3. ALES-Tagung 2014:

CYBERCRIME 2.0: VIRTUELLE FRAGEN – REALE LÖSUNGEN

Verlag für Polizeiwissenschaft, Prof. Dr. Clemens Lorei, Frankfurt 2015. 187 S., € 22,80
ISBN 978-3-86676-343-2

Es sind nicht die dicksten Überschriften und bedrohlichsten Akut-Meldungen in den Medien, doch sie finden sich regelmäßig, immer häufiger und vor allem immer beunruhigender. Gemeint ist die Cyber-Kriminalität weltweit und in unserer Zeit und Gesellschaft ganz besonders.

Fast täglich lesen, hören und vielleicht erleben wir sogar selber ein Phänomen, das vor noch nicht allzu langer Zeit reichlich fremd anmutete. Jetzt aber wird es zum täglichen(?) Risiko und zur wirtschaftlichen, wissenschaftlichen, politischen, vielleicht sogar eines Tages kulturellen Gefahr. Die Stichworte sind bekannt: Datenverlust bei staatlichen und privaten Institutionen, Hacker-Angriffe, Cyber-Mobbing, Kreditkarten-Missbrauch, Identitäts-Diebstahl, kurz: neue Kriminalitätsfelder, die sich aus der intensiven Nutzung von sozialen Netzwerken und der Verlagerung des Wirtschaftslebens in den virtuellen Raum speisen. Und zwar satt.

Was kann man dagegen tun? Zuerst einmal die Erkenntnis: Vorbeugend vielleicht so manches, nach dem Schaden auf jeden Fall das Notwendigste, zumindest für eine gewisse Zeit. Denn die andere Seite schläft nicht. Manche Experten sprechen nicht einmal mehr von einer Cyber-Kriminalität, sondern von einem regelrechten Cyber-Krieg (siehe aktuelle welt-politische Lage bzw. die entsprechende Aufrüstung der um die Vorherrschaft ringenden Mächte – was nicht nur staats-politisch gemeint ist).

Aber auch im Alltag wird offenbar der technologische Fortschritt vor allem von krimineller Seite aufgegriffen und ständig perfektioniert. Deshalb versucht das Strafrecht laufend den rapide wachsenden kriminellen Möglichkeiten durch gesetzliche Anpassungen nachzukommen (das letzte Wort sagt alles). Nun nützen aber nicht einmal neue Strafbestände etwas, wenn die Strafverfolgung durch Staatsanwaltschaften und Kriminalpolizei nicht effektiv genug betrieben werden kann. So steht außer Frage, dass die Polizei neue Instrumente braucht, um mit den raffinierten Methoden der Cyber-Kriminellen mitzuhalten. Stichworte: anonyme Internet-Kommunikation, der Einsatz von Verschlüsse-

lungs-Software und immer neues technischen Equipment auf der einen und erst einmal – bedenklich, aber nachvollziehbar – das notwendige „Nachrüsten“ auf staatlicher Seite. Außerdem gilt es bei der Diskussion um neue Ermittlungs-Befugnisse im strafprozessualen und polizeilichen Bereich jene grundrechtlichen Schranken zu berücksichtigen, auf die jeder (erst einmal) Anrecht hat, bis man ihm das Grenzwertige oder gar Kriminelle nachweisen kann. Auch hier wieder ein Stichwort, nämlich „Vorratsdaten-Speicherung“, das die einen als unverhältnismäßigen Eingriff in das Grundrecht ablehnen (was auch vom EuGH so gesehen wurde), die anderen als unverzichtbares Mittel voraussetzen, um Kommunikations-Vorgänge nach Entstehen eines Verdachts nachvollziehen und zuordnen zu können, vor allem zur Bekämpfung der leichten bis mittelschweren Kriminalität.

Diese wenigen Hinweise reichen jedenfalls aus, um den Verdacht einer inzwischen sehr realen Bedrohung zu erhärten und um gleichzeitig die Schwierigkeiten zu beleuchten, die eine erfolgsversprechende Abwehr im demokratisch-rechtlichen Rahmen garantieren sollen.

Hier hat die 3. Tagung am Austrian Center for Law Enforcement Sciences (ALES) der Universität Wien mit einer internationalen Tagung *Cybercrime 2.0: Virtuelle Fragen – Reale Lösungen“* im Jahre 2014 einen interessanten Beitrag geleistet, der inzwischen in Buchform vorliegt. Dabei ging es nicht nur um die Referate führender Experten, sondern auch um eine Podiums-Diskussion unter Beteiligung des sowohl interessierten als auch versierten Publikums (Transskript des Tonbandmitschnitts).

Der Tagungsband enthält also eine Fülle von Überlegungen, Anregungen, Einwänden, Vorschlägen, Beurteilungen, alltags-relevanten Beschreibungen und schließlich Schlussfolgerungen, die im Einzelnen nicht nur den Experten etwas sagen, in so manchen Punkten auch den Fachleuten anderer Disziplinen und sogar interessierten Laien auf diesen Gebieten etwas zur notwendigen Kenntnis der Cyber-Kriminalität beitragen können.

Die Zukunft wird solche Tagungsbände nach entsprechenden Symposien noch dringlicher machen. Oder wie es in so manchen Hinweisen herauszuhören ist: Das ist erst der Anfang (VF).