Bildquellen: Amnesty International, Human Rights Watch, Mimikama, Bellingcat; Composing: c't

Mosaik der Wahrheit

Open Source Intelligence: Wie OSINT-Experten Kriegsverbrechen aufdecken und Propaganda widerlegen

Wenn Regierungen lügen, halten Organisationen wie Bellingcat und Human Rights Watch dagegen: Mit Recherchen in sozialen Netzwerken und der Analyse von Fotos und Videos sammeln sie Beweise. Hier sind die Methoden der OSINT-Profis sowie Tools, die allen zur Verfügung stehen.

Von Christian Wölbert

Als am 8. April eine Tochka-U-Rakete am Bahnhof der ukrainischen Stadt Kramatorsk explodierte und Dutzende Zivilisten tötete, wies Moskau die Verantwortung schnell von sich. Raketen des Typs Tochka-U würden „ausschließlich von den ukrainischen Streitkräften eingesetzt“, schrieb das russische Verteidigungsministerium zwei Stunden nach dem Angriff auf Facebook.

Eine Woche später veröffentlichte das Recherchekollektiv Bellingcat eine Sammlung von Fotos und Videos aus sozialen Netzwerken und russischen Medien, die Tochka-U-Raketenwerfer der russischen Armee zeigen, zum Beispiel bei einer Parade im Februar 2021 und bei Transporten durch Belarus im März 2022 (siehe ct.de/y1xa). Die Fundstücke klären zwar nicht die Frage, wer den Bahnhof in Kramatorsk angegriffen hat, erschüttern jedoch das zentrale Argument des russischen Dementis.

Die Tochka-U-Recherche von Bellingcat ist ein Beispiel für eine Methode, die meist als „Open Source Intelligence“ oder „OSINT“ bezeichnet wird. Gemeint ist das Auffinden und Auswerten von Informationen aus öffentlichen Quellen – und die Präsentation der Funde im Netz, damit jeder das Material selbst überprüfen und seine eigenen Schlüsse daraus ziehen kann.

Transparenz statt Geheimniskrämerei

Wichtig ist dabei vor allem die transparente Arbeitsweise. Das Sichten allgemein verfügbarer Informationen an sich ist nichts Neues: Geheimdienste nutzen neben verdeckten schon immer auch offene Quellen wie Medienberichte. Doch anders als die OSINT-Community behalten sie ihre Erkenntnisse in der Regel für sich. Der Gründer von Bellingcat, der Brite Eliot Higgins, beschreibt seine Arbeits-

weise deshalb ungern als „Open Source Intelligence“, er spricht lieber von „Online Open Source Investigation“.

Wie wichtig die Methode ist, zeigte sich schon ab 2010 während des Arabischen Frühlings und später während der Bürgerkriege in Syrien und Libyen. Aufgrund der Gefahren vor Ort haben nur wenige unabhängige Reporter aus den Krisengebieten berichtet. Doch über Facebook, YouTube und Twitter konnte jeder fast in Echtzeit Gefechte, Bombenangriffe und Gräueltaten verfolgen.

Außer Journalisten und Menschenrechtsaktivisten taten das auch Menschen wie Higgins, die beruflich nichts mit den Konflikten zu tun hatten, sich aber für das Zeitgeschehen interessierten und sich gut im Netz auskannten. Higgins arbeitete damals noch als IT-Administrator und verfolgte den Arabischen Frühling in jeder freien Minute.

Mehrfach entdeckte er auf Plattformen wie YouTube Belege für Kriegsverbrechen – zum Beispiel 2013 für Giftgasangriffe des Assad-Regimes in Syrien. Seine Erkenntnisse wurden von traditionellen Medien aufgegriffen, was wiederum weitere Menschen dazu brachte, online auf Spurensuche zu gehen. 2014 gründete Higgins dann Bellingcat, um sich mit anderen Online-Rechercheuren zu vernetzen und Analysen zu veröffentlichen. Inzwischen beschäftigt allein Bellingcat 18 Angestellte und arbeitet mit Dutzenden OSINT-Experten zusammen.

Bild: Twitter/Belarusian Hajun Projet

Nach dem Angriff auf den Bahnhof von Kramatorsk behauptete die russische Regierung, keine Raketen vom Typ Tochka-U einzusetzen. Doch Recherchen in sozialen Netzwerken widerlegten diese Aussage.

Aber auch Menschenrechtsorganisationen setzen OSINT ein: Human Rights Watch (HRW) gründete 2020 ein „Digital Investigation Lab“, in dem sechs Spezialisten arbeiten. „Außerdem bilden wir ständig weitere Mitarbeiter in Open-Source-Techniken aus“, erklärt Gabriela Ivens, OSINT-Expertin bei HRW, gegenüber c’t. Amnesty International gründete 2016 das „Digital Verification Corps“, in dem rund 100 Studenten den Menschenrechtlern bei der Recherche helfen. Nach OSINT-Methoden arbeiten zudem viele Faktenchecker in Redaktionen und bei gemeinnützigen Organisationen wie Correctiv und Mimikama.

Angesichts des Kriegs in der Ukraine ist OSINT heute wichtiger denn je. Schließlich treibt kaum eine Regierung auf der Welt das Spiel mit Desinformation und Zensur so weit wie die russische. „Für Russland sind Informationen Teil des Schlachtfeldes, und man muss in der Lage sein, sich zu wehren“, sagte Eliot Higgins vor Kurzem in einem Interview mit der Zeitung The Telegraph.

Die Nadel im Instagram-Haufen

Viele OSINT-Experten haben Spezialwissen, etwa im Bereich Waffensysteme, was ihnen bei der Recherche hilft. Wichtig ist auch, die richtigen Social-Media-Accounts anzuzapfen und relevante Posts schnell aus der Masse herauszufiltern. Einige von Higgins’ ersten Rechercheerfolgen beruhten darauf, dass er jene Handvoll „Medienzentren“ in den syrischen Rebellengebieten identifiziert hatte, die überhaupt über eine Internetverbindung verfügten und Videos hochladen konnten.

Manchmal ist auch Ausdauer gefragt: Nach dem Abschuss des Fluges MH17 über der Ostukraine im Juli 2014 fanden Rechercheure von Bellingcat schnell Fotos und Videos eines Buk-Luftabwehrsystems. Doch woher war dieses Fahrzeug gekommen? Hatte die russische Armee es den Separatisten übergeben? Um das herauszufinden, klickte sich ein Bellingcat-Mitglied vier Tage lang durch belanglose Posts russischer Instagram- und Vkontakte-Nutzer, bis er ein Foto der Buk mit der gesuchten Kennnummer beim Transport durch Russland entdeckte – so schreibt es Higgins in seinem 2021 erschienenen Buch „We are Bellingcat“.

OSINT-Tricks

Das Auffinden solcher Informationen ist bei OSINT allerdings nur der erste Schritt.

c't kompakt

- „Open Source Intelligence“ beziehungsweise „OSINT“ bezeichnet das Auswerten öffentlicher Quellen und die Veröffentlichung der Funde und Recherchewege.
- Zu den wichtigsten OSINT-Methoden gehören die zeitliche und örtliche Einordnung von Fotos und Videos (Geolokalisierung, Chronologisierung).
- Mit ihren Analysen decken OSINT-Experten unbekannte Vorgänge auf und entlarven Fake News.
- Organisationen wie Bellingcat und Amnesty International veröffentlichen Recherchetipps und bieten OSINT-Webinare an.

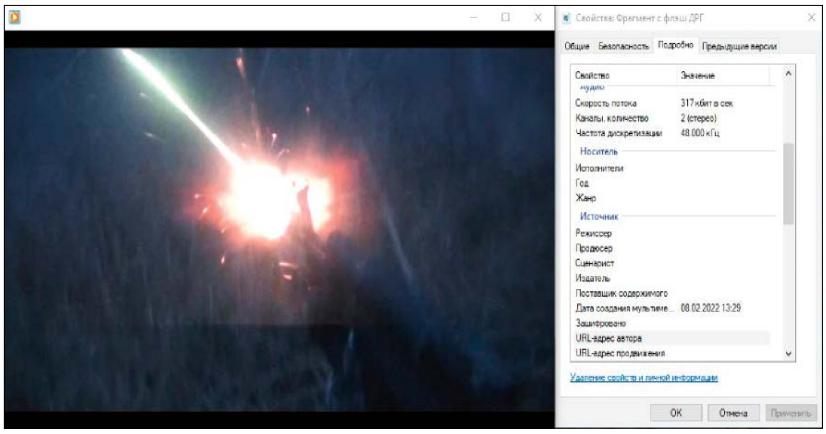
Dann beginnt die eigentliche Arbeit: Wo und wann wurden die Fotos und Videos tatsächlich aufgenommen? Und was ist auf ihnen wirklich zu sehen? Bei der Beantwortung dieser Fragen kommen immer wieder vier Methoden zum Einsatz: die Rückwärtssuche nach Bildern, die Analyse von Metadaten, die Geolokalisierung mithilfe von Karten und Satellitenaufnahmen sowie die tageszeitliche Einordnung durch die Analyse von Schatten.

Die Rückwärtssuche nach Bildern kann verraten, ob ein Foto wirklich das zeigt, was in der Beschreibung behauptet wird. Lädt man eine Bilddatei etwa bei Google hoch, sucht der Anbieter nach identischen und ähnlichen Aufnahmen. Manchmal reicht das schon aus, um festzustellen, dass ein Bild älter ist als angegeben und an einem anderen Ort aufgenommen wurde.

Die Rückwärtssuche kann aber auch dabei helfen, bislang unbekannte Personen, Objekte oder gar Landschaften zu identifizieren, die auf einem Foto zu sehen sind. In OSINT-Kreisen beliebt ist das Chrome-Plug-in „Fake news debunker by InVID & WeVerify“, das mit einem Klick Rückwärtssuchen bei diversen Suchmaschinen wie Google, Bing, Baidu und Yandex startet.

Verräterische Metadaten

Manchmal stecken auch in den Metadaten von Fotos und Videos interessante Erkenntnisse: Wenige Tage vor dem Überfall Russlands auf die Ukraine veröffentlichte die Miliz der separatistischen „Donezker



Bit Depth	24
Matrix Structure	1 0 0 0 1 0 0 0 1
Media Header Version	0
Media Create Date	2022:02:08 10:29:30
Media Modify Date	2022:02:08 10:29:30
Media Time Scale	48000
Media Duration	0:01:25
Media Language Code	eng
Balance	0
Handler Type	Alias Data
Handler Description	Alias Data Handler
Audio Format	mp4a
Audio Channels	2
Audio Bits Per Sample	16
Start Timecode	00:01:01:09
Xmp Toolkit	Adobe XMP Core 5.6-c145 79.162860, 2018/04/19-01:08:43
Create Date	2022:02:08 13:29:29+03:00
Modify Date	2022:02:08 13:30:22+03:00

Pantry Ingredients From Part	time:28236418560000f254016000000d11379 91680000f254016000000
Pantry Ingredients To Part	time:18787023360000f254016000000d11379 91680000f254016000000
Pantry Ingredients File Path	M72A5 LAW and APILAS live fire.mp4
Pantry Ingredients Mask Markers	None
Pantry Windows Atom Extension	.prproj

Bild: Twitter/@oldLentach

Dieses Video ostukrainischer Separatisten zeigt angeblich eine Sabotageaktion. Die Metadaten verraten jedoch, dass die Datei schon Tage vor dem angeblichen Datum erstellt wurde und mit der Tonspur eines YouTube-Videos kombiniert wurde.

Volksrepublik“ ein Video, das angeblich eine Sabotageaktion polnischsprachiger Söldner zeigte. Man habe die Aktion vereitelt und das Video bei einem der Angreifer gefunden, behauptete die Miliz.

OSINT-Experten fanden jedoch schnell heraus, dass das Video schon einige Tage vor dem angeblichen Angriff erstellt worden war. Dafür genügte ein Blick in die Metadaten, die zum Beispiel von Videoschnittprogrammen und von Webdiensten wie Metadata2go.com angezeigt werden. Außerdem zeigten die Metadaten, dass die Separatisten das Video mit der Tonspur eines YouTube-Videos unterlegt hatten, das eine finnischen Militärübung im Jahr 2010 zeigt (siehe ct.de/y1xa). Die Miliz hatte also stümperhaft versucht, einen Vorwand für die russische Invasion zu fabrizieren.

Zugute kam den Rechercheuren, dass das Video auf Telegram veröffentlicht worden war: Die Plattform tilgt nicht immer alle Metadaten von Fotos und Videos. „Das ist ein Datenschutzrisiko für Nutzer, aber ein Segen für Rechercheure“, schreibt Bellingcat in einem aktuellen Blogeintrag. Außerdem lassen sich Telegram-Inhalte leicht archivieren, für den Fall, dass die Plattform oder der Urheber sie löscht – in der Telegram-Desktop-Anwendung genügen dafür zwei Klicks. Wer Videos etwa von YouTube herunterladen will, benötigt hingegen Tools wie youtube-dl.

Wo …

Bei vielen Recherchen spielt Geolokalisierung eine zentrale Rolle, also die Feststellung, wo eine Aufnahme entstanden ist. Dabei suchen OSINT-Experten nach markanten Merkmalen, etwa Gebäuden, Schildern oder Straßenverläufen, die sich mit anderen Quellen abgleichen lassen – etwa mit Karten, anderen Fotos und Satellitenaufnahmen.

Eine wichtige Rolle spielte die Geolokalisierung zum Beispiel bei der Aufklärung des schon erwähnten Abschusses von MH17 im Jahr 2014. Durch den Abgleich von Fotos mit älteren Google-Street-View-Aufnahmen konnten Bellingcat-Rechercheure den Weg des Buk-Raketenabwehrsystems von Russland bis zur Nähe der Abschussstelle engmaschig belegen.

Anfang 2021 geolokalisierten Rechercheure von Amnesty International ein Video eines Massakers an unbewaffneten Gefangenen in Äthiopien, obwohl darin keinerlei Gebäude zu sehen waren. Amnesty gelang es, unscheinbare Geländeformationen in 3D-Daten aus Google Earth und Satellitenaufnahmen wiederzufinden. So konnte die Organisation ihre Vorwürfe gegen äthiopische Regierungstruppen untermauern (siehe ct.de/y1xa).

… und wann?

Ähnlich wichtig ist die Chronologisierung, also die Feststellung, wann ein Foto oder Video aufgenommen wurde. Auch dabei helfen mit etwas Glück Satellitenbilder: In Google Earth Pro vergleicht man mit einem Schieberegler bequem Aufnahmen von verschiedenen Tagen und sieht, wie Umgebungen sich über die Zeit verändern. So konnte Bellingcat zum Beispiel nachweisen, dass ukrainische Buk-Systeme sich im Juli 2014 nicht an einem bestimmten Ort nahe der MH17-Absturzstelle aufgehalten hatten, wie das russische Verteidigungsministerium behauptet hatte – sondern einen Monat vorher.

Um die Uhrzeit einer Aufnahme zu bestimmen, erfassen OSINT-Experten die Länge eines darin sichtbaren Schattens im Vergleich zum zugehörigen Objekt. Die Webanwendung SunCalc (suncalc.org) berechnet anhand dieser Daten, zu welcher Uhrzeit dieses Objekt-Schatten-Verhältnis passt – vorausgesetzt, Ort und Datum sind bekannt. Ende 2021 wies Human Rights Watch unter anderem mithilfe von SunCalc den zeitlichen Ablauf der Ereignisse bei einem Massaker an Demonstranten

Bild: Twitter/@digitaljonah

Nach dem Bombenangriff auf eine Entbindungsklinik in Mariupol postete die russische Botschaft in Israel ein Foto, das angeblich ukrainisches Militär vor der Klinik zeigte. Durch Geolokalisierung ließ sich das schnell widerlegen.

mit mindestens 65 Toten in Myanmar nach (siehe ct.de/y1xa).

Halböffentliche Quellen

In manchen Fällen geben OSINT-Rechercheure sich nicht mit öffentlichen Quellen zufrieden. „Wir haben Verträge mit mehreren Anbietern von Satellitendaten, zum Beispiel Planet Labs, und kaufen nötigenfalls Bildmaterial ein“, sagt Gabriela Ivens von Human Rights Watch.

Auch Bellingcat ist Kunde bei Planet Labs und ließ im Herbst Follower darüber abstimmen, zu welchem Ort man ein Foto einkaufen sollte – die Mehrheit entschied sich für einen Flughafen in Libyen. Die Auflösung der Planet-Labs-Bilder liegt bei 50 Zentimetern. „Noch vor wenigen Jahren waren Satellitenbilder dieser Qualität für gemeinnützige Organisationen und unabhängige Rechercheure kaum verfügbar“, schreibt Bellingcat.

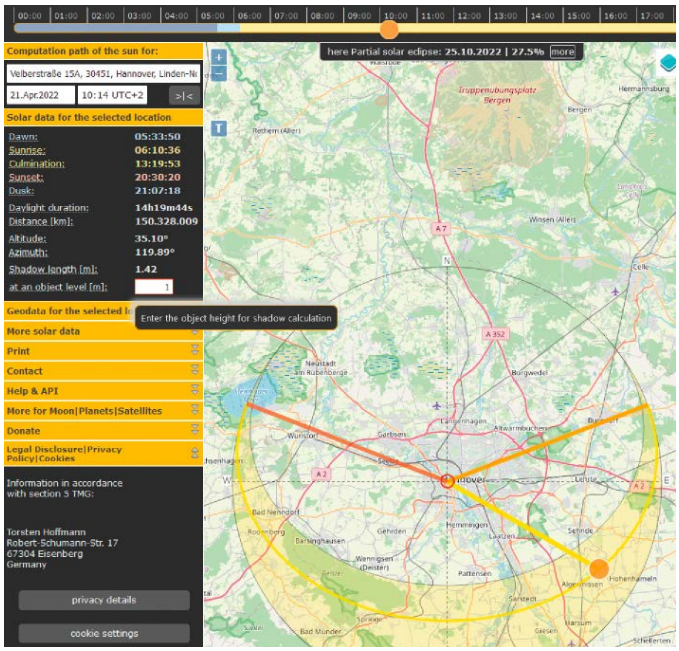
Da Firmen wie Planet Labs als vertrauenswürdig gelten und das Material meist gut überprüft werden kann, führt der Einkauf solcher Bilder in der OSINT-Community selten zu Diskussionen. Heikler ist der Einkauf aus anonymen Quellen: Bellingcat hat mehrfach über dubiose Mittelsmänner die Datenbanken russischer Fluglinien und Behörden angezapft, etwa zur Enttarnung der Spione, die Alexei Nawalny sowie Sergei Skripal und seine Tochter vergifteten. Auf Telegram gibt es sogar Bots, über die man Daten russischer Behörden kaufen kann.

Bei Bellingcat wurden diese Datenbeschaffungen heftig debattiert, schreibt Higgins in seinem Buch. Alle Untersuchungen sollten auf offenen Quellen beruhen, aber in „sorgfältig beurteilten Einzelfällen“ gehe man darüber hinaus. Wichtig sei, das Material aus verdeckten Quellen besonders kritisch zu hinterfragen.

Mitmachen erwünscht

Die OSINT-Community legt viel Wert darauf, Anfänger in Recherchetechniken und beim Umgang mit Tools auszubilden – schließlich haben die meisten Experten von heute selbst erst vor ein paar Jahren als Quereinsteiger angefangen.

Bellingcat veröffentlicht nicht nur Recherchen, sondern auch Anleitungen. In einer gigantischen Google-Tabelle listet die Organisation außerdem Software-Tools und Webdienste auf, die für OSINT nützlich sein können (siehe ct.de/y1xa). Bellingcat bietet auch Online-Workshops an, die in der Regel allerdings über 800 Euro kosten. Ein kostenloses OSINT-Webinar für Einsteiger gibt es von Amnesty International (siehe ct.de/y1xa).



Aus dem Verhältnis der Länge eines Schattens zum zugehörigen Objekt berechnet SunCalc die Uhrzeit. So lässt sich oft feststellen, wann ein Foto aufgenommen wurde.

Außer um Tools und Tricks geht es in solchen Kursen auch um die Frage, wie man sich davor schützt, von brutalen Fotos und Videos aus Kriegsgebieten traumatisiert zu werden. Auch Standards im Umgang mit personenbezogenen Daten spielen eine wichtige Rolle. Was schiefgehen kann, wenn OSINT-Anfänger ihre Fähigkeiten überschätzen und Standards missachten, zeigten Reddit-Nutzer nach dem Anschlag auf den Bostoner Marathon 2013: Sie beschuldigten öffentlich zwei unbeteiligte Männer, das Attentat verübt zu haben.

Doch wer gründlich recherchiert, minutiös dokumentiert und jede Veröffentlichung sorgfältig abwägt, kann mit etwas Glück kleinere oder größere Mosaiksteine zur Wahrheitsfindung beitragen. Bellingcat bindet manchmal gezielt die Öffentlichkeit ein und lagert Aufgaben wie die Ortsbestimmung von Fotos an Twitter-Follower aus. Und jedermann kann komplette Recherchen bei der Plattform einreichen und zur Veröffentlichung vorschlagen. Zu tun gibt es – leider – mehr als genug. *(cwo@ct.de)* c't

Beispiel-Recherchen, Tools: ***ct.de/y1xa***

Wie unabhängig ist Bellingcat?

Russische Propagandisten werfen Bellingcat immer wieder vor, für die US- oder die britische Regierung zu arbeiten, weil sich ein Großteil der Recherchen um Verbrechen der russischen und der syrischen Regierung dreht. Eliot Higgins verteidigt diesen inhaltlichen Schwerpunkt in seinem Buch „We are Bellingcat“ mit der Aussage, dass die Regierungen in Syrien und Russland zu den „unehrlichsten und gewalttätigsten“ auf der Welt zählten. Er verweist darauf, dass Bellingcat auch den rechtswidrigen Einsatz von US-Waffen im Jemen und einen Bombenangriff der US-Luftwaffe auf eine Moschee in Syrien aufgedeckt hat.

Betrieben wird die Rechercheplattform von einer niederländischen Stiftung. Diese nimmt laut eigener Aussage grundsätzlich keine Spenden von einzelnen Staaten an, aber von zwischenstaatlichen Organisationen wie der EU und den UN. Aktuell stamme ein Drittel der Bellingcat-Einnahmen aus Workshops, der Rest komme von Spendern. Zu den Geldgebern gehören demnach die EU und diverse private Stiftungen. In den Anfangstagen wurde Bellingcat laut Higgins auch von Google gefördert.