ARGUMENTATION KOMPAKT

Ein Service der Hanns-Seidel-Stiftung für politische Entscheidungsträger

Hanns Seidel Stiftung

Ausgabe vom 23. November 2017 – 11/2017

Cybercrime

Kea-Sophie Stieber /// Das von Cybercrime ausgehende Gefährdungs- und Schadenspotenzial steigt. Die Politik muss die Voraussetzungen dafür schaffen, dass Strafverfolger der immer besser werdenden Möglichkeiten der Verschlüsselung und Verschleierung von Kommunikation im Internet nicht machtlos gegenüberstehen. Die Transnationalität der Straftaten erfordert eine intensive grenzüberschreitende Zusammenarbeit. Freiheit und Sicherheit stehen nicht in Konkurrenz zueinander. Vielmehr ist Sicherheit die Voraussetzung für Freiheit, ohne diese empfindlich zu beschneiden. ///

Cybercrime

Handlungsempfehlungen[1]

- Eine **effektive europaweite und internationale Zusammenarbeit** ist unabdingbar und eines der wichtigsten Instrumente. Diese muss weiter institutionalisiert werden und über gemeinsame Ermittlungsgruppen, Rechtshilfe und persönliche Kontakte hinausgehen. Insbesondere die bereits durch die Europäische Union und Cybercrime Konvention geschaffenen Voraussetzungen müssen genutzt und ausgebaut werden.
- Die **strafrechtliche Verantwortlichkeit für Techniker / Technik** muss definiert und normiert werden. Hier stellen sich ähnliche Probleme wie beim autonomen Fahren oder anderen selbstständigen Prozessen. Besonders diffizil wird die Haftung bei sogenannten **semiautonomen Bots**, die lernfähig sind und sich eigenständig über die originäre Technik hinaus entwickeln.
- Die **Zusammenarbeit von Wirtschaft und Sicherheitsbehörden** braucht einen eindeutigen Rechtsrahmen. Hierzu gehört auch die Balance zwischen Innovationspotenzial und Kriminalitätsrisiko neuer Technologien.
- **Spezialwissen und Erfahrung** sind der Schlüssel zu einer erfolgreichen Bekämpfung von Cybercrime. Eine Spezialisierung und Fortbildung auf polizeilicher und justizieller Ebene versetzt die Verfolgungsbehörden in die Lage, **effizienter und schneller** zu reagieren. Hierzu gehört auch eine umfassende Ausstattung mit entsprechend aktueller IT.
- Um durch die immensen Datenmengen nicht die Ermittlungen unmöglich zu machen, muss die Entwicklung **künstlicher Intelligenz** zur Auswertung von Daten weiter voranschreiten. Auch hierfür bedarf es eines Rechtsrahmens.
- Die **Zentralstelle Cybercrime** Bayern ist ein absolutes Positivbeispiel und wichtiger Schritt für die nachhaltige Bekämpfung entsprechender Straftaten. Die weitere **Unterstützung politischer, finanzieller, technischer und personeller Natur** ist unumgänglich.
- In vielerlei Hinsicht kann es sinnvoll sein, einen **Vergleich zur analogen Welt** zu ziehen – sowohl im Rahmen der analogen Anwendung der StPO als auch ermittlungstaktisch. Es muss immer ein Fehler des Täters vorliegen, um ihn überführen zu können.
- Die Politik muss die Voraussetzungen dafür schaffen, dass Strafverfolger der immer besser werdenden Möglichkeiten der **Verschlüsselung und Verschleierung von Kommunikation im Internet nicht machtlos gegenüberstehen**. Lange Gesetzgebungsprozesse müssen abgekürzt werden, die Behörden müssen mit dem aktuellen Stand der Technik ausgestattet sein.
- Bürger und Wirtschaft müssen im Mittelpunkt stehen.
- Der Gesetzgeber muss die **Diskrepanz** zwischen Gewährleistung von **Datensicherheit und den neuen, umfassenden Ermittlungsmethoden** gegen Straftäter der digitalen Welt überwinden bzw. lösen. Die parlamentarische Verantwortlichkeit für Eingriffe in Digitalgrundrechte kann für wesentliche Entscheidungen nicht verlagert werden.

Einführung

Die **globale Vernetzung** über das Internet bringt **enorme Vorteile** für Politik, Wirtschaft und Gesellschaft durch **sekundenschnelle Kommunikation**, Handel und Information. Gleichzeitig birgt diese Entwicklung negative Begleiterscheinungen durch vielfältige **Angriffsflächen**. Die Digitalisierung aller Lebensbereiche stellt den Rechtsstaat vor enorme Herausforderungen. Das Voranschreiten ist jedoch nicht mehr aufzuhalten, so dass das Recht auf allen Ebenen hieran angepasst werden muss. Ein essenzieller Aspekt davon ist die Sicherheit des Einzelnen und der Wirtschaft.

Bayern hat hier bereits eine wegweisende Institution etabliert. Die 2015 eingerichtete Zentralstelle Cybercrime ist bayernweit zuständig für die Bearbeitung **herausgehobener Ermittlungsverfahren** im Bereich der Cyberkriminalität und ist dafür **hochspezialisiert**. Sie ermittelt in Zusammenarbeit mit den entsprechenden Spezialisten der bayerischen Polizei oder des Bundeskriminalamts und mit internationalen Partnern z. B. bei Angriffen auf bedeutende Wirtschaftszweige oder bei Verfahren aus dem Bereich der organisierten Cyberkriminalität.

Kriminalitätslage und Straftaten

Cybercrime umfasst Straftaten, die sich **gegen informationstechnische Systeme** wenden oder mittels derer begangen werden. Der Begriff schließt somit sämtliche Delikte ein, die in **Zusammenhang mit dem Internet** stehen. Die Anzahl dieser Delikte lag im Jahr 2016 bei 82.649 und ist damit im letzten Jahr um 80,5 % gestiegen. Um ein Vielfaches höher ist jedoch das Dunkelfeld, also die Zahl der Cybercrime-Straftaten, die polizeilich nicht erfasst werden. Eine realistische Schätzung ist laut BKA nicht möglich.

Die maßgeblichen Beweggründe, eine Straftat über das Internet zu begehen, lassen sich etwa in drei Blöcke unterteilen

- die Veranlassung von Zahlungen oder Transaktionen (beispielsweise durch das Abfangen von Daten, Täuschung, Erpressung und ähnlichen Delikten)
- die Verbreitung unwahrer oder gefälschter Informationen
- die Nutzung des (hauptsächlich Dark-) Internets per se, um verbotene Dienstleistungen oder Waren zu vertreiben

Maßgeblicher Nutzen für die Täter bei diesen Delikten ist die Anonymität, die das Internet in vielen Fällen noch gewährleistet.

Typische Cybercrime-Delikte sind

- Ausspähen und Abfangen von Daten, §§ 202a, 202b StGB: Der sog. Informationsdiebstahl (Phishing) über gefälschte E-Mails oder Websites erfasst den „Diebstahl“ digitaler Identitäten, Zahlungsmittel etc.
- Computerbetrug, § 263a StGb: erfasst insbesondere die Verwertung des Phishing
- Datenveränderung / Computersabotage, § 303 b StGB
- Identitätsdiebstahl / Täuschung im Rechtsverkehr
- Computerviren
- Kinderpornographie

- Menschenhandel
- Cybermobbing / Fake News
- Installation von Ransomware, die den PC sperrt, um Lösegeld für eine Entsperrung zu erpressen

Täter

Das Spektrum der Täterstruktur reicht vom klassischen Einzeltäter bis hin zu organisierten internationalen Tätergruppierungen, die die Anonymität des Internets auch untereinander nutzen. Fast drei Viertel der registrierten Delikte wird von **unter 50-Jährigen** begangen. Es handelt sich zunehmend jedoch nicht mehr ausschließlich um Täter mit fundierten IT-Kenntnissen. Es hat sich mittlerweile ein eigener Kriminalitätsstrang etabliert, Software, die zur Ausübung verschiedenster Internet- und Kommunikationsstraftaten benötigt wird, gebrauchsfertig anzubieten **(„crime as a service")**. Dadurch haben auch Täter **ohne umfassende IT-Kenntnisse** die Möglichkeit, solche Straftaten mit verhältnismäßig geringem Aufwand und eigenem Know-how zu begehen.

Schutzmöglichkeiten

Ein hundertprozentiger Schutz vor Straftaten aus dem Internet kann ebenso wenig gewährleistet werden wie vor solchen in der analogen Welt. Durch **technische Vorkehrungen** wie Antivirenprogramme, Browsereinstellungen, Firewalls und Verschlüsselungen kann bereits eine Vielzahl von Sabotageangriffen abgefangen werden. Hinzukommen muss jedoch unbedingt die **persönliche Sensibilisierung** sowohl im Privaten als auch im Arbeitsumfeld. Essenziell hierbei ist die Einrichtung sicherer Passwörter, keine suspekten Anhänge zu öffnen sowie das kritische Prüfen und Hinterfragen, bevor Links oder Pop-ups angeklickt werden.

Problemfelder

Fälle von Cybercrime beinhalten oftmals überdurchschnittliche **komplexe technische und rechtliche Probleme**. Das Gefahrenpotenzial steigt durch zunehmende Internetnutzung und Etablierung des „Internet der Dinge". Das Fortschreiten der Technik unterliegt einem **steten Wandel**, dem der **Gesetzgeber bisher nicht zufriedenstellend begegnen** konnte. Ein erster Erfolg ist die Einführung der Quellen-Telekommunikationsüberwachung (Quellen- TKÜ), die die Möglichkeit geschaffen hat, bei schweren Straftaten auch verschlüsselte Kommunikation via WhatsApp und Skype zu überwachen.

Folgende Problemfelder sind besonders präsent

- Das Recht bezieht sich in vielerlei Hinsicht noch auf analoge Prozesse. Eine **umfassende Aktualisierung des StGB sowie der StPO** sind dringend erforderlich. Aufgrund des Bestimmtheitsgrundsatzes im Straf-/ Strafprozessrecht kann nur punktuell (und meist verspätet) auf neue Entwicklungen reagiert werden. Es gibt beispielsweise noch keine Norm, die spezifisch die Beschlagnahme eines Email-Postfaches regelt. Auch bei anderen Ermittlungstechniken muss immer wieder im Einzelfall geklärt werden, ob diese unter bestehende Eingriffsnormen der StPO gefasst werden können (z. B. IP-Tracking, WLAN Tracking, Network mapping).

- Zu den größten tatsächlichen Herausforderungen gehören die exorbitant **großen Datenmengen**, die auf potenzieller Täter-Hardware existieren. Die gängige Festplattengröße lässt es zu, eine Vielzahl an Daten zu speichern (derzeit bis zu 14 TB pro Festplatte). Deren **Auswertung** ist bereits personell und zeitlich nicht zu bewerkstelligen. Zudem bieten „unwichtige" Datensätze häufig ein gutes Versteck für relevante Inhalte.
- Das **Dunkelfeld** der Cyberkriminalität ist sehr hoch: Unternehmen befürchten wirtschaftliche Einbußen, wenn sie Cyberattacken anzeigen. Auch Sexualdelikte werden der Polizei nur verhalten zur Kenntnis gebracht.
- Erhebliche tatsächliche und rechtliche Probleme treten bei Ermittlungen im **Darknet** auf. Gerade hier wird jedoch eine Vielzahl an Straftaten begangen bzw. hat ihren Ursprung. Wird das Tornetz korrekt verwendet, ermöglicht es eine **umfassende Anonymisierung**. Werden sog. Tails genutzt, werden auch keine Spuren auf dem eigenen Rechner hinterlassen. Der physische Datenstandort ist meist nicht ermittelbar. Auf rechtlicher Ebene ergeben sich hier Hindernisse im Rahmen des **Legalitätsprinzips** beispielsweise bei der Nutzung von Exploits sowie Zugriffen auf den Server selbst.
- Vor ebenfalls große Herausforderungen werden Staat und Ermittlungsbehörden in Sachen **Datensicherheit und Privatsphärenschutz** gestellt. Sie dienen sowohl dem Schutz des Bürgers als auch der Wirtschaft und genießen Grundrechtsschutz, dürfen aber gleichzeitig nicht dem Schutz von Straftätern dienen und Ermittlungsarbeit behindern. Die Notwendigkeit der sicheren Kommunikation in Regierungsangelegenheiten, Unternehmensgeheimnissen und dem Schutz der Privatsphäre steht die ebenfalls zunehmend ausgefeilte Verschlüsselung von Täterkommunikation gegenüber.
- Ein tatsächliches Hemmnis ist dabei auch, dass **Beweismittel** oft nur für kurze Zeit zur Verfügung stehen, da sie schnell gelöscht werden können.
- **Internationale Vernetzung: Die Grenzenlosigkeit des Datenverkehrs** führt dazu, dass nahezu alle Cybercrime-Ermittlungen **internationale Berührungspunkte** haben. Beispielsweise operieren Täter aus dem Ausland oder die Server stehen dort. Auch die Tatmuster betreffen oft Geschädigte in mehreren Ländern. Der in Art. 2 der UN-Satzung garantierte traditionelle Grundsatz der Nichteinmischung soll dem Schutz der Souveränität von Staaten dienen und kann somit internationalen Ermittlungen entgegenstehen. Die internationale Vernetzung in diesem Bereich ist noch nicht ausreichend etabliert.

Fazit

Die neuen und disruptiven Technologien ermöglichen neue Kriminalitätsformen und Begehungsweisen. Eine Anpassung des Rechts und der Verfolgungspraxis ist dringend notwendig. Die Herausforderung liegt darin, die Angst vor Kontrollverlust des Staates einerseits und die vor einem Überwachungsstaat auszubalancieren. Dabei darf jedoch nicht aus dem Fokus geraten, dass jede Art der Strafverfolgung in die Freiheitsrechte der Bürger eingreift – auch auf analoger Ebene. Der Staat darf sich jedoch nicht in seinen Ermittlungen selbst lähmen. Noch ist in vielen Fällen Eigenschutz der beste Schutz. Jeder Einzelne kann durch passende technische Schutzmechanismen eine wichtige Basis schaffen.

Anmerkung

[1] Der Oktober ist der „Europäische Monat der Cybersicherheit“. Es handelt sich dabei um eine Unterstützungskampagne der EU, die jedes Jahr im Oktober stattfindet. Sie zielt darauf ab, das Bewusstsein der Gefahren für die Cybersicherheit in der Bevölkerung zu fördern und durch Bildung sowie bewährte Praktiken aktuelle Sicherheitsinformationen anzubieten. Die Hanns-Seidel-Stiftung hat in diesem Rahmen ein Rechtspolitisches Symposium mit Experten aus Recht, Politik und Praxis zu der Thematik durchgeführt. Aus diesem sind die Thesen und Handlungsempfehlungen dieses Papiers erwachsen.

Weitere Informationen und Quellen

https://www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/bamberg/spezial_1.php

https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyberkriminalitaet-node.html

https://www.polizei.bayern.de/lka/kriminalitaet/internet/index.html/329

https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html

https://de.statista.com/themen/1834/internetkriminalitaet/

https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html

https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html

Autorin

Ass. jur. Kea-Sophie Stieber
ist Referentin für Recht und Verfassung, Europäische Integration der Akademie für Politik und Zeitgeschehen, Hanns-Seidel-Stiftung, München.

Impressum: Hanns-Seidel-Stiftung e.V., Lazarettstraße 33, 80636 München
Vorsitzende: Prof. Ursula Männle, Staatsministerin a. D.; Generalsekretär: Dr. Peter Witterauf