Matthias Monroy

# Cybersecurity-Initiativen als Teil einer Technologieoffensive

## Europol macht mobil, BKA ist Superuser

Die EU-Polizeiagentur Europol fordert die Einrichtung eines europäischen „Anti-Terror-Zentrums“ und die Überlassung geheimdienstlicher Informationen. Im Juli geht eine Meldestelle für unliebsame Internetinhalte an den Start. Zur Erforschung und Beschaffung neuer Analysewerkzeuge steuert hier auch das Bundeskriminalamt (BKA) seine Erfahrungen bei und nimmt gleichzeitig eine prominente Rolle in der Verteilung der dabei zu vergebenen Leitungsfunktionen ein.

Die Einrichtung von Europol wurde 1992 im Vertrag von Maastricht als „Europäisches Polizeiamt“ mit Sitz in Den Haag festgeschrieben. Vorausgegangen war ein Vorschlag Deutschlands im Europäischen Rat aus dem Jahr 1991, eine „Europäische Kriminalpolizeiliche Zentralstelle“ zu errichten, um die grenzüberschreitende Kooperation zu vereinfachen. Bis zur Ausgestaltung und Annahme eines Europol-Übereinkommens widmete sich Europol ab 1994 in der European Drug Unit (EDU) der Rauschgiftkriminalität und Geldwäsche. In ihrer Geschichtsschreibung sieht Europol 1999 als das Jahr, in dem die Behörde in ihrer heutigen Form entstand. Das Aufgabengebiet wandelte sich hin zu neuen Formen grenzüberschreitender Straftaten, darunter die Fälschung der neuen Euro-Währung und von Kreditkarten, Geldwäsche, Wirtschaftskriminalität und Korruption, Umweltkriminalität, Schutzgelderpressung, KFZ-Kriminalität oder Produktpiraterie, aber auch Kriminalitätsforschung und grenzüberschreitende Aus- und Fortbildung.

Vor fünf Jahren mauserte sich die „Polizeibehörde“ Europol schließlich zur „Polizeiagentur“ und wird seitdem wie die anderen EU-Agenturen durch den Gesamthaushalt der Europäischen Union finanziert. Das Europol-Übereinkommen wurde durch einen Ratsbeschluss ersetzt. 2011 bezog Europol ein neues Hauptquartier im Stadtteil Statenkwartier in Den Haag. Vor zwei Jahren hatte Europol seine „Arbeits- und Analysedateien” zu bestimmten Kriminalitätsbereichen komplett neu organisiert. Nun heißen sie „Focal Points“ und unterteilen sich in die Bereiche „organisierte Kriminalität“ und „Terrorismus“. Mitgliedstaaten können einem „Focal Point“ nach Belieben beitreten.

## Anzahl gespeicherter Datensätze erhöht sich stetig

Europol hat Arbeits- oder Kooperationsabkommen mit zehn EU-Einrichtungen (darunter Eurojust und Frontex), 18 Drittstaaten und drei internationalen Einrichtungen (Interpol, UNODC, WCO) abgeschlossen. Zur besseren Zusammenarbeit mit US-Behörden unterhält Europol ein Büro in Washington. Seit vorletztem Jahr betreibt Europol das „Europol Cybercrime Center" (EC3). Im Jahr 2013 arbeiteten 850 Personen bei Europol, darunter 160 sogenannte „Verbindungsbeamte". Sie sind für den Kontakt zu den Behörden der EU-Mitgliedstaaten verantwortlich.

Laut dem Jahresbericht der EU-Polizeiagentur Europol für 2013 hat sich der Anzahl gespeicherter Datensätze deutlich erhöht: So seien die im Europol Informationssystem abgelegten Objekte damals um 31% auf rund 245.000 angewachsen. Noch drastischer fiel die Zunahme gespeicherter Personen aus. Diese sei um 47% auf rund 71.000 Verdächtige oder verurteilte Straftäter_innen gestiegen. Monatlich seien rund 38.000 Nachrichten getauscht worden, der Jahresbericht spricht von 18.300 grenzüberschreitenden Maßnahmen. In 90 Fällen habe die Agentur dabei ihr „mobiles Büro" zur Verfügung gestellt: So kann bei Hausdurchsuchungen oder anderen Zwangsmaßnahmen jederzeit auf die Informationssysteme von Europol zugegriffen werden.

## Neue Werkzeuge zum Data Mining

In seinem Arbeitsprogramm für 2015 kündigt die Polizeiagentur Europol die Einführung eines ganzen Arsenals neuer Analysesoftware an. Die Rede ist von „fortgeschrittenen Werkzeugen für Datenverarbeitung, aufklärungsbasierte Analyse, darunter auch strategische Analyse und Analyse offener Quellen". Schon vor zwei Jahren schrieb Europol von Anwendungen zu „Data Fusion". Gemeint ist Data Mining, also die Möglichkeit, die existierenden Datenbestände in Beziehung zu setzen und grafisch anzuzeigen. Das Wall Street Journal hatte darüber hinaus berichtet, dass Europol an der Entwicklung neuer digitaler Analysewerkzeuge zur Mustererkennung arbeitet. Ausweislich eines Zitats des Europol-Chefs Trols Oerting geht es dabei um Einbrüche in Wohnungen und Fahrzeuge. Eine solche Vorhersagesoftware wird derzeit von mehreren deutschen Landeskriminalämtern getestet. Data Mining und „Predictive Analytics" sollten laut Oerting durch ein 150 Millionen Euro-Programm von Europol beforscht werden. Dabei handelt es sich wohl um das EU-Forschungs- und Rahmenprogramm, wo Europol an einigen Projekten beteiligt ist.

Im Arbeitsprogramm werden die Anwendungen als „future-forecasting and scenario techniques" beschrieben. Es ist aber unklar, inwiefern ihr Einsatz überhaupt rechtlich einwandfrei ist. Data Mining ist Polizeibehörden in Deutschland beispielsweise verboten. Auch die neue „Ma3tch"-Technologie zur Echtzeit-Analyse von Finanzdaten, auf deren Einführung Europol drängt, darf vom deutschen Bundeskriminalamt (BKA) nicht angewandt werden. Würden aus Deutschland angelieferte Daten bei Europol mit automatisierten Verfahren verarbeitet, könnte es sich um einen Ver-

stoß gegen Datenschutzbedingungen handeln. Deutschland ist laut eigenen Angaben „zweitstärkster Nutzer“ von Europols Informationssystemen. Auf Nachfrage erklärt die Bundesregierung, ihr sei „nicht bekannt, welche Anwendungen Europol für die konkrete Auswertung einzelner Ersuchen nutzt“. Anfragen aus Deutschland würden „ergebnisorientiert gestellt“, eine Eingrenzung auf bestimmte Analysetools finde nicht statt.

## Zentraler Tracking-Server bei Europol

Welche weiteren, neuen Anwendungen Europol nun beschaffen will ist ebenfalls unklar, die Worthülsen im Arbeitsprogramm lassen aber einige Rückschlüsse zu. So sollen Verfahren zur Auswertung und zum Vergleich biometrischer Daten eingeführt werden. Europol beabsichtigt, auf das neue EU-System zur Speicherung von Fingerabdrücken im Schengener Informationssystem zuzugreifen. Auch die Beschaffung von Software zur Erkennung von Personen und Sachen in Bild- und Videodaten steht laut dem Arbeitsprogramm auf der Europol-Wunschliste.

Bald sollen die Arbeiten an einem „European Tracking System“ abgeschlossen sein, mit dem europäische Polizeibehörden ihre GPS-Peilsender (etwa an Fahrzeugen Verdächtiger) auch grenzüberschreitend betreiben können. Europol richtet hierzu einen zentralen Server ein, der außer durch die Mitgliedstaaten auch von „Third Parties“ genutzt werden kann. Die Ausgabeformate der Peilsender werden hierfür standardisiert.

Die EU-Kommission hat nun zusätzliche Mittel von 12,5 Millionen Euro bereitgestellt. Als Begründung der IT-Aufrüstung dient die im Rechtsetzungsverfahren befindliche neue Europol-Verordnung, wonach die Agentur in einem „erweiterten Mandat“ ihre Analysefähigkeiten verbessern und ausweiten soll. Geplant ist etwa, dass Europol zukünftig selbst Daten von europäischen Polizeibehörden einsammeln darf und nicht mehr auf entsprechende Lieferungen warten muss. Die Verabschiedung der neuen Verordnung ist aber nicht in Sicht: Die immensen Auswirkungen auf den Datenschutz werden von vielen EU-Abgeordneten kritisiert. Im Entwurf des Rates ist vorgesehen, dass Europol zukünftig selbst nach Informationen suchen darf. Zunächst wäre dies auf das Internet beschränkt. Personenbezogene Daten sind aber ausdrücklich eingeschlossen.

## BKA steuert Erfahrungen bei

Auch die Fähigkeiten zur Verarbeitung von Gesichtsbildern sollen ausgebaut werden. Laut dem Bundesinnenministerium (BMI) sei das Bundeskriminalamt (BKA) von Europol um Informationen zu seinem „Fotovergleichs/-identifizierungswerkzeug“ gebeten worden. Dabei sei es auch um Anwendungen gegangen, die beim BKA „in der Erprobung oder in Planung“ sind. Als Hintergrund der Anfrage habe Europol ein „stark an-

gestiegenes Datenvolumen“ beklagt. Insbesondere fielen immer mehr Bilder und Videoaufnahmen „im Zusammenhang mit der ‚Syrienreisen-Problematik'“ an. Gemeint sind wohl „ausländische Kämpfer“: Angehörige der EU-Mitgliedstaaten, die sich in Syrien oder dem Irak islamistischen Gruppen anschließen und später nach Europa zurückkehren. Europol hat hierzu ein eigenes Analyseprojekt „Travellers“ gestartet, an dem auch das BKA teilnimmt. In umfangreichen Dossiers werden alle verfügbaren Informationen über einzelne Personen zusammengetragen. Die erst letztes Jahr begonnene Datensammlung enthielt zum Stichtag 31. Januar Beiträge zu 2.835 Personen.

Nun ist die Einrichtung eines „Europäischen Zentrum zur Terrorismusbekämpfung“ bei Europol geplant. Auch die EU-Kommission schlägt mittlerweile ein solches „European Counter Terrorism Centre“ (ECTC) vor. Bisher waren entsprechende Pläne lediglich vom Anti-Terrorismusbeauftragten der EU befürwortet worden. Vor einem Monat hatte schließlich Europol selbst für ein ECTC geworben. Die Polizeiagentur will auf diese Weise auch geheimdienstliche Informationen („intelligence data“) speichern und analysieren. Europol will dadurch „zentrale Nachrichtenlücken“ („key intelligence gaps“) schließen.

## „Vorrangiger Informationskanal“ für geheimdienstliche Informationen?

Das vorgeschlagene ECTC folgt offensichtlich dem Vorbild amerikanischer „Fusion Centres“ und dem deutschen „Gemeinsamen Terrorismusabwehrzentrum“ (GTAZ) in Berlin-Treptow. Dort arbeiten alle zuständigen Polizei- und Geheimdienstbehörden in themenspezifischen Arbeitsgruppen zusammen. Derartige Analysegruppen existieren bei Europol mit den „Focal Points“. Nur eine Woche nach dem Europol-Papier hat auch die Justiz-Agentur Eurojust einen offensichtlich abgestimmten, gleichlautenden Vorschlag zur Verarbeitung von „intelligence data“ gemacht. Europol und Eurojust machen sich mit dem neuen Vorschlag den Umstand zunutze, dass es keine einheitliche Definition für den Begriff „intelligence data“ gibt.

Europol will sogar zum „vorrangigen Informationskanal“ für „intelligence data“ werden. Die Daten könnten von Geheimdiensten der Mitgliedstaaten angeliefert werden. In Deutschland wäre dies das Bundesamt für den Verfassungsschutz. Derzeit darf Europol keine als „Geheim“ oder „Vertraulich“ eingestufte Daten verarbeiten. Das könnte sich laut dem Europol-Papier vom März ändern. Das EU-Anti-Terror-Zentrum soll abgeschottete, abhörsichere Hochsicherheitstrakte erhalten. Dies wäre nötig, um die Anforderungen für die Verarbeitung als vertraulich oder geheim eingestufter Informationen zu erfüllen.

Europol begründet seine Vorschläge mit Aufforderungen des Rates, seine Anstrengungen zum Informationsaustausch unter den Mitgliedstaaten zu verstärken. Derartige Formulierungen waren womöglich gar nicht als Aufforderung zum Aufbau einer geheimdienstlichen Kriminalpolizei gedacht, finden sich aber seit 9/11 in vielen Ratsdokumenten. Auch in den Beschlüssen zur Einrichtung des Schengener Informations-

systems, des SWIFT-Abkommens oder Abkommen zum Tausch von Fluggastdaten tauchen Formulierungen zur Verarbeitung von „intelligence data“ auf.

## Meldestelle für Internetinhalte

Inzwischen hat Europol auch Details zu einer geplanten „EU-Meldestelle für Internetinhalte“ skizziert. In einem Konzeptpapier werden Aufgabenbereiche und Vorgehensweisen dieser „EU Internet Referral Unit“ beschrieben. Die Pläne zum Aufbau der Meldestelle sind erst seit einem Treffen der EU-Innenminister_innen im März 2015 bekannt.

Im April hatte die EU-Kommission in ihrer „Europäischen Sicherheitsagenda“ erklärt, die Meldestelle solle bereits ab dem 1. Juli einsatzbereit und dem ebenfalls noch nicht errichteten „Europäischen Zentrum zur Terrorismusbekämpfung“ angegliedert werden. Der Fokus beider Einrichtungen liege demnach zunächst auf islamistischem Terrorismus. Die EU-Mitgliedstaaten sollen nun Kontaktstellen für die Meldestelle benennen. In Deutschland läge die Zuständigkeit wohl bei der Staatsschutzabteilung des Bundeskriminalamts (BKA). Für Mitte April hatte Europol die nationalen Ableger der Meldestelle zu einem operativen Treffen eingeladen.

Europol will mithilfe der neuen Einrichtung den „terroristischen Missbrauch des Internets“ eindämmen. Geplant seien sowohl „präventive“ als auch „pro-aktive“ Maßnahmen. So würden unliebsame Inhalte oder Accounts bei Sozialen Medien markiert und entsprechende Informationen unter den Behörden der EU-Mitgliedstaaten verteilt. Eine „dynamische Aufklärung“ soll weitere Informationen zu den dahinter stehenden Personen oder Organisationen besorgen.

## „Beseitigung“ und Sperre

In der „Europäischen Sicherheitsagenda“ hatte die Kommission davon gesprochen, die Meldestelle solle die Mitgliedstaaten bei der „Beseitigung gewalttätiger extremistischer Online-Inhalte“ unterstützen. Auch im nun veröffentlichten Europol-Dokument ist die Rede vom „removal of content“. Die ebenfalls erwähnte Sperre („suspension“) bezieht sich wohl auf Accounts bei Sozialen Medien. Vor jeder Maßnahme soll Europol eine „ganzheitliche Risikoeinschätzung“ vornehmen. Diese sollte auch die möglichen Auswirkungen auf die Leser_innen der zu entfernenden Inhalte bewerten.

Doch die Accounts und Webseiten werden von Polizeien und Geheimdiensten auch zur Beobachtung oder Infiltration genutzt. Das Offline-Nehmen von Internetauftritten soll deshalb unterbleiben, wenn sie brauchbare Informationen liefern oder für Ermittlungen benötigt werden. Genannt werden Twitter-Accounts, die – sofern das Geotagging aktiviert ist – GPS-Koordinaten in ISIS-Gebieten offenlegen könnten. Auch würden Geheimdienste über Twitter Informationen über „lokale Ereignisse“ erhalten.

Die Meldestelle soll laut der Kommission eng „mit Partnern aus der Wirtschaft“ kooperieren. Gemeint sind unter anderem Google, Facebook und Microsoft, mit denen Europol bereits im Oktober vergangenen Jahres zu einem Abendessen zusammenkam. Im Mai ist ein weiteres Treffen geplant. Dort sollen auch „Bedenken der Strafverfolgungsbehörden in Bezug auf die neuen Verschlüsselungstechniken Raum gegeben werden“.

## BKA legt Grundstein

Das deutsche BKA hatte 2007 den Grundstein für die neue Meldestelle gelegt. Damals startete der deutsche Staatsschutz bei Europol das Projekt „Check the Web“, das ebenfalls „Veröffentlichungen terroristischer Organisationen und von Personen aus dem islamistisch-jihadistischen Spektrum“ speichert und analysiert. Die Abteilung beschäftigt Linguist_innen für sieben beobachtete Sprachen, darunter auch russisch. Gespeichert werden Videos, Audiodateien, Textveröffentlichungen und Erklärungen. Eine eigens angelegte Analysedatei enthält Daten über mehr als 10.000 „Dokumente und Individuen“. Als „assoziierte Drittstaaten“ dürfen derzeit auch die Schweiz und Australien darauf zugreifen.

Die neue Meldestelle will nicht nur auf dem Projekt „Check the Web“ aufbauen. Auch die Expertise des gerade einmal zwei Jahre alten „Cybercrime-Zentrums“ (EC3) soll bei der Analyse und Beseitigung unliebsamer Inhalte helfen. Im Europol-Dokument werden dessen Fähigkeiten zur „Cyber-Aufklärung“ und forensischen Analyse gelobt. Das Zentrum habe auch gute Erfahrung in der Analyse von Massendaten.

Laut der Antwort auf eine Kleine Anfrage ist das BKA an mindestens 17 Maßnahmen von Europol beteiligt, die sämtlich die bessere Ausforschung und Kontrolle des Internet zum Ziel haben. So sollen etwa eine „Internetauswertungskoordinierungsgruppe“ gegründet und „Maßnahmen gegen inkriminierte Kommunikationsplattformen“ gestartet werden. Die Maßnahmen waren von Europol zuerst im ebenfalls nicht öffentlichen „Operativen Aktionsplan zur Priorität ‚Cyberangriffe‘“ aufgeführt worden. Zwar wird als Zeitraum für die Maßnahmen sämtlich das Jahr 2015 angegeben. Einige von ihnen werden aber laut der Bundesregierung erst 2016 beendet.

## Ausgerechnet mit Großbritannien „Cyberbedrohung“ auf Mitgliedstaaten abwehren

Mehrere der Projekte werden sogar vom BKA geleitet, bei anderen fungiert die deutsche Behörde als „Co-Leiter“ oder als „Unterstützer“. Worin sich die konkrete Beteiligung ausdrückt bleibt unklar, auch die personellen Ressourcen werden nicht mitgeteilt. Laut der Antwort auf eine frühere Kleine Anfrage sind „Aktionsleiter“ „insbesondere für die Koordination der Aktivitäten der Teilnehmer an der Maßnahme ver-

antwortlich“. Sie sollten sich des Weiteren „mit den Co-Aktionsleitern zur weiteren Gestaltung der Maßnahme abstimmen und weitere Teilnehmer einbinden“.

Bekannt war bislang lediglich die deutsche Teilnahme an der Arbeitsgruppe „Joint Cyber Action Task Force“ (J-CAT). Die Einheit ging im September 2014 bei Europol an den Start und gehört zum European Cybercrime Center. Im Fokus stehen Hackerangriffe, Botnets, Bitcoins und NutzerInnen, die sich via TOR und I2P unsichtbar machen. Die J-CAT soll Bedrohungen möglichst im Vorfeld analysieren und ihre Gefährlichkeit gewichten. Hierfür werden sowohl „offene Quellen“ als auch polizeiliche Erkenntnisse aus Ermittlungen genutzt.

Eine der neuen Arbeitsgruppen soll „Cyberbedrohungen mit Auswirkung auf zwei oder mehr Mitgliedstaaten“ identifizieren. Die Aktionsleitung ist ausgerechnet Großbritannien übertragen, das nach Medienberichten selbst für einen Cyberangriff auf EU-Einrichtungen verantwortlich sein soll und dabei den Trojaner „Regin“ einsetzte. Die Co-Aktionsleitung der Maßnahme liegt bei Europol. Die EU-Agentur hatte damals kein Mandat erhalten, den mutmaßlich vom britischen Geheimdienst GCHQ durchgeführten Angriff aufzuklären.

**MATTHIAS MONROY** ist Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift Bürgerrechte & Polizei/CILIP. In Teilzeit Mitarbeiter des MdB Andrej Hunko. Publiziert in linken Zeitungen, Zeitschriften und Online-Medien, bei Telepolis, Netzpolitik und in Freien Radios.