**Angela Giger*/Marvin Stark**/ Vivian Stein*****

# 11. Zürcher Präventionsforum

### Neue Technologien im Dienste der Prävention: Möglichkeiten – Risiken

## I. Einleitung

Der technische Fortschritt schafft neue Gelegenheiten für Kriminalität. Man denke nur an Hacking, Trojanische Pferde und andere Schadsoftware oder Miniwanzen zur Überwachung und illegalen Aufzeichnung von Bild und Ton. Technik ist aber auch ein Hilfsmittel für die Kriminalprävention. Bauliche Massnahmen an Gebäuden, Videoinstallationen im öffentlichen Verkehr, automatisierte Suchläufe im Internet, Drohnen, elektronische Fussfesseln und Apps auf Mobiltelefonen: Sie alle können zur Verhinderung von Straftaten und zur Beweissicherung eingesetzt werden. Analyse-Tools mit Zugriff auf eine Vielzahl an Daten ermöglichen zudem Prognosen über die Kriminalitätsentwicklung. Auch Software mit künstlicher Intelligenz wird in der Kriminalprävention zum Einsatz kommen. Technische Massnahmen sind also wesentlicher Bestandteil der Prävention auf allen Ebenen. Unter der Leitung von Prof. Dr. Christian Schwarzenegger, Professor für Strafrecht, Strafprozessrecht und Kriminologie an der Universität Zürich, und Hauptmann Rolf Nägeli, Chef des Kommissariats Prävention der Stadtpolizei Zürich, setzte sich das 11. Zürcher Präventionsforum zum Ziel, über den Stand der Präventionsmassnahmen im Bereich technische Innovationen und Prävention zu informieren und beste Praktiken aufzuzeigen. Damit bot die diesjährige Tagung einen Überblick über neueste Entwicklungen und Forschung zur Wirksamkeit technischer Kriminalprävention und ermöglichte durch das Zusammenbringen von Expertinnen, Experten und Interessierten aus den Bereichen Polizei, Justiz, Stadtverwaltung, Sicherheit, Soziales, Forschung, Technik und Politik einen breiten Informationsaustausch zwischen Theorie und Praxis.

## II. Technik in der polizeilichen Präventionsarbeit

Nach der Forumseröffnung durch Oberstleutnant Daniel Blumer, Rechtsanwalt und Kommandant der Stadtpolizei Zürich, gaben Ladina Cavelti, wissenschaftliche Mitarbeiterin am Kriminologischen Institut der Universität, und Prof. Dr. Christian Schwarzenegger einen Überblick zur Kriminalprävention durch technische Massnahmen und deren Entwicklungstendenzen. Obwohl Technologie positiv wahrgenommen und in der Kriminalprävention (z.B. im Einbruchschutz) erfolgreich eingesetzt wird, hat sie auch ihre negative Seite. Dies wurde am Beispiel der umfassenden Überwachung der Uiguren in China veranschaulicht, die u.a. eine flächendeckende Kontrolle durch Überwachungskameras und GPS-Sender in allen Autos und Bussen umfasst. Technologie ist folglich ein Dual-Use-Instrument.[1] Technische Entwicklungen schaffen immer neue Möglichkeiten für die Kriminalprävention und finden in verschiedensten Bereichen Anwendung, die von Pre Crime Observation Systems (Precobs)[2] und Crime Mapping in der Polizeiarbeit[3] bis hin zur elektronischen Warensicherung im Detailhandel reichen. Sie sollen den Täter durch Einwirkung auf sein rationales Kalkül beeinflussen. Verschiedene Faktoren schränken jedoch die Wirksamkeit der Massnahmen ein. Diese können auf der Seite des Menschen (z.B. des selten rational handelnden Täters) oder auf technischer Seite liegen. Videoüberwachungssysteme (CCTV)[4] als «klassische» technische Massnahmen haben im deutschsprachigen Raum keine präventive Wirkung. Ebenso wenig sind sie mit einer Erhöhung des allgemeinen Sicherheitsgefühls verbunden. Ähnliche Resultate ergab das Review von 44 Studien, die schwerpunktmässig in Grossbritannien durchgeführt wurden. Im polizeilichen Bereich finden z.B. Precobs und Software, die musterbasiert Kriminalitätsprognosen für ein bestimmtes Gebiet stellen, Anwendung. Einen Einblick in die neue Welt der Kriminalprävention und Polizeiarbeit mittels technischer Massnahmen ermöglicht ein Blick nach China, wo es mit einem Netzwerk von Überwachungskameras möglich ist, eine Person innert sieben Minuten zu lokalisieren oder ihre mit anderen (Personen-)Daten zu verknüpfen, was mit einem Videoausschnitt[5] veranschaulicht wurde. Dadurch sei die Kriminalitätsrate in China äusserst niedrig. Mit der wachsenden Bedeutung von Cybercrime nimmt die Bedeutung technischer Präventionsmassnahmen zu. Sie können eine drastische Verbesserung der Effizienz und Wirksamkeit des Strafrechtssystems bewirken, doch ergeben sich auch neue Probleme: Es entsteht eine Abhängigkeit von komplizierter Technik, die u.U. nicht mehr selbst bedient werden kann. Zudem hängt die erfolgreiche Anwendung von der Qualität der vorhandenen Daten ab, woraus die Gefahr einer Auslagerung der Präventionsarbeit auf Private entsteht (z.B. Facebook), zumal diese teils im Besitz von aussagekräftigeren Daten sind. Mit Technik ist heutzutage vieles möglich, aber mittels der Frage nach der

* MLaw, wissenschaftliche Assistentin und Doktorandin am Lehrstuhl von Prof. Dr. Christian Schwarzenegger für Strafrecht, Strafprozessrecht und Kriminologie, Universität Zürich.
** Wissenschaftlicher Hilfsassistent am Lehrstuhl von Prof. Dr. Christian Schwarzenegger für Strafrecht, Strafprozessrecht und Kriminologie, Universität Zürich.
*** Wissenschaftliche Hilfsassistentin am Lehrstuhl von Prof. Dr. Christian Schwarzenegger für Strafrecht, Strafprozessrecht und Kriminologie, Universität Zürich.

1 Im Sinne des doppelten Verwendungszwecks mit sowohl positiver als auch negativer Wirkung.
2 Software zur Kriminalitätsprognose.
3 Verbrechenskartierung der Verbrechen-Hotspots (Zusammenstellung, Darstellung und Analyse von Verbrechensmustern).
4 Closed Circuit Television.
5 «In Your Face – China's All-Seeing State» (<https://www.youtube.com/watch?v=pNf4-d6fDoY>).

richtigen Balance müssen Auswüchse unterbunden werden. Es ist deshalb erforderlich, dass der Gesetzgeber die normativen Einschränkungen der Rechte der Betroffenen neu definiert.

Das Thema der polizeilichen Kriminalprävention abgerundet hat Dr. Ulrich Schimpel, Federal CTO bei IBM Schweiz und Mitglied bei IBM CTO Europe Team, mit seinem Referat über die künstliche Intelligenz zur Unterstützung der erfolgreichen polizeilichen Präventionsarbeit. Einleitend erklärte er, dass sich die aktuellen Systeme mit der Verarbeitung von unstrukturierten Daten sehr schwertun. Solche Daten ohne formalisierte Struktur (z.B. Texte in natürlicher Sprache, Tonaufnahmen, Bilder und Videos) machen aber den Grossteil heutiger Daten aus. Daher braucht es Systeme zur Massenverarbeitung. Hier kommen die wissensbasierten Systeme mit künstlicher Intelligenz ins Spiel. Während die meisten herkömmlichen Systeme nur auf Befehle reagieren können, ohne eine Erklärung dafür zu haben, können wissensbasierte Systeme erklären, wieso sie auf eine bestimmte Lösung gekommen sind. Ermöglicht wird dies, indem das System sowohl strukturierte als auch unstrukturierte Daten sammelt und in einem Wissens-Graph miteinander verbindet. In einem Feedback-Loop werden ausserdem Lösungen ins System zurückgeführt, um neue Zusammenhänge zu schaffen. Es ist auch wichtig, das System bei der Entwicklung gezielt mit einschlägigem Expertenwissen zu füllen; im Bereich der Präventionsarbeit etwa mit forensischen Geschichten und Videos. Geht ein ermittlungsrelevanter Text ins System ein, erkennt dieses Schlüsselwörter, ordnet sie einer Kategorie zu und versteht deshalb Zusammenhänge und den Satz als Ganzes. Im Anschluss wird mit dem System so lange ein Dialog geführt, bis dieses aufgrund der Informationen eine Lösung vorschlagen kann. Stösst es auf Probleme, wird automatisch ein Chat erstellt, in welchem ihm die Experten Fragen stellen und falls nötig weitere Informationen zukommen lassen. Weiterführend erläuterte Schimpel, in welchen Bereichen wissensbasierte Systeme eingesetzt werden. In Manchester, wo der Heroin-Konsum sehr verbreitet ist, konnte damit relativ einfach vorhergesagt werden, wo sich der nächste Hotspot bilden wird. Dasselbe System wird nun auch für die Vorhersage genutzt, in welchen Gebieten die nächsten Fahrraddiebstähle oder Raubüberfälle stattfinden werden. Im Vereinigten Königreich wird ausserdem ein wissensbasiertes System verwendet, um das Risiko einzuschätzen, ob Kinder kriminellen Gruppen beitreten. Hierfür wurden riesige Mengen an relevanten Daten aus Schulen, Sozialarbeit und Rapports über solche Gruppen in den Wissens-Graph des Systems eingeschleust. Dadurch konnte u.a. festgestellt werden, dass es bestimmte Lebensabschnitte im Leben von Kindern gibt, in denen sie besonders dafür anfällig sind, kriminell ausgebeutet zu werden. In einem von der EU mitbegründeten Projekt (PROTON) geht es ferner darum, die Gefahr von Terrorismus und organisierter Kriminalität anhand des Cyberverhaltens zu erkennen. Ziel ist es, herauszufinden, wo rekrutiert wird, damit gegebenenfalls frühzeitig eingegriffen werden kann. Ob durch den Einbezug künstlicher Intelligenz alle Probleme der Präventionsarbeit gelöst werden, liess Schimpel das Publikum aber kritisch hinterfragen. Als Beispiel für eine sehr weitgehende Verflechtung von Mensch und Maschine im Bereich der Prävention nannte auch er die Videoüberwachung und das Punktesystem in China. Erwähnenswert sind ferner die von einigen amerikanischen Richtern verwendeten Systeme, die anhand von Algorithmen das Strafmass berechnen und dabei die Gefahr von Wiederholungstaten miteinbeziehen. Jeder Einzelne müsse sich die Frage stellen, was in unserer Gesellschaft noch akzeptiert werden könne. Maschinen sollten uns nicht ersetzen. Vielmehr soll die Zusammenarbeit von Mensch und Technologie das Ziel sein. Welches Wertesystem gewollt ist, darf aber nie Maschinen überlassen werden, denn hier sind wir ihnen noch weit überlegen.

## III. Technik im Straf(prozess)recht

Dr. Jasmine Stössel, ausserordentliche Staatsanwältin bei der Staatsanwaltschaft des Kantons Schaffhausen, referierte über die Verwendung von Electronic Monitoring (EM), das seit 1. Januar 2018 im Schweizer Erwachsenenstrafrecht normiert ist. Es gibt ein weites Spektrum an technischen Möglichkeiten zur Durchführung von EM, die von einer reinen (nachträglichen) Ab- und Anwesenheitskontrolle der überwachten Person an einem bestimmten Ort zu einer bestimmten Zeit durch Radiofrequenz-Technologie bis zu einer Echtzeitverfolgung des Überwachten mittels GPS reicht. Die Kontrolle erfolgt dabei über einen Sender, den die Person an einer manipulationssicheren Fussfessel trägt. Schwierigkeiten können sich bei der GPS-Überwachung an Orten ergeben, an denen der Satellitenempfang schlecht ist, da dadurch die Ortungsgenauigkeit negativ beeinträchtigt wird. Zur Behebung dieses Problems müssen verschiedene Netzwerke (Mobilfunk, WLAN oder eine Kombination von Radiofrequenz- und GPS-Überwachung) zur Ortung kombiniert werden. Da dabei viele Daten über die Person gesammelt werden, bedarf es aus Gründen des Datenschutzes einer gesetzlichen Regelung für deren Speicherung und Bearbeitung. Im *Strafprozess* kann EM seit 1. Januar 2011 als Ersatzmassnahme zur Untersuchungshaft genutzt werden.[6] Hier stehen v.a. technische Aspekte im Vordergrund, mittels derer eine Flucht- und eine Wiederholungsgefahr bei ortsspezifischen Delikten verhindert werden sollen. Im *Strafvollzug* wird EM hauptsächlich bei kurzen Freiheitsstrafen angewendet, um eine soziale und berufliche Desintegration zu verhindern (Front-Door-Variante).[7] Andererseits kann es am Ende der Verbüssung langer Freiheitsstrafen eingesetzt werden, um einen kontrollierten, individuellen Übergang zwischen offenem Vollzug und (bedingter) Entlassung zu ermöglichen, wobei die Funktion als Arbeits- und Sozialprogramm

[6] Art. 237 Abs. 3 Schweizerische Strafprozessordnung vom 5. Oktober 2007 (StPO), SR 312.0.

[7] Art. 79*b* Abs. 1 lit. a Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0.

im Vordergrund steht (Back-Door-Variante).[8] Vor der eidgenössischen Einführung seien in sieben Kantonen rund 250 Anwendungsfälle bekannt gewesen. Ferner ist EM seit 1. Januar 2015 zur Überprüfung von strafrechtlichen Kontakt- und Rayonverboten denkbar.[9] Auch im Rahmen *zivilrechtlicher Massnahmen* soll EM künftig zum Schutz vor häuslicher Gewalt angewendet werden.[10] Spezialpräventiv kann es durch die erhöhte Entdeckungsgefahr eines Verstosses gegen die Vollzugsbedingungen abschreckend wirken. Dieser Effekt nimmt jedoch mit Zeitablauf ab und setzt voraus, dass Vertrauen in die Verlässlichkeit der Technologie besteht. Von zentraler Bedeutung für eine nachhaltige und positive Verhaltensänderung ist vielmehr die Betreuung der überwachten Person. Zudem bietet EM selbst bei aktiver GPS-Überwachung keinen sicheren Schutz vor Straftaten, weshalb im Zweifelsfall von ihrer Anwendung abzusehen ist.

Thomas Wenk, Chef des Kompetenzzentrums Digitale Ermittlungsdienste der Stadtpolizei Zürich, klärte am Nachmittag über aktuelle Phänomene der digitalisierten Kriminalität und Cybercrime-Prävention auf. Zu Beginn hielt er begrifflich fest, dass Cybercrime bloss eine Teilmenge der digitalisierten Kriminalität umfasst. Während letztere jegliche Delikte beinhaltet, die unter Zuhilfenahme von Mitteln der Internettechnologie verübt werden, beinhaltet Cybercrime einzig Angriffe gegen Computersysteme. Auch die Täterschaft unterscheidet sich stark: Während die Täter bei der digitalisierten Kriminalität mehrheitlich lokal ansässige Personen oder solche mit lokalem Bezug sind, ist diejenige von Cybercrime oft in hohem Mass organisiert und operiert von verschiedenen Ländern aus. Zudem setzen die Täter regelmässig ermittlungserschwerende Technologien ein. Zur Bekämpfung von Cybercrime wären daher landes- und kontinentübergreifende Organisationen notwendig, die genauso global und flexibel handeln können wie die Gegenseite. Da heutzutage aber weder eine solche existiert noch die rechtlichen Grundlagen dazu bestehen, lohnt es sich nicht, vermehrt in die Bekämpfung von Cybercrime zu investieren. Vielmehr ist das einzige wirksame Mittel die Prävention. Man muss die Bevölkerung auf diese Art der Kriminalität sensibilisieren und Schutzmassnahmen gegen Cyberangriffe (z.B. Phishing[11] oder Malware[12]) aufzeigen. Praxisnah verdeutlichte Wenk anhand zwei realer Straffälle die Vorgehensweise der Stadtpolizei Zürich bei digitalisierter Kriminalität. Im ersten Fall klärte er darüber auf, dass es dank Algorithmen möglich ist, ein gesamtes Betriebssystem spezifisch auf verbotene Pornografie zu durchsuchen. Im vorliegenden Beispiel war aber letztlich nicht der beschuldigte Computer-Besitzer der Täter, sondern eine Drittperson, die ihm das verbotene Material ferngesteuert auf das Betriebssystem herunterlud, um sich für eine (zulässige) Kündigung zu rächen. Der zweite Beispielfall handelte von einem Fahrraddieb, dem aufgrund der Datenauswertung seines konfiszierten Smartphones (Fotos, E-Mails, App- und Gerätedaten) und der Erstellung eines detaillierten Bewegungsprofils mittels Cloud-Daten mindestens 58 Delikte innert nur elf Wochen nachgewiesen werden konnten. Dieses Urteil ist noch ausstehend.[13] Wenk schloss sein Referat mit den Worten, dass es nie vollkommene technische Sicherheit geben wird und eine entsprechende präventive Ausbildung das Beste ist, was man tun kann.

## IV. Datenauswertung zwecks Prävention und Beweissicherung

Bereits Prof. Dr. Christian Schwarzenegger hat darauf hingewiesen, dass Überwachung im öffentlichen Raum – mit Ausnahme vom Erkennen auffälligen Vorverhaltens z.B. im Vorfeld eines Raubüberfalls auf ein Juweliergeschäft – nicht stark präventiv, vielmehr repressiv zur Aufklärung von Straftaten (und/oder Unfällen) geeignet sei. Daran knüpften nachfolgende Referate an: Dr. Ulf Blanke, Co-Founder bei Antavi GmbH in Zürich, stellte das von seinem Unternehmen entwickelte App-gestützte Crowd-Management-System für Veranstaltungssicherheit und dessen Einsatzführung vor. Eingangs lenkte er die Aufmerksamkeit auf die mit Grossveranstaltungen einhergehenden Probleme. Durch die unterschiedlichen Verhaltensweisen der Besucher werden Menschenmassen zu komplexen Systemen, weshalb oft auch die Planung versagt. Regelmässig sind es Lokalinteraktionen in den Menschenansammlungen, die zu gefährlichen Auswirkungen auf die gesamte Masse führen. Das Ziel der App («Ops») ist es daher, präventiv solche Problempunkte zu erkennen, um frühzeitig eingreifen zu können. Dazu wird eine Leitzentrale geschaffen, welche die Zusammenarbeit und Kommunikation der Einsatzkräfte steuert. Als ideales Mittel der Umsetzung dient das allgegenwärtige Smartphone. Durch die App wird ein Format geschaffen, auf das jeder User Zugriff hat. Sie stellt einen digitalen Zwilling des entsprechenden Events her, erleichtert das Crowd-Management und ermöglicht eine vereinfachte Einsatzführung. Per QR-Code[14] kann den Einheiten beigetreten werden. Die von ihnen in die App eingetragenen Informationen zu etwaigem Alkohol- und Drogenmissbrauch oder medizinischen Notfällen werden in Echtzeit allen Usern über ein separates Netzwerk zur Verfügung gestellt und sogleich analysiert. Zur effizienten Kommunikation innerhalb der Teams sind Chats verfügbar. Die App wird u.a. von der Zürcher Stadtpolizei sowie privaten Sicherheitsanbietern

[8] Art. 79*b* Abs. 1 lit. b StGB.
[9] Art. 67 Abs. 3 StGB.
[10] Zur Überprüfung von zivilgerichtlich angeordneten Annäherungs-, Ort- und Kontaktverboten i.S.v. Art. 28*b* Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (ZGB), SR 210, siehe Art. 28*c* E-ZGB (BBl 2016 7869 f.; Ablauf der Referendumsfrist: 7.4.2019).
[11] Dabei wird mit Tricks versucht, an Zugangsdaten zu elektronischen Dienstleistungen zu gelangen.
[12] Dabei wird versucht, bösartige Software auf fremden Computern zu installieren.
[13] Vgl. Medienmitteilung der Stadtpolizei Zürich vom 4.4.2019 (<https://www.stadt-zuerich.ch/pd/de/index/stadtpolizei_zuerich/medien/medienmitteilungen/2019/april/hinweise_aus_der bevoelkerunghalfenbeiermittlungvonseriendieb.html>).
[14] Zweidimensionaler Quick-Response-Code.

verwendet und kam bereits bei mehr als 30 Events zum Einsatz (u.a. Münchner Oktoberfest und Züri Fäscht). Doch auch die Besucher werden als Datenerzeuger einbezogen. Durch die Zusammenarbeit mit Festival- und Stadt-Apps werden sie mit ihrer Zustimmung geortet und eine Karte erstellt, die den Personenfluss auf der Veranstaltung anzeigt. So ist ersichtlich, wo Engpässe entstehen. Überdies werden mit den Personendaten weitere Diagramme und Karten erstellt, welche etwa die Belastung des Verkehrsnetzes oder Wegfindungsentscheidungen der Besucher abbilden. Der Vorteil für den datenschaffenden User besteht darin, ebenso eine Karte bereitgestellt zu erhalten, auf welcher die Besucherdichte in den Festzelten und Arealen eingeschätzt werden kann. Dadurch werden insbesondere Personen mit Platzangst, Kinder oder Tiere vor grossen Menschenmassen gewarnt. Durch die Zusammenarbeit der Antavi GmbH mit dem öffentlichen Verkehr wird den Usern ausserdem angezeigt, welche Haltestellen überlastet sind. Insgesamt hat die nachträgliche Datenauswertung der Hotspots an Unfällen und Kriminalität präventive Wirkung für kommende Veranstaltungen.

Ein vergleichbarer Bezug zur Thematik von Beweissicherung in Form von Datenaufzeichnungen wurde von Bettina Zahnd, Leiterin der Unfallforschung und Prävention der AXA Winterthur, mit ihrer Präsentation der Verkehrsunfallprävention und neuen Risiken durch Fahrerassistenzsysteme (FAS)[15] gezogen. Anhand diverser, auf Daten der AXA beruhenden Studien erläuterte sie zunächst die Wirksamkeit verschiedener FAS bei der Verhinderung der häufigsten Unfallarten. Mit einem Antiblockiersystem (ABS) hätten z.B. in 65 untersuchten Fällen von Motorradauffahrkollisionen 75% der Stürze und 13,8% aller Unfälle verhindert werden können. Ferner verzeichnete der Dacia Sandero mit elektronischer Stabilitätskontrolle 47% weniger Schleuderunfälle als das gleiche Fahrzeug ohne FAS. Auch die Wirksamkeit von Notbremsassistenten (AEBS) konnte nachgewiesen werden: In 866 Fällen von Auffahrkollisionen eines Volvo XC60 und 79 Fällen der Mercedes-B-Klasse wurden 30% bzw. 69% weniger Zusammenstösse bei Fahrzeugen mit AEBS festgestellt. Keine Wirksamkeit zeigten einzig die Parkassistenzsysteme, wohl auch deshalb, weil viele Unfälle ausserhalb des Sensorbereichs verursacht werden. Zusammenfassend ist die Wirksamkeit von FAS – unter Ausnahme von Parkassistenzsystemen – nachgewiesen. Trotzdem können sie nicht alle Unfälle verhindern. Zahnd erläuterte zudem die sechs verschiedenen Stufen der Automatisierung, die vom Fahren ohne jegliche FAS (Level 0) bis hin zum vollautomatisierten Fahren (Level 5) reichen, wobei heute eine Automatisierung bis Level 2 (Teilautomatisierung) möglich ist. Das grösste Risiko geht derzeit von einer bedingten Automatisierung (Level 3) aus, bei der das Fahrzeug grundsätzlich autonom fährt, den Fahrer aber auffordern kann, die Führung wieder zu übernehmen. Gefahrenquellen sind hier der Vorgang der Kontrollübergabe an den Fahrer und das zu grosse Vertrauen in die Technik. Weitere Problemfelder liegen in Cyberrisiken wie Hackerangriffen und Mischverkehr von (nicht-)autonomen Verkehrsteilnehmern. Bei Letzterem liegt die Herausforderung darin, bereits im Voraus das Verhalten bei unausweichlicher Frontalauffahrkollision einzuprogrammieren. Dieses «moralische Dilemma» wurde an folgendem Beispiel veranschaulicht: Entscheidung des autonomen Fahrzeugs zwischen der Kollision mit einem unerlaubterweise überholenden Quad (1 Fahrer, ungeschützt) und einem verkehrsregelkonform fahrenden Personenwagen (mehrere Insassen möglich, durch Karosserie wohl besser geschützt). Als Fazit wurde festgehalten, dass mit der Erhöhung der Automatisierung neue Risiken geschaffen werden, aber Uneinigkeit darüber herrscht, ob dadurch auch mehr Unfälle verursacht werden. In der anschliessenden Diskussion wurde als realistisches Zukunftsszenario die Zulässigkeit des autonomen Einparkens ohne Fahrer erwähnt.

Den Themenbereich umrundend, gab Dr. Dario Brescianini, Institut der Neuroinformatik der Universität Zürich, einen Einblick in die Welt der (autonomen) Drohnen, deren technischen Entwicklung und möglichen Einsatzbereichen. Neben privater Nutzung dienen Drohnen den Behörden hauptsächlich der Überwachung mittels Videoaufzeichnung sowie der Such- und Rettungsmission durch das Erstellen von Ansichten vom Gebäudeinnern. Gerade hierfür werden die Drohnen immer kleiner und autonomer. Waren die nichtmilitärischen Drohnen früher über einen halben Meter gross, kann ihr heutiger Durchmesser rund fünf Zentimeter betragen. Im Fachhandel sind ferngesteuerte Drohnen erhältlich, die Sichtkontakt oder eine Kommunikationsverbindung benötigen. Ebenso sind bereits solche mit teilautonomer Navigation auf dem Markt, die mit einfachen Befehlen gesteuert werden (z.B. «Folge mir»). Vollautonome Drohnen, die selbstständig fliegen und Hindernissen ausweichen, befinden sich in der aktuellen Forschung. Die autonome Drohne lokalisiert sich dabei mittels Kameras und stabilisiert sich selbständig. Mit GPS weiss sie nur, wo sie sich befindet, erhält aber keine Information über ihre Umgebung. Auch funktioniert GPS nur im Freien und stösst im Innern von Gebäuden an seine Grenzen. Die sog. simultane Lokalisierung erfolgt durch maschinelles Sehen über die Kamera. Die Drohne wird dabei mit markanten Bodenpunkten mit starken Kontrasten wie Kanten oder Raumecken (initiale Punktwolke) «trainiert». Ihr System verwendet diese Daten dann dazu, sie im Flug zu stabilisieren. Hierfür nehmen die Kameras während des Flugs die Umgebung auf und das Steuerungssystem gleicht die Bilder mit den bereits gespeicherten Daten ab. So weiss die Drohne immer, wo sie ist. Ein Computer an Bord übernimmt schliesslich die Bildanalyse und generiert eine Karte der Umgebung. Dadurch kann die autonome Drohne auch auf sicherem Gelände landen oder Hindernisse erkennen. Drohnen können nach heutigem Stand der Technik auch so konzipiert werden, dass sie während des Flugs ihre Grösse anpassen, um

[15] Z.B. Müdigkeitswarner, Abstandregelsystem, Spurhalteassistent, Notbremssystem, Einparkhilfen etc.

durch eine Lücke zu passen. Darüber hinaus widmet sich die derzeitige Forschung der Navigation mithilfe künstlicher Intelligenz, damit die autonome Drohne künftig selbständig Manöver planen und anderen Drohnen ausweichen kann. In autonomen Drohnenrennen schätzt das neuronale Netz der Drohne z.B. die Distanz zum nächsten Durchflugstor selbständig ab.

In der anschliessenden Diskussionsrunde wurde auch bei diesem Referat klar, dass die Problematik des doppelten Verwendungszwecks immer wieder aufgegriffen werden kann. Neue Technologie ist zugleich Segen und Fluch: Im Sinne des Fortschritts bei der Überwachung, aber auch des zunehmenden kriminellen Einsatzes (z.B. unzulässige Luftpost mittels Drohne in Strafvollzugsanstalt).

## V. Zusammenfassung

Als Abschluss fasste Prof. Dr. CHRISTIAN SCHWARZENEGGER die Ergebnisse der diesjährigen Tagung zusammen. Hervorzuheben ist die ständige Dual-Use-Problematik neuer Technologien und das stetig wachsende, immer weniger strukturierte Datenvolumen. Schliesslich muss man bezüglich Nutzbarmachung aller Daten kritisch bleiben und die Verhältnismässigkeit zwischen Rechtsstaatlichkeit und Sicherheit im Auge behalten, damit die Grenzen zum Überwachungsstaat wie in China nicht überschritten werden.

Die Beiträge der Tagung werden von Schulthess Juristische Medien AG Zürich in der «Europa Institut-Reihe» publiziert.