Bundeskriminalamt

Tatort Internet –
eine globale Herausforderung für die Innere Sicherheit

BKA-Herbsttagung vom 20. – 22. November 2007

Polizei in der digitalen Welt

Kurzfassung Vortrag

Jörg Ziercke

Präsident,

Bundeskriminalamt Wiesbaden

BKA

EINGANGSTHESEN:

1. Globalisierung und Internationalisierung von Terrorismus und Organisierter Kriminalität lassen die Strafrechtspflege und Gefahrenabwehr an ihre territorialen und funktionalen Grenzen stoßen.

2. Technische Innovationssprünge prägen die Kriminalität des 21. Jahrhunderts. Die rasante Entwicklung der Informations- und Kommunikationstechnologie hat die weltweite Kommunikation, Interaktion und Datenspeicherung tiefgreifend gewandelt. Tat- und Tätertypologien verändern sich grundlegend.

3. Die Verletzlichkeit moderner, vernetzter Infrastrukturen wird weltweit an Bedeutung gewinnen. Angriffe auf kritische Infrastrukturen über Bot-Netze werden klassische Formen terroristischer Anschläge ergänzen.

4. Kryptierung und Anonymisierung schafft verfolgungsfreie Räume! Verschlüsselung verhindert den Zugriff auf Beweismittel, die auf digitaler Hardware abgelegt sind. Verschlüsselung verhindert den Zugriff auf Informationen und damit eine rechtzeitige Gefahrenabwehr.

5. Klassische Eingriffsinstrumente - wie die Wohnungsdurchsuchung oder die Beschlagnahme von Computern - reichen zur Bekämpfung terroristischer und organisierter krimineller Netzwerke nicht aus. Konspiration prägt das kriminelle Kommunikationsverhalten, religiöser islamistischer Terrorismus verfolgt seine Ziele langfristig.

6. Der Verfassungswert einer wirksamen Strafverfolgung und Gefahrenabwehr erfordert die kontinuierliche Anpassung polizeilicher Instrumentarien. Wir müssen den von Terroristen und Schwerstkriminellen längst vollzogenen digitalen Quantensprung aufholen. Wer einer solchen Anpassung ausweicht, macht die Polizei nicht nur blind. Er kündigt auch das Sicherheitsversprechen des Staates gegenüber seinen Bürgern und damit die elementare Grundbedingung eines friedlichen Zusammenlebens auf.

Im digitalen Zeitalter hat sich die **Ermittlungspraxis grundlegend geändert**. Während es vor fünf oder zehn Jahren z. B. bei Wohnungsdurchsuchungen vor allem darum ging, schriftliche Unterlagen sicherzustellen, stoßen wir heute auf die unterschiedlichsten technischen Geräte und Speichermedien. Informationen mit Beweiswert legen die Täter nicht nur auf ihrem PC, sondern auch im Internet ab. Zum Telefonieren nutzen Täter heute nur noch selten Festnetzanschlüsse, stattdessen

gewinnt die Internet-Telefonie an Bedeutung. Frei zugängliche Möglichkeiten der Kryptierung, der Steganografie und Anonymisierung, die Verschleierung von IP-Adressen und die Verwendung von Passwörtern lassen klassische polizeiliche Ermittlungsinstrumente immer mehr ins Leere laufen.

Auf diese Entwicklungen hat die Polizei bereits mit **neuen Bekämpfungsansätzen** und der Schaffung von **Spezialdienststellen** reagiert. So gibt es seit Mitte der 1990er Jahre Dienststellen für anlassunabhängige Recherchen im Internet, im BKA die „Zentralstelle für anlassunabhängige Recherchen in Datennetzen“, kurz ZaRD. Die Online-Streife sucht im Internet systematisch nach strafbaren Inhalten - deliktsübergreifend. Bund und Länder haben eine gemeinsame „Koordinierungsgruppe für anlassunabhängige Recherchen im Internet“ (KaRIn) eingerichtet.

Heute gibt es kaum noch einen Kriminalitätsbereich, in dem das **Internet als Tatmittel** keine Rolle spielt: zur Begehung von Betrugsdelikten, Wirtschaftsstraftaten und zur Verbreitung von Kinderpornografie ebenso wie zum Einsatz von Schadsoftware. Insbesondere die IuK-Kriminalität erweist sich aufgrund ihres enormen Schadenspotenzials und ihrer hohen Dynamik als besondere Herausforderung für die Sicherheitsbehörden.

Auch Terroristen nutzen das Internet auf vielfältige Weise: für die Verbreitung von Propaganda, für Spendenaufrufe, zur Radikalisierung, Rekrutierung und Ausbildung neuer Unterstützer und Kämpfer ebenso wie zur Tatvorbereitung und hoch konspirativer Kommunikation. Auch die Infrastruktur terroristischer Netzwerke hat das Internet erheblich verändert.

Das Schadenspotenzial der Internetkriminalität ist immens – durch das Internet sind Täter in der Lage, Firmen und sogar Staaten in die Knie zu zwingen. Auch Viktimisierungsprozesse haben sich durch das Tatmittel Internet erheblich verändert. Zum einen hat sich durch das Internet die Wahrscheinlichkeit für „Jedermann“, Opfer zu werden, deutlich erhöht. Zum anderen wird die Intensität der Viktimisierung, z. B. beim Handel mit kinderpornografischem Bildmaterial, verschärft.

Diese Trends bei der Kriminalitätsentwicklung dürfen jedoch nicht zu der realitätsfernen Schlussfolgerung führen, wir sollten künftig auf das Internet verzichten. Ebenso falsch ist die Forderung, das Internet müsse als Teil des allgemeinen Lebensrisikos frei von jeglichen Beschränkungen sein. Das Internet darf kein verfolgungsfreier Raum sein! Die Polizei ist gefordert, den Schutzauftrag des Staates für alle Bürger zu erfüllen und Kriminalität zu bekämpfen - unabhängig davon, in welcher Form und an welchem Ort sie verübt wird.

WIE MÜSSEN SICH DIE SICHERHEITSBEHÖRDEN IN DIESER DIGITALEN WELT AUFSTELLEN?

Die aktuellen Entwicklungen lassen nur einen Schluss zu: Die Polizei muss den technologischen Sprung, den die Gefährder- und Täterseite längst vollzogen hat, so schnell wie möglich aufholen. Dabei muss der rasante technologische Wandel bei der Suche nach Lösungen bereits heute mit vorausgedacht werden. Daher brauchen wir flexible rechtliche Rahmenbedingungen, also **technikoffene Lösungen**.

Außerdem benötigen wir eine breite Auswahl an polizeilichen Instrumenten, die von der Schwere und Sozialschädlichkeit eines Delikts genauso wie vom speziellen Modus Operandi abhängig sind. Aus einsatztaktischen Erwägungen und angesichts des Grundsatzes der Verhältnismäßigkeit greifen wir nur auf Maßnahmen zurück, die zweckgeeignet und mit Blick auf die jeweils aktuelle Gefahrenlage angemessen und zielgerichtet sind.

Um frühzeitig Ansatzpunkte für Überwachungsmöglichkeiten zu gewinnen und Angehörige krimineller Netzwerke identifizieren bzw. die Strukturen solcher Netzwerke überhaupt erhellen zu können, benötigen wir die so genannte **Vorratsdatenspeicherung**. Dabei geht es nur um die Identifizierung der IP-Inhaber. Kommunikationsinhalte werden nicht gespeichert.

Um auf relevante Informationen im Computer des Beschuldigten verdeckt, frühzeitig und vor allem gezielt zugreifen zu können, bevor diese verschlüsselt oder unauffindbar im Internet abgelegt werden, benötigen wir die **Online-Durchsuchung**. Dabei werden keine „Hackertools“ oder „Trojaner“ zum Einsatz kommen. Wir benötigen keine back doors kommerzieller Programme, sondern entwickeln Software als Unikate, die auch auf mögliche Risiken für Betroffene und Unbeteiligte hinreichend überprüft werden. Diese Software ist so ausgestaltet, dass auf den Zielsystemen keine Daten manipuliert werden. Der gesamte Einsatz wird umfangreich dokumentiert und ist vor allem auch durch die Gerichte immer nachvollziehbar. Ein Einsatz der Online-Durchsuchung für flächendeckende Fahndungen ist weder beabsichtigt noch möglich.

Die **Quellen-TKÜ**, eine besondere Form der konventionellen Telekommunikations-überwachung (TKÜ), ermöglicht die Überwachung verschlüsselter Internet-Telefonie. Die Quellen-TKÜ ist keine Alternative zur Online-Durchsuchung, da sie einen gänzlich anderen Zweck verfolgt: Bei der Quellen-TKÜ wird die laufende Kommunikation vor der Verschlüsselung bzw. nach der Entschlüsselung abgegriffen.

In der digitalen Welt steht die Polizei bei der Sicherstellung von Computertechnologie und bei der TKÜ vor dem Problem der Auswertung von **Massendaten**. Hierzu setzen

wir ein spezielles Auswertetool ein, dessen Funktionalitäten in Zukunft u. a. durch Fremdsprachenerkennung und Metadatenextraktion erweitert werden sollen.

SCHLUSSTHESEN:

1. Der rasante technische Wandel verändert Tat- und Tätertypologien grundlegend.

2. Klassische kriminalgeografische Räume werden durch den virtuellen Raum entgrenzt. Die Dezentralität des Internets befördert die Dezentralität von Netzwerken des Terrorismus und der Organisierten Kriminalität. Aber auch der Aktionsraum von Einzeltätern ist per Mausklick weltumspannend.

3. Verschlüsselung und Anonymisierung schaffen verfolgungsfreie Räume mit fatalen Folgen für die Innere Sicherheit, sowohl für die Strafverfolgung als auch für die Gefahrenabwehr.

4. Die Ungleichzeitigkeiten von Technik und Recht müssen beseitigt werden. Der Staat darf sich nicht blind, taub und handlungsunfähig machen.

Von daher brauchen wir eine **Kriminalistik der digitalen Welt**. Das heißt:

1. Wir brauchen technikoffene und damit flexible rechtliche Regelungen zur Strafverfolgung und Gefahrenabwehr.

2. Wir brauchen die Online-Durchsuchung als wirkungsvolle Maßnahme zur Aufhellung gespeicherter Daten und Informationen.

3. Wir brauchen die Quellen-TKÜ als unverzichtbare Maßnahme zur Kommunikationsüberwachung insbesondere im Bereich der Organisierten Kriminalität.

4. Wir benötigen die entsprechende technische und personelle - sehr spezialisierte - Ausstattung, um die Auswertung von Massendaten bewältigen zu können. Zur Bündelung knapper Ressourcen führt kein Weg an der Bildung von Kompetenz-Centern vorbei.

Das Bundeskriminalamt und die Polizeien des Bundes und der Länder stehen für die Bewahrung rechtsstaatlicher Freiheiten und für einen offenen und fairen Dialog auf der Basis unserer Lage- und Gefährdungserkenntnisse. Zu einem solch fairen Dialog, der ein kritischer Diskurs sein kann, fordern wir unsere Kritiker auf.