

Cyberkriminalität und künstliche Intelligenz

Ist die Polizei auf den digitalen Täter vorbereitet?

Von Thomas Jungfer, stellvertretender Bundesvorsitzender

In den letzten Jahren hat sich die Kriminalität verändert, sie ist schneller, internationaler und digitaler geworden. Und genau das stellt die Polizeien vor große Herausforderungen. Während früher der Streifenbeamte vor allem auf der Straße Präsenz zeigte, verlagern sich Straftaten heute zunehmend in den virtuellen Raum. Cyberangriffe, KI-gestützte Betrugsmaschinen, Deepfake-Technologien und organisierte Internetkriminalität stellen die Sicherheitsbehörden vor Herausforderungen, die noch vor wenigen Jahren kaum vorstellbar waren. Doch obwohl die Täter längst digital agieren, arbeitet die Polizei vielerorts noch immer mit Strukturen, die aus einer anderen Zeit stammen. Der digitale Streifenwagen fährt längst mit Blaulicht, doch vielerorts noch ohne die Ausstattung, die er dringend benötigt.

Die Zahl der Delikte im Bereich Cyberkriminalität steigt kontinuierlich. Besonders besorgniserregend ist dabei die Geschwindigkeit, mit der künstliche Intelligenz inzwischen auch für kriminelle Zwecke eingesetzt wird. Betrüger imitieren täuschend echt Stimmen von Angehörigen, erstellen professionell wirkende Phishing-Mails oder manipulieren digitale Inhalte so glaubwürdig, dass Bürgerinnen und Bürger kaum noch zwischen echt und gefälscht unterscheiden können. Die Täter sitzen dabei häufig nicht mehr im Nachbarort, sondern agieren international, anonym und hochprofessionell organisiert. Der digitale Raum ist längst zu einem neuen Einsatzgebiet geworden, mit enormer Dynamik und wachsender Bedrohungslage.

Für die Polizei bedeutet diese Entwicklung einen tiefgreifenden Wandel ihrer täglichen Arbeit. Ermittlungen werden komplexer, technische Anforderungen steigen und klassische Fahndungsmethoden stoßen zunehmend an ihre Grenzen. Gleichzeitig erwarten Bürgerinnen und Bürger zu Recht, dass der Staat auch im digitalen Raum Sicherheit gewährleistet. Doch genau hier zeigt sich ein strukturelles Problem: Die Polizei kann mit der Geschwindigkeit technologischer Entwicklungen oftmals kaum Schritt halten. Aus Sicht der DPoIG ist deshalb ein entschlossener Modernisierungskurs bundesweit zwingend erforderlich.

In vielen Dienststellen fehlt es nach wie vor an moderner technischer Ausstattung, spezialisierten IT-Kräften und ausreichenden Fortbildungsangeboten. Polizeibeamtinnen und Polizeibeamte leisten täglich hochprofessionelle Arbeit, häufig unter enormem Druck und mit großem persönlichen Engagement. Dennoch stoßen sie zunehmend an Grenzen, wenn komplexe Cyberdelikte mit veralteter Technik oder personeller Unterbesetzung bearbeitet werden müssen. Besonders kleinere Behörden stehen vor der Herausforderung, digitale Kriminalität mit begrenzten Ressourcen bekämpfen zu müssen.



© Marco Urban/DPoIG

Hinzu kommt der zunehmende Konkurrenzdruck durch die freie Wirtschaft. Gut ausgebildete IT-Spezialisten sind auf dem Arbeitsmarkt stark gefragt und verdienen in privaten Unternehmen oftmals deutlich mehr als im öffentlichen Dienst. Für die Polizei wird es dadurch immer schwieriger, qualifizierten Nachwuchs langfristig zu gewinnen und zu halten. Gleichzeitig wächst der Bedarf an Experten rasant. Die Digitalisierung der Kriminalität schreitet schneller voran als der Ausbau entsprechender Sicherheitsstrukturen. Gerade deshalb braucht es jetzt klare politische Entscheidungen und langfristige Investitionen in die innere Sicherheit.

Die DPoIG fordert seit Jahren eine konsequente Stärkung der digitalen Sicherheitsarchitektur in Deutschland. Dazu gehören vor allem eine deutlich bessere technische Ausstattung der Polizeibehörden, mehr spezialisierte IT-Ermittler sowie bundesweit einheitliche Standards bei der Bekämpfung von Cyberkriminalität.

Darüber hinaus fordert die DPoIG eine stärkere Investition in Aus- und Fortbildung. Polizeibeamtinnen und Polizeibeamte müssen frühzeitig auf digitale Einsatzlagen vorbereitet werden. Cyberkompetenz darf künftig kein Zusatzwissen einzelner Spezialisten mehr sein, sondern muss fester Bestandteil moderner Polizeiarbeit werden.

Ebenso notwendig sind attraktivere Rahmenbedingungen, um qualifizierte Fachkräfte langfristig für den Polizeidienst zu gewinnen. Wer im Wettbewerb mit der freien Wirtschaft bestehen will, muss moderne Arbeitsbedingungen, Entwicklungsperspektiven und eine leistungsgerechte Besoldung anbieten. Sicherheit im digitalen Raum wird in Zukunft maßgeblich davon abhängen, ob es gelingt, ausreichend qualifiziertes Personal für diese Aufgaben zu gewinnen.

Innere Sicherheit darf nicht erst dann politisch priorisiert werden, wenn Schäden bereits entstanden sind. Der Staat muss handlungsfähig bleiben – analog wie digital. Denn Kriminalität kennt längst keine Grenzen mehr, weder geografisch noch technologisch. Sicherheit endet nicht an der Haustür oder auf der Straße, denn sie beginnt längst auch auf Servern, in Netzwerken und auf Smartphones. —