.

77 BGH 3 StR 403/20, HRRS 2022 Nr. 905: Rn.13 nennt Erhalt des Hawala Systems als gemeinsam verfolgten Zweck. Aber in Rn.15 führt BGH nun aus, dass es auch einen altruistischen Zweck gebe, welcher ebenfalls unterstützend heranzuziehen sei.

Dies gilt auch dann, wenn der Zusammenschluss vorgibt, nur wirtschaftliche Zwecke zu verfolgen. Ob die Organisationsstruktur bei Gruppen wie LockBit jedoch über das Maß hinausgeht, dass zur persönlichen Bereicherung der Beteiligten erforderlich ist, ist äußerst fraglich. Somit spricht nachdem bisher Ausgeführtem viel dafür, dass nach der deutschen Rechtslage es sich bei LockBit um Fälle der bandenmäßigen Erpressung oder des bandenmäßigen Betruges handeln würde (soweit es LockBit z.B. nicht möglich ist, die gehackten Daten ins Internet zu stellen), nicht jedoch um eine kriminelle Vereinigung, die u.a. auf Erpressung und Betrug ausgerichtet ist. Denn der gemeinsam verfolgte Zweck, bleibt, sowohl nach Willen des Gesetzgebers als auch nach der Rechtsprechung und herrschenden Meinung, das zentrale Element, um eine Abgrenzung von Bande und krimineller Vereinigung zu ermöglichen.[78]

Dennoch ist nicht völlig ausgeschlossen, dass der BGH, unter Bezugnahme auf die Gesetzesmaterialien[79], auch ein Gewinn und Machtstreben als ausreichend erachtet falls sich, wie bei LockBit oder vergleichbaren Ransomware-Gruppen eine Gruppenidentität gebildet hat, mit eigenem Willensbildungsprozess und Einflussnahme auf Öffentlichkeit. Wie der nächste Abschnitt zeigen wird, ist eine derartige Aufweichung des Tatbestandes nicht erforderlich.

4.3.1.2. Die „Marke“ als Lösung

An diesen grundsätzlichen dogmatischen Zweifeln an der Anwendbarkeit des § 129 StGB auf Ransomware-Gruppierungen wie LockBit, ändert die Existenz einer ‚Marke‘ nur den ersten Blick nichts. Diese ‚Marke‘ oder die Selbstdarstellung in der Öffentlichkeit kann als eine Notwendigkeit für die erfolgreiche Erpressung interpretiert werden: Dem Opfer wird so signalisiert, dass man sich auf die Täter verlassen kann, wenn bezahlt wird, wird alles gut, andernfalls werden die angedrohten Konsequenzen auch wirklich herbeigeführt.

Aber gerade diese Aufmerksamkeit in der Öffentlichkeit führt zu massiven Zahlungserschwerungen, durch internationale Sanktionen, gerade durch das US-amerikanischen Department of Justice, sodass sich ein offen-

78 BGH wistra 2021, 441, 444; BGH, Urteil vom 22. Mai 2019 – 2 StR 353/18 –, juris Rn. 33.

79 BT DS 18/11275, 11.

sives mediales Auftreten nicht allein aus finanziellen Gesichtspunkten erklären lässt. Daher ist es ist naheliegend, dass es auch um Aufmerksamkeit um ihrer selbst willen geht, gerade bei LockBit und dessen ‚Sprecher' LockBitSup[80] nach außen hin. So gesehen erklärt sich einerseits das Bedürfnis, unter einem bestimmten Namen in der Öffentlichkeit aufzutreten, welches es bei rein geheimdienstlichen Akteuren nicht gibt,[81] andererseits auch, dass die Namen selten gewechselt werden, nach zu aufsehenerregenden Taten.[82] Doch wird auch im Fall von internationalen Sanktionen an dem Bedürfnis, unter einer Marke aufzutreten, nicht aufgegeben. Somit lässt sich auch bei Zusammenschlüssen, die wie LockBit in ihrer Selbstdarstellung nur nach finanziellem Gewinn streben, ein gemeinsam verfolgtes Interesse in dem Bedürfnis nach Aufmerksamkeit sehen.

Freilich könnte man dies auch anders interpretieren: Die Aufmerksamkeit, auch wenn sie den unmittelbaren finanziellen Interessen eher schadet, dient (auch) der Rekrutierung von Talent, insb. Programmierern, LockBit veranstaltete im Juni 2020 ein Preisausschreiben für wissenschaftliche Aufsätze mit neuen Strategien für den Einsatz von Ransomware,[83] Probleme hier (insbesondere bei der Entwicklung der neusten LockBit Version), sollen, zusammen mit Ermittlungserfolgen, maßgeblich zu dem jüngsten Bedeutungsverlust von LockBit geführt haben.[84] Doch erfolgt die Rekrutierung über Darknet Foren, der mediale Auftritt außerhalb hiervon ist überzeugender mit einem Geltungsdrang zu erklären, als mit einer rein wirtschaftlichen Zweckverfolgung.

4.3.2. Nordkoreanische Gruppierungen

Gruppierungen aus Nordkorea (wie zB Lazarus) bezwecken in aller erster Linie die Beschaffung von finanziellen Mitteln für den international (nicht

80 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023).
81 Namen wie Lazarus für nordkoreanische Hacker-Gruppierungen sind von Sicherheitsunternehmen oder staatlichen Stellen vergeben worden.
82 Häufiger nach betrügerischem Umgang mit Affiliates: https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023), in Bezug auf REvil.
83 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023).
84 https://analyst1.com/ransomware-diaries-volume-3-lockbits-secrets/ (abgerufen am 27.08.2023).

mehr ganz so) isolierten Staat.[85] Der erste aufsehenerregende flächendeckende Ransomware-Angriff, WannaCry, soll von staatlichen nordkoreanischen Hackern (Lazarus) begangen worden sein.[86] Hier lässt sich das Bestehen einer kriminellen Vereinigung unproblematisch bejahen, da die Mittel dem Staat zugutekommen sollen, für den die Hacker arbeiten.[87] Somit scheint die persönliche Bereicherung der Mitglieder nicht das gemeinsame Interesse des Zusammenschlusses zu sein. Nordkoreanische Hacker sind im Bereich der Ransomware-Gruppierungen weniger stark präsent, traten jüngst als Affiliates auf.[88] Auch frei verfügbare Ransomware wie MAUI wird von nordkoreanischen Einheiten wie APT45 wohl nach wie vor eingesetzt,[89] wenngleich die öffentliche Aufmerksamkeit und die öffentlich bekannten Fallzahlen sind als bei russischsprachigen Ransomware-Gruppierungen.

Nordkoreanische Hackergruppen sind organisatorisch wohl entweder Teil des General Staff Department des Militärs oder des Reconnaissance General Bureau (RGB), erstere ist überwiegend in Sabotage und Informationsbeschaffung, letztere in illegaler Mittelbeschaffung durch Cyberkriminalität tätig,[90] öffentlich verfügbare Informationen sind hier spärlich. Im Bereich der illegalen Mittelbeschaffung ist der Cyberangriff auf die Bangladesch Central Bank am 4.2.2016 erwähnenswert: 10 Monate im System, um Abläufe kennen zu lernen, dann erfolgten Kontoabbuchungen über das

85 Oder auch um Cyberspionage zu finanzieren, vgl. https://cloud.google.com/blog/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage?hl=en (abgerufen am 31.03.2025).

86 https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-now-deploying-qilin-ransomware/;.s.o. Ausnutzung einer von der NSA entdeckten Schwachstelle (Tool, dass diese ausnutzte: EternalBlue) in Windows, welche die NSA aber geheim hielt, um diese Schwachstelle selbst ausnutzen zu können. Hacker(n) unter dem Namen ShadowBroker gelang es, dieses Tool zu stehlen, veröffentlichten es online. Anschließend wurde es für WannaCry von nordkoreanischen Hackern ausgenutzt und verbessert https://www.bleepingcomputer.com/news/security/one-year-after-wannacry-eternalblue-exploit-is-bigger-than-ever/; *Caesar*, The Incredible Rise of North Korea's Hacking Army, NewYorker, 19.04.2021.

87 *Caesar*, The Incredible Rise of North Korea's Hacking Army, NewYorker, 19.04.2021.

88 https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-now-deploying-qilin-ransomware/ (abgerufen am 23.03.2025).

89 https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine?hl=en (abgerufen am 31.03.25).

90 *Caesar*, The Incredible Rise of North Korea's Hacking Army, NewYorker, 19.04.2021; *Couretas*, Cyber Operations, 2024, S. 122f., demnach RGB dem GSD der Armee untergeordnet sei, iVa Mandiant.

SWIFT System bei Federal Reserve am 4.2.2016, iHv fast 1 Mrd. US-$, wenngleich aufgrund eines Zufalls nicht der vollständige Betrag transferiert wurde.[91] Bei der Infiltration der IT Systeme lukrativer Ziele wird raffiniert vorgegangen, beim Lesen der Vorgänge kann man sich einer gewissen Paranoia nicht erwehren.[92]

4.3.3. Chinesische Gruppierungen

Chinesische Gruppierungen sind im Bereich des Ransomware-Geschäfts eher seltener vertreten – hier scheint Wirtschafsspionage sowie die Vorbereitung eventueller Sabotageakte im Krisenfall im Vordergrund zu stehen, genau wie die mit dem russischen SVR in Verbindung gebrachte Gruppierungen sind chinesische Akteure eher advanced persistend threats (APT)[93]. Auch hier handelt es sich um semi-staatliche Akteure, vergleichbar mit den staatlichen Akteuren Nordkoreas. Informationen sind hier sogar für Mutmaßungen zu spärlich.

5. Fazit und Ausblick

Cyberkriminalität ist gut organisiert. Ein maßgeblicher Grund hierfür ist das Problem der Durchsetzung des staatlichen Strafanspruchs und -interesses,[94] da Landesgrenzen von Tätern überschritten werden: In Land A wird agiert, Taten werden aber zu Lasten von Land B begangen, mit

91 *Caesar*, The Incredible Rise of North Korea's Hacking Army, NewYorker, 19.04.2021, erfolgreich iHv 101 Mio US$; dies war kein Ransomware-Angriff, ausgeführt von BeagleBoyz/Bluenoroff, welche Teil von Lazarus seien, die wiederum eine Abteilung des RGB seien; *Couretas*, Cyber Operations, 2024, S. 124.

92 Lesenswert: *Caesar*, The Incredible Rise of North Korea's Hacking Army, NewYorker, 19.04.2021: Vorspielen eines Bewerbungsverfahren bei einem existierenden Unternehmen, einschließlich Videokonferenz-Interview mit Bewerber und Schauspieler, der dem CIO des Unternehmens ähnelte (& vorgab, dieser zu sein), um das Opfer dazu zu bringen, anschließend eine infizierte PDF Datei zu öffnen.

93 Nationalstate Ransomware S. 19; *Couretas*, Cyber Operations, 2024, S. 105f.

94 Sowie des staatlichen Gewaltmonopols allgemein: Siehe hierzu den folgenden Vorfall (eher ein Gerücht): LockBit führte einen Ransomware-Angriff gegen entrust.com aus, drohte mit der Veröffentlichung interner Daten. Daraufhin erfolgte ein DDoS-Angriff auf die von LockBit zur Veröffentlichung der Daten ihrer Opfer genutzten Server, mit der Nachricht: „DELETE_ENTRUSTCOM_MOTHERFUCKERS"; Quelle: https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023).

dem Land A keine engen Beziehungen unterhält. Daher ist es für die Strafverfolgungsbehörden von Land A keine große Priorität, den Aktivitäten Einhalt zu gebieten. Dies ermöglicht festere hierarchische Strukturen, da der Verfolgungsdruck geringer ist. Bei Entdeckung werden die Täter wohl nicht selten von den nationalen Geheimdiensten rekrutiert, um dann zum Erreichen politischer Ziele weiter zu agieren. Die Anwendung von § 129 StGB auf Ransomware-Gruppierungen erscheint auf den ersten Blick sehr naheliegend, doch wie gezeigt wurde, steht schon die Subsumtion vor einem erheblichen Begründungsaufwand. Auf der Grundlage öffentlich bekannter Informationen sind ideologische Ransomware-Gruppen, wie die nordkoreanische Lazarus Gruppe, die sogar in den staatlichen Militärapparat integriert ist, unproblematisch erfasst. Auch bei halbstaatlichen Gruppierungen wie EvilCorp spricht viel für die Bejahung einer kriminellen Vereinigung i.S.v. § 129 StGB. Organisationen wie LockBit propagieren eine reine Gewinnerzielungsabsicht. Die ausgeprägten Organisationsstrukturen können hier kein Indiz für ein gemeinsames Interesse darstellen, da sie notwendig sind für die Gewinnerzielung. Nur wenn der Grad an Organisation über das dafür erforderliche Maß hinausgeht, beziehungsweise nicht allein mit der Gewinnerzielungsabsicht erklären lässt, taugt es als Indiz für ein darüberhinausgehendes gemeinsames Interesse.

Doch zeigt das Auftreten in der Öffentlichkeit, dass es den Beteiligten maßgeblich auch um die Selbstdarstellung geht – in einem Umfang, wie es nicht allein für die Gewinnerzielung erforderlich zu sein scheint. Dies ist unserer Meinung nach ein entscheidendes Argument, mit dem auch nach dem ‚klassischen' (aber nach wie vor gültigen) Vereinigungsbegriff eine kriminelle Vereinigung bejaht werden kann. Dies ist natürlich aus öffentlich bekannten Informationen schwer einzuschätzen, aber bereits aus diesem begrenzten Fundus an Wissen zeigt sich, dass der BGH seine Rechtsprechung zur kriminellen Vereinigung nicht aufgeben müsste, wenn irgendwann einmal die faktischen Hindernisse, die einem Verfahren entgegenstehen, überwunden werden sollten.