



2011/34 Lifestyle

<https://jungle.world/artikel/2011/34/fang-einen-pluenderer>

Die digitalen Ermittlungsmethoden der britischen Polizei

Fang einen Plünderer!

Von **matthias monroy**

Die britischen Behörden wollen die Beteiligten an Riots und Plünderungen aufspüren. Polizei und Geheimdienst stellen dafür das Internet auf den Kopf.

Jeweils vier Jahre Haft für einen Aufruf zu Randalen auf Facebook – obwohl die Einträge der beiden Verurteilten in ihren Herkunftstädtchen Warrington und Northwich folgenlos blieben. Das waren die bisher härtesten Urteile, die von einem britischen Gericht nach den Riots in Großbritannien ausgesprochen wurden. Premierminister David Cameron lässt von Polizei, Geheimdiensten und der Industrie prüfen, inwieweit Verurteilten der Zugang zu Twitter und Facebook entzogen oder ihr Internetzugang gleich ganz abgeschaltet werden könnte: »Die freie Zirkulation von Informationen kann für Gutes genutzt werden. Sie kann aber auch für Schädliches genutzt werden.« Derweil wurde bereits ein Jugendlicher für vermeintlich »schädliches Verhalten« zu drei Monaten Hausarrest verurteilt. Gegen einen 17jährigen wurde neben Sozialstunden ein zwölfmonatiger Facebook ban verhängt. Scotland Yard hat auf Twitter und Facebook weitere Jugendliche bzw. teils sehr junge Männer unter anderem aus der Grafschaft Essex im Verdacht, deren Namen – sofern sie nicht minderjährig sind – bereits im Internet veröffentlicht wurden.

Die britischen Behörden kämpfen mit harten Bandagen über die Vorherrschaft im Internet. »Wir werden diese Art von Verhalten in Essex nicht tolerieren«, schwadronierte der für die Grafschaft zuständige Polizeipräsident und forderte eine Politik der Nulltoleranz auch in sozialen Netzwerken. Fotos von Verdächtigen kursieren derzeit nicht nur auf Polizeiwebsites, sondern werden auch auf der Bilder-Plattform Flickr gepostet. Die polizeiliche Mitteilung zu dieser sogenannten Operation Withern ähnelt den anonymen Ankündigungen von Hackergruppen wie Anonymous oder Lulzsec: »Heute werden wir die ersten von vielen Bildern der Verdächtigen veröffentlichen. Das Ziel von Operation Withern ist, diejenigen zur Rechenschaft zu ziehen, die gewalttätige und kriminelle Taten begangen haben.« Die Polizei in Manchester twitterte indes die Namen von Verdächtigen. Der stellvertretende Polizeipräsident Garry Shewan polterte in dem Thread gegen den Premierminister, dieser interessiere sich nicht genug für die Auswüchse des in Großbritannien verpönten antisocial behaviour.

Bei Google wird mit der Gruppe »London Riots Facial Recognition« versucht, Gesichter von Verdächtigen zu identifizieren und hierfür die in Deutschland erst kürzlich vom größten Suchmaschinendienst freigeschaltete Funktion der Gesichtserkennung zu nutzen. In einem

Spreadsheet auf Google, das Daten zu angeklagten Teilnehmern an den Riots sammelt und von der Tageszeitung Guardian aktualisiert wird, waren bis Ende vergangener Woche bereits mehr als 1 000 vermeintliche Beteiligte unter ihren Klarnamen und mit Herkunftsorten sowie teilweise den ergangenen Urteilen aufgeführt.

Mit »Catch a looter« wurde zudem eine Website der Organisation Crimestoppers UK aufgesetzt. Diese stellt Bilder von Plünderern online, um »die Nachbarschaft sicherer zu machen«. Wegen der großen Anzahl der Beiträge stellte der Betreiber das Angebot allerdings eilig wieder ein. Unterstützt werden die Initiativen von Polizei, Internet-Blockwarten und Google durch Prominente, die über den Twitter-Feed »Riotcleanup« dazu aufrufen, sich mit Besen an den Aufräumarbeiten zu beteiligen.

Ein Sprecher der Metropolitan Police bestätigte vergangene Woche, dass die Behörden sogar eine Abschaltung der social media erwogen haben, wies jedoch gleichzeitig auf deren Funktion als »sehr nützliches Aufklärungsmittel« hin. Tatsächlich gilt das Internet nicht nur als Tatort, sondern auch als Ermittlungswerkzeug. Dass mit dem Fluch der neuen Straftaten im Internet auch ein Segen für die Ermittlungsbehörden verbunden ist, hatte bereits vor einem Jahr ein Artikel in der deutschsprachigen Zeitschrift Kriminalistik herausgearbeitet. In der Strafverfolgung können sich Behörden auf die bereitwillige Unterstützung von Web-Plattformen verlassen, die ganze Abteilungen unterhalten, um im Falle von Ermittlungen auch nicht öffentliche Profildaten der Nutzer auszuhändigen. Bei der Auswertung der im Web 2.0 öffentlichen Informationen setzen Polizeien und Geheimdienste Computer ein, um zunächst vermeintlich bedeutungslose Datensätze in sozialen Netzwerken oder auf Websites untereinander in Beziehung zu setzen und ihnen damit einen höheren Informationswert zu verschaffen. Spezielle Software kann etwa Personen- und Sachdaten sowie Ereignisse miteinander verknüpfen, Wahrscheinlichkeiten berechnen und Voraussagen treffen. Mit »Virtuoso« finanziert die EU-Kommission ein Forschungsprojekt, das eine automatisierte Auswertung sozialer Netzwerke entwickelt. Der Guardian berichtete jüngst, dass die Londoner Polizei eine Software der US-Firma Oculus gekauft habe, die auch vom US-Militär eingesetzt wird. Geotime, so der Name dieser Software, vergleicht nicht nur Informationen aus dem Internet, sondern kann diese mit Geodaten aus der Satellitennavigation, Mobilfunkdaten oder auf Vorrat gespeicherten IP-Adressen verknüpfen. Daten aus Finanztransaktionen können ebenfalls integriert werden. Auch ohne Zugriff auf die Inhalte von Kommunikation sind derartige Analysen von hohem Informationsgehalt. Die Journalistin Christiane Schulzki-Haddouti beschreibt in der aktuellen Ausgabe der polizeikritischen Fachzeitschrift Bürgerrechte & Polizei/CILIP, wie Kontakte zwischen Verdächtigen mit Hilfe von Verkehrsdaten sogar besser identifiziert werden können als über Befragungen. Studien ergaben, dass Netzwerkbeziehungen vollständig aufgedeckt werden können, wenn nur acht Prozent der Gruppe überwacht werden.

Allerdings erfährt die britische Öffentlichkeit wenig über die gegenwärtigen digitalen Ermittlungsmethoden. Eine Polizeisprecherin erklärte nun, dass die Polizei durch die Auswertung von Twitter sogar weitere Sachbeschädigungen verhindert habe – angeblich seien neben Shopping Malls auch Austragungsorte der nicht nur in der Linken kritisierten Olympischen Spiele 2012 ins Visier der randalierenden Kids geraten. Wie die Ermittler an diese Informationen gelangten, wird bislang verschwiegen. Vermutlich haben einige der Verhafteten ihre Account-Daten ausgehändigt, mit denen die Polizei jetzt mitlesen kann und einen Überblick über die an der Kommunikation beteiligten User erhält.

Ähnlich dürften die Kriminalisten mit Nachrichten der in Großbritannien sehr populären Mobiltelefone der Marke Blackberry verfahren, die wegen ihrer besser gesicherten

Kommunikation neben der britischen Polizei auch den Innenbehörden anderer Länder Kopfzerbrechen machen. Als einziger Mobilfunkanbieter verschlüsselt der kanadische Hersteller Research in Motion (RIM) seine Textnachrichten des Dienstes BlackBerry Messenger (BBM), die überdies gratis sind. Die Regierungen Indiens, Indonesiens, Saudi-Arabiens und der Vereinigten Arabischen Emirate hatten deshalb von RIM verlangt, ihnen Abhörfunktionen einzuräumen, und hierfür teilweise Zugeständnisse bekommen. Da die BlackBerry-Textnachrichten nicht Ende-zu-Ende-verschlüsselt sind und nur zwischen Usern und den Servern der Firma sicher übertragen werden können, dürfte RIM selbst die Nachrichten entschlüsseln können.

Mittlerweile wurde der ansonsten nur für Terrorismus, Massenvernichtungswaffen und Spionage bemühte Inlandsgeheimdienst MI5 beauftragt, die Verschlüsselung von BlackBerry Messenger zu knacken. Das könnte sich in der Praxis als leichter als vermutet herausstellen oder sogar bereits passiert sein, da das verwendete kryptographische Verfahren in Sicherheitskreisen als einfach gilt. Unterstützt wird der Ermittlungseifer des MI5 durch das Government Communications Headquarter (GCHQ), das mit Kryptographie, Datenübertragung und geheimdienstlicher Aufklärung digitaler Kommunikation befasst ist. Das GCHQ sichert die britischen Computersysteme und betreibt Satelliten-Horchstationen.

Blackberry-Telefone werden auch für Nachrichten an Gruppen und ganze Netzwerke genutzt, weshalb sie tatsächlich eine gewichtige Rolle in der Kommunikation bei den Riots oder den Angriffen auf Polizeistationen gespielt haben dürften. In Essex hat die Polizei eine 18jährige festgenommen, die angeblich per BBM zu Aufständen aufrief, in Southampton wurde ein 27jähriger verhaftet und bis zu seinem Prozess auf freien Fuß gesetzt. RIM hatte der Polizei zuvor eilig und ohne öffentlichen Druck angetragen, »sie in jeder uns möglichen Weise zu unterstützen«, wofür die Firma nicht nur von der Organisation Reporter ohne Grenzen heftig kritisiert wurde, die darin einen »beunruhigenden Präzedenzfall in einem westlichen Staat« sieht.

Prompt wurde RIM selbst zum Ziel einer wenigstens digitalen Sachbeschädigung, als Hacker unter dem Namen »TeaMp0isoN« den offiziellen BlackBerry-Blog übernahmen und die Nachricht »Dear Rim; You Will _NOT_ assist the UK Police« hinterließen. Gedroht wurde, ansonsten eine Datenbank mit RIM-Angestellten zu veröffentlichen. Eine weitere aus datenschutzrechtlicher Perspektive durchaus fragwürdige Nutzung von BlackBerry-Diensten hatte indes bereits der Stadtrat des Londoner Stadtteils Camden vorgenommen und kurz nach Beginn der Riots eine Nachricht an 800 Teenager geschickt. Ihnen wurde geraten, an jenem Tag doch lieber daheim zu bleiben. Zweifelhaftes Lob der britischen digitalen Nulltoleranz kam derweil aus China: Die staatliche Website »Global Times« freut sich, dass Zensur-Gräben zwischen Ost und West bald zugeschüttet seien. Jene, die eine ungehinderte Entwicklung des Internet verlangten, seien gehalten, ihre Ideen zu überdenken.