Bürgerrechte & Polizei

Cilip 98
Nr. 1/2011

Internet unter Kontrolle? Die Staatsgewalt im Web 2.0

Ergebnisse der „Werthebach-Kommission"
„Ordnung und Vernichtung – Die Polizei im NS-Staat"

Inhalt

Internet unter Kontrolle? Die Staatsgewalt im Web 2.0

Redaktionsmitteilung

So schnell kann das gehen: Noch im Frühjahr dieses Jahres applaudierten PolitikerInnen und Medien auch hierzulande den „Facebook-Revolutionen" in Tunesien und Ägypten. Mutige BloggerInnen hatten der Meinungsfreiheit zum Durchbruch verholfen. Via Twitter kamen die Demo-Termine und auf YouTube konnte man Handy-Filme der Aufständischen bestaunen.

Nur wenige Monate später ist die Begeisterung verflogen. Im „Spiegel" wettert Bundesinnenminister Hans-Peter Friedrich Anfang August gegen die „anonymen Blogger", bei denen sich Anders Breivik, der Attentäter von Oslo, die Versatzstücke seiner Ideologie zusammengesucht hat. Warum müssen sie „ihre wahre Identität nicht offenbaren?", fragt er. Ein Vermummungsverbot fürs Internet will er aber nicht gefordert haben. Im britischen Unterhaus entsetzt sich Premier David Cameron darüber, dass sich die Randalierer in London und anderen Städten über die diversen „social media" verabredet haben. Er propagiert Kommunikationssperren.

Der „Cyberspace" ist seit Jahren eine ideale Projektionsfläche für SicherheitspolitikerInnen, Polizei, Geheimdienste und im wachsenden Maße auch für Militärs. Die Gremien und Institutionen zur Sicherung dieser „kritischen Infrastruktur" gegen Angriffe von Hackern, Kriminellen, Terroristen oder feindlichen Staaten boomen. Das Internet ist längst (auch) zu einem Testfeld neuer verdeckter Überwachungsmethoden geworden.

***

Die Hamburger Polizeikommission war der einzige Versuch, eine von Justiz und Parlamenten unabhängige Form der Kontrolle zu etablieren. Sie wurde nach nur zwei Jahren wieder abgeschafft. Haben solche Institutionen heute bessere Chancen? Welche Modelle kommen dafür in Frage? Mit diesem Thema wird sich die kommende Ausgabe von Bürgerrechte & Polizei/CILIP befassen.
(Heiner Busch)

Digitaler Untergrund

Kriminalisten und Kriminalisierte wetteifern im Web 2.0

von Matthias Monroy und Heiner Busch

Mit der Ineinssetzung von Krieg, Terror und organisierter Kriminalität werden uferlose Kontrollinstrumente des Internet begründet. Dabei hat es bislang keinen „cyber-terroristischen" Angriff gegeben.

Das digitale Böse lauert bei jedem Mausklick: So jedenfalls will es ein im Januar eigens für das Kriminalitätsphänomen Internet erstellter Bericht von Europol glauben machen. Das fortan alle zwei Jahre publizierte „Threat Assessment on Internet Facilitated Organised Crime" (iOCTA)[1] der EU-Polizeiagentur analysiert, wie das Internet als Kommunikationsmittel, Informationsquelle, Marktplatz, Ort zur Suche nach Gleichgesinnten und Finanzdienstleister dient. Nichts Neues eigentlich, nur dass im Focus von Europol vor allem organisierte Kriminelle stehen, die demnach mit neuen digitalen Möglichkeiten ihre „offline organisierte Kriminalität" befördern: Herstellung von und Handel mit Drogen, Menschenhandel, Produktpiraterie, Steuerbetrug mit so genannten „Karussellgeschäften", Währungsfälschung, Waffenhandel oder Kinderpornografie. Online-Glücksspiele helfen laut Europol, das ergaunerte Geld weltweit und damit schwer nachvollziehbar in geregelte Finanzströme zu überführen. Auch illegalisierte Migration wird laut Europol vom Internet begünstigt.

In dem von Europol entdeckten „digitalen Untergrund" werden vor allem illegal erlangte Personen- oder Finanzdaten gehandelt, um etwa mit manipulierter Identität Zugang zu Konten oder Kreditkarten zu bekommen. Umgeschlagen werden beispielsweise Adressen, Telefonnummern, Namen und mit ihnen verknüpfte Geburtsdaten. Das Internet bringt laufend neue Kriminalitätsphänomene hervor, darunter das Ab-

1 Europol: Threat Assessment. Internet Facilitated Organised Crime – iOCTA, Den Haag 2011, s. www.europol.europa.eu unter „publications"

greifen von Passwörtern („Phishing“), das Umleiten auf nachgeahmte Webseiten („Pharming“), das Zirkulieren von Schadsoftware oder das Hacken von Firmenwebseiten. Computer werden durch Viren manipuliert und dadurch untereinander vernetzt, um in sogenannten Botnetzen automatisierte Angriffe auf Server auszuführen.

Fluch und Segen digitaler Tsunamis

Die „cyberkriminelle Ökonomie“ richtet angeblich beträchtliche finanzielle Schäden an. Die EU-Agenturen Europol, Eurojust und Frontex sprechen in einem gemeinsamen Bericht von rund 750 Milliarden Euro jährlichen Verlusten für die Privatwirtschaft.[2] Den nicht legalisierten Download von Videos, Musik und Spielen sowie Software bilanzierten Konzerne 2009 auf rund 61 Milliarden US-Dollar.[3] Die frühere EU-Wettbewerbskommissarin und jetzige Kommissarin für die Digitale Agenda zitiert eine Studie des World Economic Forum (WEF) von 2008, die auch Grundlage einer bereits letztes Jahr verabschiedeten Mitteilung der Kommission gewesen war.[4] Die Verfasser behaupten dort eine Wahrscheinlichkeit von 10 bis 20 Prozent, dass sich in den kommenden zehn Jahren ein größerer Ausfall von Informationsinfrastrukturen ereignen würde. Der Weltwirtschaft könnten dadurch Kosten von rund 250 Milliarden US-Dollar entstehen. Andersherum sind die Investitionen in „Cyber-Sicherheit“ beträchtlich und versprechen hohe Wachstumsraten: Die Consulting-Firma Frost & Sullivan ermittelte in einer im Februar 2011 herausgegebenen Studie, dass Nordamerika mit 38 Prozent der größte Absatzmarkt für „Cyber-Sicherheit“ ist, Westeuropa und Asien machen demnach insgesamt die Hälfte des gesamten Marktes aus.[5]

Die „Zukunftsgruppe“, die das im Dezember 2009 verabschiedete „Stockholmer Programm“ vorbereitete, hatte von einem „digitalen Tsunami“ gesprochen.[6] Die in diesem Gremium vereinten Innenminister

2 Ratsdok. 9359/10 v. 7.5.2010

3 www.eos-eu.com/LinkClick.aspx?fileticket=1M94q5KmJdM%3D&tabid=225&mid=1109; eine Studie von 2011 kommt auf umgerechnet 41,4 Milliarden Euro allein für die nichtlizensierte Nutzung von Software: http://portal.bsa.org/globalpiracy2010

4 WEF: Global Risks 2008, Cologny, Genève 2008; Amtsblatt der EU (ABl. EU) C 255 v. 22.9.2010; KOM(2009) 149 endg. v. 30.3.2009

5 Frost & Sullivan: Cyber Security – From Luxury to Necessity, February 2011

6 www.bmi.bund.de/cae/servlet/contentblob/128602/publicationFile/15773/European_home_affairs_executive_final_report_de.pdf, in der deutschen Übersetzung des Papiers

von neun EU-Staaten hatten dabei allerdings keine Katastrophe vor Augen, sondern begeisterten sich über die „gewaltigen Informationsmengen, die für öffentliche Sicherheitsorganisationen nützlich sein können." Eine Vorstellung über das Volumen zukünftiger Datenhalden gibt die Industrie, die bis zum Jahr 2020 mit einer „Explosion von Unternehmensdaten um das 44-Fache" rechnet und ebenfalls einen „Daten-Tsunami" heraufziehen sieht.[7] Im Bereich von Polizeien und Geheimdiensten dürften ähnliche Dimensionen zu erwarten sein. Nicht anders kann verstanden werden, wenn sich die vom damaligen deutschen Innenminister Wolfgang Schäuble initiierte „Zukunftsgruppe" den polizeilichen „Zugang zu fast grenzenlosen Mengen nützlicher Informationen" wünscht.

Dass mit dem „Fluch" an neuen Straftaten im Internet auch ein „Segen" für die Ermittlungsbehörden verbunden ist, hatte letztes Jahr ein Artikel in der „Kriminalistik" herausgearbeitet.[8] Untersucht wurde die Bedeutung des Web 2.0 bzw. von Sozialen Netzwerken wie Facebook, StudiVZ oder SchülerVZ für polizeiliche Ermittlungen. Die beiden Autoren analysieren, dass eine ganze Reihe realer polizeilicher „Lagen" auch im Internet abgebildet werden bzw. dort recherchiert werden können: Beleidigungen, Betäubungsmitteldelikte, Stalking, Unterhaltspflichtverletzungen, Betrugsstraftaten, Sexualstraftaten, Urheberrechtsverletzungen, Vortäuschung und Aufforderung zu Straftaten oder politisch motivierte Kriminalität. In ihrer Verfolgung können sich Behörden auf die bereitwillige Unterstützung von Betreibern der Web-Plattformen verlassen, die ganze Abteilungen unterhalten, um im Falle von Ermittlungen auch nicht-öffentliche Profildaten der Nutzer auszuhändigen.[9]

Bei der Auswertung der im Web 2.0 verborgenen Informationen setzen Polizeien und Geheimdienste Software ein, um zunächst vermeintlich bedeutungslose Datensätze in Sozialen Netzwerken oder Webseiten untereinander in Beziehung zu setzen und ihnen damit einen höheren Informationswert zu verschaffen. Die Software verknüpft etwa Personen- und Sachdaten sowie Ereignisse, berechnet Wahrscheinlichkeiten und trifft Voraussagen. Anbieter behaupten, die Programme auch an das Bun-

---

der Zukunftsgruppe wird die Formulierung „Daten-Tsunami" verwendet.

7 http://telekom.report.at/index.php/wirtschaft-a-politik/35611-daten-tsunami

8 Henrichs, A.; Wilhelm, J.: Polizeiliche Ermittlungen in Sozialen Netzwerken, in: Kriminalistik 2010, H. 1, S. 30-36

9 Siehe hierzu ein Leak der „Facebook Law Enforcement Guidelines": http://info.publicintelligence.net/Facebook2010.pdf

deskriminalamt, an Landeskriminalämter sowie andere Polizeidienststellen verkauft zu haben.[10] Mit „Virtuoso“ finanziert die EU-Kommission ein ähnliches Forschungsprojekt, das eine automatisierte Auswertung Sozialer Netzwerke entwickelt.[11] Erst kürzlich berichtete die britische Tageszeitung „Guardian“, dass die Metropolitan Police of London mit „Geotime“ eine Software der US-Firma Oculus gekauft habe, die auch vom US-Militär eingesetzt werde.[12] „Geotime“ vergleicht nicht nur Informationen aus dem Internet, sondern kann diese mit Geodaten aus der Satellitennavigation, Mobilfunkdaten oder auf Vorrat gespeicherten IP-Adressen verknüpfen. Auch Daten aus Finanztransaktionen können integriert werden.

Dennoch fühlen sich Kriminalisten mehr und mehr ausgesperrt, da die Observierten oft anonymisierte oder verschlüsselte Kommunikationskanäle benutzen, die ein effektives „Aufspüren und Überwachen“ erschweren. Polizeien und Geheimdienste nutzen deshalb Schadsoftware, um aus der Ferne in private Rechner einzudringen und per Bildschirmfoto Aktivitäten in Chats zu dokumentieren oder auch das vorgefundene Dateisystem zu durchsuchen.[13] Die hierfür genutzten Programme firmieren als „Remote Forensic Software“ und werden in Deutschland vom BKA angeblich selbst entwickelt und inzwischen auch eingesetzt.[14]

Recherchen der US-Bürgerrechtsorganisationen Electronic Frontier Foundation ergaben kürzlich, dass das FBI inzwischen großflächig Spähsoftware einsetzt.[15] Vom französischen Inlandsgeheimdienst DCRI sind ähnliche Aktivitäten bekannt.[16] Und auch auf EU-Ebene werden immer wieder Initiativen gestartet, um „Maßnahmen zur Erleichterung von Ferndurchsuchungen“ zu etablieren. Bereits 2008 hatte der Rat der EU eine „Partnerschaft zwischen der Polizei und dem privaten Sektor“ ange-

10 www.heise.de/tp/artikel/31/31425/1.html
11 www.virtuoso.eu
12 www.guardian.co.uk/uk/2011/may/11/police-software-maps-digital-movements
13 Die 81. Konferenz der Datenschutzbeauftragten von Bund und Ländern hat in einer Entschließung vom 17. März 2011 darauf aufmerksam gemacht, dass rechtliche Regelungen in Deutschland angesichts weitgehender Funktionalitäten der Software fehlen; s. www.datenschutz.de/dsb-konferenz.
14 BT-Drs. 17/5677 v. 29.4.2011
15 www.eff.org/deeplinks/2011/04/CIPAV_Post
16 http://vasistas-blog.net/2010/11/25/unerlaubte-online-durchsuchungen-durch-den-franzosischen-geheimdienst