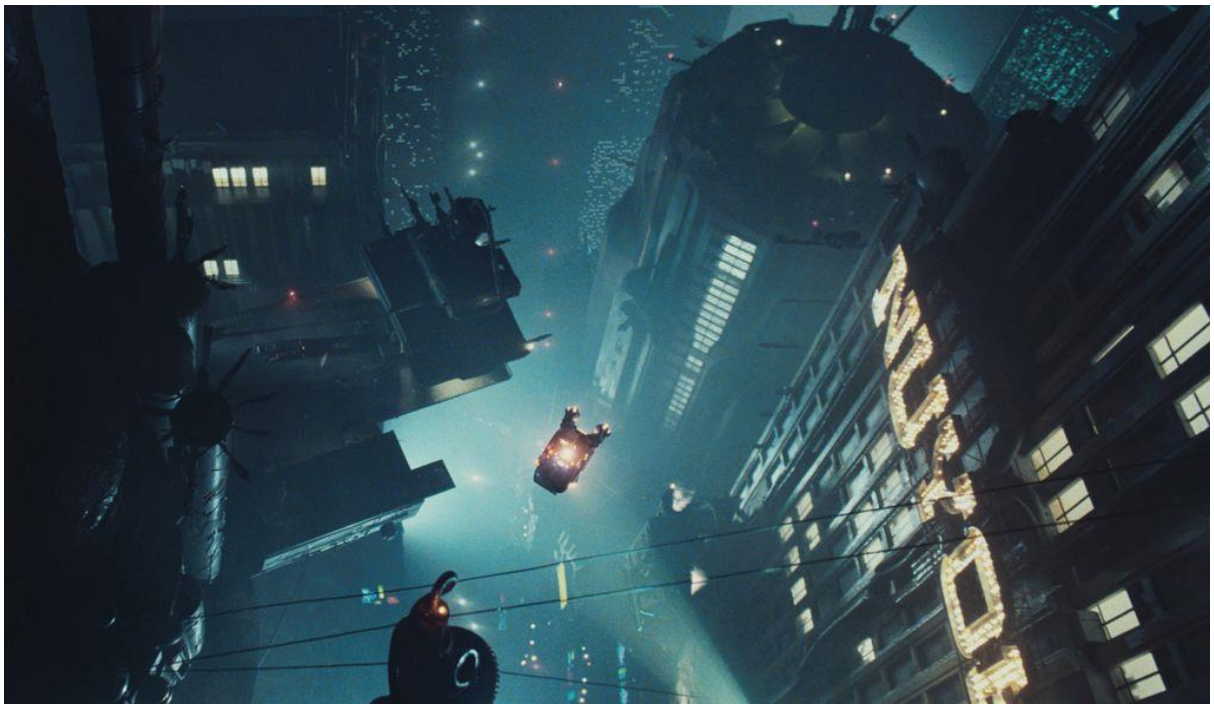
Frankfurter Allgemeine
Einspruch
Alles was Recht ist
HERAUSGEGEBEN VON WERNER D'INKA, JÜRGEN KAUBE, BERTHOLD KOHLER, HOLGER STELTZNER

Cyberkriminalität

Im dunklen Teil des Internets

Justiz und Sicherheitsbehörden stehen am Anfang eines neuen Zeitalters

Von Rüdiger Soldt



© Fototex, Szene aus dem Film "Bladerunner: Final Cut" von 1982

TRIBERG, 10. Dezember. Das Internet stellt Richter, Anwälte, Staatsanwälte und Polizei wahrscheinlich vor die größte Herausforderung seit der Einführung des modernen Strafrechts. Das gilt für die Praxis der Strafverfolgung etwa bei der Bekämpfung des illegalen Waffenhandels im „dark net“, aber ebenso für systematische und rechtsphilosophische Fragen. Wenn beispielsweise das „autonome Fahren“ eines Tages Realität ist, werden Staatsanwälte und Richter die Schuldfrage nicht mehr allein an einer Person, dem Autofahrer, festmachen

können. „Wild West im Web – aktuelle Herausforderungen für die Sicherheit im Internet“ hat der baden-württembergische Justizminister Guido Wolf (CDU) das „38. Triberger Symposium“ zu aktuellen Fragen der Rechtspolitik genannt.

So sagte Bettina Limperg, die Präsidentin des Bundesgerichtshofs (BGH): „Wir müssen uns mit neuen Beweismitteln wie der DashCams im Straßenverkehr beschäftigen. Die Zunahme des Internethandels setzt den Handel unter Druck, sie führt auch zu einem Rückgang der Zivilverfahren. Auch die Frage, ob die Aufgaben eines Richters oder eines Staatsanwalts mit einem gut gefütterten Algorithmus nicht sogar besser zu lösen sind, stellt sich ja schon.“ Sie skizzierte damit die Spannweite der Fragestellungen, die die Digitalisierung für die Justiz aufwirft.

Derzeit ist weniger von politischer Bedeutung, ob Algorithmen bald besser sind als leibhaftige Anwälte. Es ist vielmehr die Frage, was der Staat tun muss, um einerseits die zunehmende Internetkriminalität zu bekämpfen und andererseits Institutionen und Unternehmen vor Cyberattacken zu schützen.

Uwe Siegrist von der Schwerpunktstaatsanwaltschaft zur Bekämpfung von Informations- und Kommunikationskriminalität in Mannheim gab einen Einblick in die Schwierigkeiten bei der Strafverfolgung im „dark net“. Jeden Tag nutzen zwei Millionen Menschen diesen „dunklen Teil“ des Internets, allein in Deutschland gibt es 1500 „dark net“-Server. Die Kommunikation erfolgt völlig anonym, Kriminalbeamte und Staatsanwälte können nicht auf „IP-Adressen“ zurückgreifen, um zu ermitteln, wer eine Waffe gekauft oder verkauft hat. Jede Kommunikation wird über drei Server umgeleitet, damit sie nicht nachzuverfolgen ist. 57 Prozent der Seiten im „Tor-Darknet“ haben heute eindeutig illegale Inhalte: Angeboten werden Waffen, Kreditkartendaten, Drogen und illegale Computerprogramme. Die Strafverfolgung ist äußerst kompliziert.

Aber das „dark net“ kann auch von Oppositionsbewegungen in Diktaturen zur Information genutzt werden. Journalisten und einige Zeitungen sind wiederum dankbar für die Möglichkeiten, die das „dark net“ bietet, denn in Zeiten des Datenjournalismus ist es für Informanten eine ideale geheime Plattform zur Hinterlegung großer Datenmengen. Eine Verfolgung der Straftaten ist vor allem eine Frage der personellen und technischen Ausstattung der Staatsanwaltschaften.

Auf der Tagung waren sich die meisten Fachleute einig, dass im Strafgesetzbuch eher kleine Anpassungen notwendig sind, um die wachsende Internetkriminalität effizient zu bekämpfen. Jörg Eisele, Strafrechtsprofessor an der Universität Tübingen, erinnerte daran, dass schon 1986 wichtige Strafnormen eingeführt worden seien, etwa mit dem zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität. Die Digitalisierung von Wirtschaft und Gesellschaft führe aber unweigerlich zu einem stetigen Anstieg der Computerdelikte. Die Zahl der Verurteilungen sei immer noch recht niedrig: So wurden 2015 zum Beispiel 9629 „Straftaten des Ausspähens und Abfangens“ registriert, es gab aber nur 46 Verurteilungen. Bei den Delikten „Datenveränderung und Computersabotage“ erfasst die Kriminalitätsstatistik 3537 Straftaten, verfolgt wurden lediglich 34 Fälle. In einem wird nach dem „Bundeslagebild Cybercrime“ jeder zweite private Computernutzer und jedes fünfte Unternehmen Opfer eines Cyberangriffs. Etwa 250 000 Fälle von Cyberkriminalität gibt es, die mit dem Tatmittel Internet begangen werden, in 70 Prozent der Fälle handelt es sich um Computerbetrug.

Eisele sieht gesetzgeberischen Handlungsbedarf weniger bei den schon seit Mitte der achtziger Jahre normierten Straftaten wie dem „Computerbetrug“ oder der „Fälschung beweiserheblicher

Daten“, eher bei Straftatbeständen, mit denen das Verbreiten illegaler Inhalte verhindert werden soll, etwa von Kinderpornographie. Hier müsste nach Auffassung Eiseles der Paragraph 11, Absatz 3 des Strafgesetzbuches um den Begriff „Daten“ ergänzt werden, so dass das Speichermedium nicht mehr das entscheidende Kriterium für eine erfolgreiche Strafverfolgung sei. Eisele hält es für notwendig, das gesamte Strafgesetzbuch durchzugehen, damit die Verbreitung von illegalen Schriften tatsächlich unabhängig vom Medium, auf dem sie gespeichert sind, verfolgt werden kann. Der Strafrechtler hält auch einen Straftatbestand „digitaler Hausfriedensbruch“ für diskutabel, um etwa „Pishing-Attacken“ auf Bankkonten abzuwehren. Ein erster im Bundesrat diskutierter Gesetzentwurf sei zu weitgehend gewesen, weil er neben der „unbefugten“ auch die „ungefragte Benutzung“ unter Strafe gestellt habe. Ausschlaggebend für eine solche Strafnorm müsse der „Schädigungszweck“ oder die „Schädigungsneigung“ sein. Ansonsten sei nämlich die ungefragte Benutzung eines digital gesteuerten Rasenmähers strafbar, so Eisele.

Justiz, Politik und Sicherheitsdienste stehen noch am Anfang eines neuen Zeitalters. Die „Zentrale Stelle für Informationstechnik“ (Zitis) in München wurde erst in diesem Jahr vom Bundesinnenministerium als Dienstleister vor allem zur Verbesserung der „digitalen Forensik“ gegründet, damit die Sicherheitsbehörden (BND, Bundespolizei, Verfassungsschutz) die nötigen technischen Ermittlungsmittel an die Hand bekommen. Die in München ansässige Behörde soll bis 2024 etwa 400 Mitarbeiter haben. Eine noch nicht abschließend geklärte Frage ist, ob der Staat Software-Sicherheitslücken auch nutzen soll, ob er im „Cyberkrieg“ auch aktiv tätig werden darf, um Schlimmeres zu verhüten. BGH-Präsidentin Bettina Limperg war sich angesichts der vielfältigen Herausforderungen in einem Punkt ziemlich sicher: „Die Digitalisierung geht nicht mehr weg.“