Bessere Internet-Ermittlung durch Open Source Intelligence (OSINT)

Drei Trends, Herausforderungen und Lösungsansätze für die polizeiliche OSINT-Arbeit

Berlin, 07.11.2022

Bessere polizeiliche Internet-Ermittlung durch Open Source Intelligence

Wer erinnert sich noch an MySpace, Google+ oder studiVZ? Social-Media-Plattformen scheinen gerade erst die Kommunikation über das Internet revolutioniert zu haben, da verschwinden zahlreiche von ihnen bereits wieder von der Bildfläche. Der schnelle Wandel bei Endgeräten und Internet-Trends im Jahresrhythmus brachte neue Plattformen wie TikTok, Snapchat oder Twitch hervor, während MySpace, Google+ oder studiVZ abgeschaltet wurden.

Solche Trends stellen die **Arbeit der Polizei mit Internet-Daten vor wachsende Herausforderungen**. Modulare Software, mehr Vernetzung und die methodische Weiterbildung im Bereich **Open Source Intelligence (OSINT)** können hier Abhilfe schaffen. Das PD-Team aus dem Bereich Öffentliche Sicherheit arbeitet – in Kooperation mit Sicherheitsbehörden – an diesen Lösungsansätzen für die **Verbesserung der polizeilichen Ermittlungen im Internet**.

Drei Trends in sozialen Netzwerken – begleitet von einer stetig wachsenden Informationsflut

Die **rasanten Entwicklungen im Bereich der sozialen Medien** folgen verschiedenen Trends: Auch rund 20 Jahre nach ihrem Aufkommen wachsen soziale Netzwerke in Deutschland Jahr um Jahr weiter – sowohl mit Blick auf die **Zahl der Nutzenden** als auch in Bezug auf deren **tägliche Verweildauer** im Internet.[1]

Gleichzeitig ändert sich die Nutzung von Plattformen permanent: Während das Netzwerk studiVZ mit rund 6,2 Millionen Nutzenden im Jahr 2009 eines der erfolgreichsten Online-Angebote in Deutschland war, ist diese Plattform heute von der Bildfläche verschwunden.

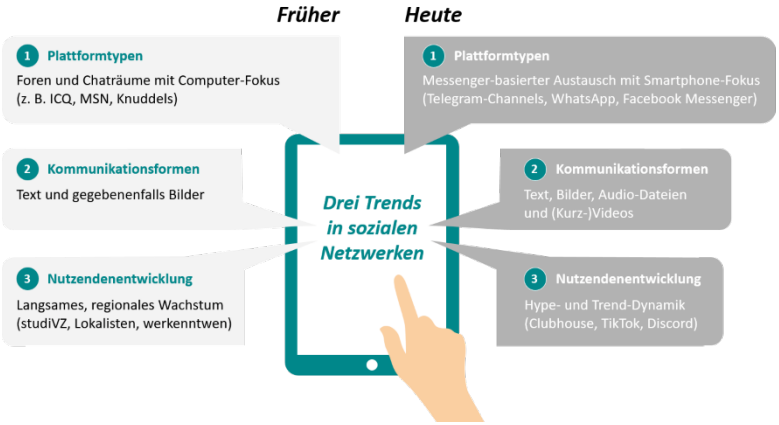


Abbildung 1: Drei Trends in sozialen Netzwerken (eigene Darstellung)

Darüber hinaus drängen jährlich neue Dienste auf den Markt – in den vergangenen Jahren beispielsweise zahlreiche Angebote im Bereich der Direktnachrichten (z. B. Telegram, Signal, Facebook Messenger) oder des sogenannten Lip Sync (z. B. TikTok sowie z. T. Snapchat oder Instagram).[2] Hierbei kommt es teilweise zum **sprunghaften Anstieg von Nutzendenzahlen, wodurch eine Plattform auch für die Polizeiarbeit an Relevanz gewinnt**. Am Beispiel von Instagram lässt sich dies gut verdeutlichen: Innerhalb eines Jahres konnte das soziale Netzwerk die Zahl seiner Nutzenden weit mehr als verdoppeln. Sie stieg von 7 Millionen Anfang 2017 auf 17 Millionen Ende 2018.[3]

[1] 25 Jahre ARD/ZDF-Onlinestudie (09.11.2021): Nach Corona-Tief steigt die Unterwegsnutzung wieder, Streaming und die Mediatheken sorgen weiter für mehr Mediennutzung im Internet, https://www.ard-zdf-onlinestudie.de/files/2021/Beisch_Koch.pdf, zuletzt abgerufen am 26.10.2022.

[2] Our World in Data, Esteban Ortiz-Ospina (18.09.2019): The rise of social media, https://ourworldindata.org/rise-of-social-media, zuletzt abgerufen am 26.10.2022.

[3] KONTOR 4, Ronja Tonn (03.01.2022): Social Media 2022: Aktuelle Nutzerzahlen, https://www.kontor4.de/beitrag/aktuelle-social-media-nutzerzahlen.html#social_media_zahlen, zuletzt abgerufen am 26.10.2022.

Soziale Medien stellen zwar nur einen – wenn auch wichtigen – Teilbereich des Umgangs mit im Internet grundsätzlich frei verfügbaren Daten dar. Dennoch kann ihre **dynamische Entwicklung stellvertretend für andere Internet-Bereiche** verstanden werden, in denen es ebenfalls zu **schnellen Veränderungen von Plattformen** (z. B. von klassischen Foren hin zu Telegram-Kanälen), **Kommunikationsformen** (z. B. die Verschiebung von Text über Audio-Nachrichten hin zu Kurz-Videos) oder **Nutzendenzahlen** (z. B. studiVZ 2010 vs. TikTok 2020) kommt.

Diese Dynamik stellt auch die Polizei vor Herausforderungen: Denn die Strafverfolgung oder Gefahrenabwehr mithilfe von Informationen aus dem Internet ist nur dann erfolgreich, wenn die damit einhergehende „Informationsflut" bewältigt werden kann. Unter dem Stichwort **Open Source Intelligence** nähert sich die Polizei der **Informationsgewinnung aus offenen Quellen**, die heute meist im Internet zu finden sind. Von Webseiten über soziale Netzwerke bis hin zu technischen Details: Das Internet bietet eine **Fülle von Informationen, die als Grundlage polizeilicher Erkenntnisse dienen können**.

Drei Herausforderungen für die Arbeit der Polizei mit offenen Internet-Daten

Mit den wachsenden Datenmengen, wechselnden Kommunikationsformaten und dem schnellen Auftauchen und Verschwinden von Internet-Quellen steigen auch die Ansprüche der Polizei an die Anwendungen zur Erhebung und Verarbeitung von Internet-Daten. **(1) Eine moderne OSINT-Software muss schnell auf Veränderungen reagieren können.**

Allerdings nützt die beste Ermittlungs-Software nichts, wenn man nicht weiß, wie sie eingesetzt werden soll oder, wenn sich der Software-Einsatz nicht ebenso zügig weiterentwickelt wie die Informationsverbreitung im Internet selbst. Das heißt im Klartext: Für die erfolgreiche Polizeiarbeit im Internet **kommt es** neben einer adäquaten Software auch **auf die Methodik an – bei der fachlichen Aus- und Weiterbildung** von Ermittlerinnen und Ermittlern **sowie deren Vernetzung**.

Im Laufe einer immer stärkeren Verbreitung von Smartphones haben Anwenderinnen und Anwender „gelernt", dass Software ohne ausführliche Erklärung auskommt und „einfach mal rumklicken" schon zu einem ganz guten Ergebnis führt. Dieses Prinzip gilt für OSINT nicht. **(2) Für eine umfassende und professionelle Recherche brauchen OSINT-Anwenderinnen und -Anwender Detailwissen**, das weit über Klicken und Ausprobieren hinausgeht. Doch auch dieses Detailwissen entwickelt sich nicht annähernd so rasant weiter wie Plattformen und Informationen im Internet selbst.

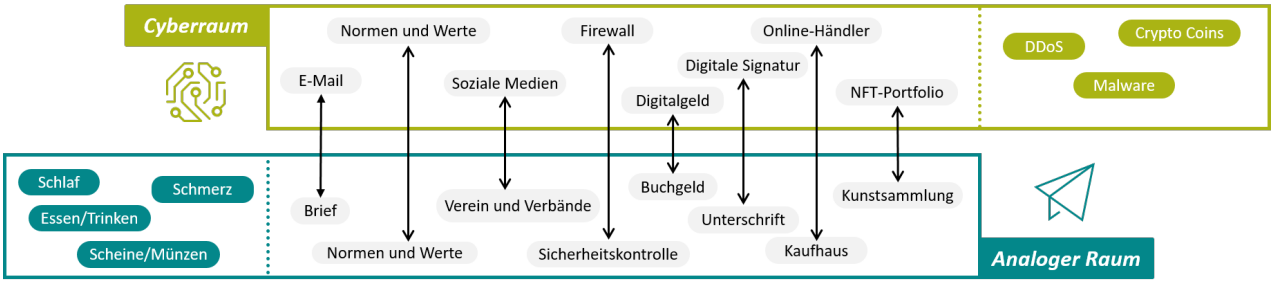


Abbildung 2: Ähnliche Phänomene im analogen und Cyberraum (eigene Darstellung)

Das Internet durchdringt alle Lebensbereiche und es spiegelt den analogen Raum: Briefe werden zu E-Mails, Kaufhäuser zum Online-Handel und Bargeld wird zur Kryptowährung. Diese Anwendungsbreite stellt eine weitere Herausforderung für die polizeiliche Arbeit mit OSINT dar: **(3) Die Fähigkeiten von Internet-Ermittlern und OSINT-Analystinnen sind nicht klassisch einem Deliktfeld zuzuordnen.** OSINT-Informationen sind

in den Bereichen von Cybercrime, organisierter Kriminalität oder des Internet-Betrugs genauso relevant wie im polizeilichen Staatsschutz, bei Vermisstenfällen oder der Bekämpfung von Kinderpornografie.

Diese Vielseitigkeit führt dazu, dass **OSINT-Bereiche organisatorisch unterschiedlich verortet** sind: Manche Polizeibehörden siedeln OSINT-Kompetenz in **Fachreferaten** an, die besonders intensiv mit dem Internet oder offenen digitalen Informationen arbeiten (z. B. Cybercrime oder Internet-Betrug). Andere Behörden zentralisieren die OSINT-Fähigkeiten in **Fachbereichen für die Internet-Ermittlung**. Im Bereich des Internet-Monitorings verhält es sich genauso: Die Expertinnen und Experten sind teilweise direkt in Leitstellen, Lagezentren oder auch speziellen Internet-Monitoring-Referaten verortet. Die **unterschiedliche Zuordnung** beeinflusst das Zugehörigkeitsgefühl und führt zum Teil zu unnötigen Abgrenzungen zwischen Kolleginnen und Kollegen, was eine **effiziente Ermittlung tendenziell erschwert**. Denn wer weiß, vielleicht ist ja die Herangehensweise der OSINT-Analystin bei der Betrugsbekämpfung auch für den Beamten im Bereich der Bekämpfung von Cybercrime relevant?

Internet-Ermittlerinnen und OSINT-Analysten bei der Polizei stehen somit vor einer dreifachen Herausforderung: Die **Anwendungsbereiche von Internet-Ermittlungen** sind **vielseitig** und **organisatorisch „zersiedelt“**, OSINT-Quellen und -Methodik **entwickeln sich rasant** und bessere Software allein löst das Problem nicht.

Drei Lösungsansätze zur Verbesserung der polizeilichen OSINT-Fähigkeiten

Um mithilfe von Open Source Intelligence die polizeiliche Arbeit im Internet zu verbessern, bieten sich drei Lösungsansätze in den Bereichen Software, Vernetzung und Weiterbildung an:

1. **Modulare Software-Anwendungen** adressieren die vielschichtigen und dynamischen Bedarfe in Bundes- und Landesbehörden.
2. Die bessere technische Ausstattung muss von einem **„Community Building“-Ansatz** zur besseren Vernetzung flankiert werden.
3. **Organisatorischen Herausforderungen** im Bereich OSINT müssen Sicherheitsbehörden im Rahmen der **fachlichen Weiterentwicklung** begegnen, beispielsweise mithilfe des „T-Modells“ zur Fähigkeiten-Entwicklung (siehe Abbildung 4).

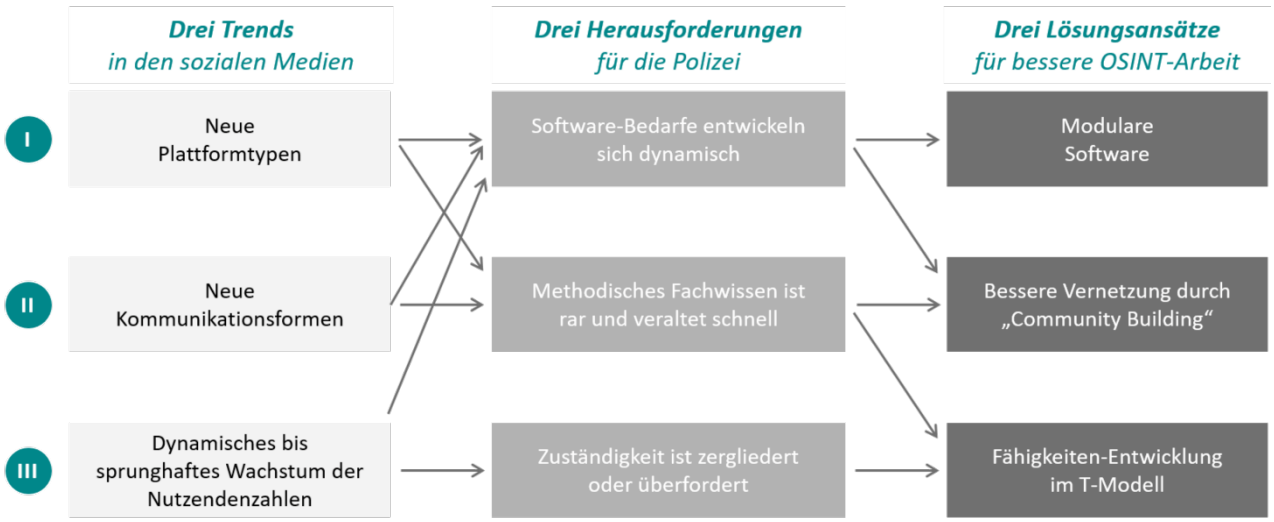


Abbildung 3: Drei Trends – drei Herausforderungen – drei Lösungsansätze (eigene Darstellung)

Bedarfsgerechte und modulare Software

Unter einem Modul versteht man im Bereich der Software-Entwicklung eine „funktional geschlossene Einheit", die einen „bestimmten Dienst bereitstellt".[4] **Modulare Anwendungen haben zahlreiche Vorteile**: Sie sind einfach zu warten, leicht erweiterbar und können auch cross-funktional in anderen Anwendungen zum Einsatz kommen. Das heißt, bei neuen oder geänderten Bedarfen kann ein Modul schnell angepasst werden.

Zudem können Funktionalitäten in einem modularen System mithilfe eines Rechte- und Rollenkonzepts Fall- oder Maßnahmen-spezifisch zu- oder abgeschaltet werden. Hinsichtlich verfassungs- oder datenschutzrechtlicher Prüfungen haben Behörden, die die Software einsetzen, die Möglichkeit, **einzelne Module auf der Grundlage der unterschiedlichen Polizeigesetze zur Gefahrenabwehr zuzuschalten** und diese vor der Beschaffung oder im Falle einer Prüfung getrennt beschreiben und bewerten zu lassen.

Modulare und flexibel anpassbare Anwendungen verbessern die polizeilichen Fähigkeiten im Bereich der Internet-Ermittlung und sorgen dafür, dass die polizeilichen **Anwenderinnen und Anwender schnell auf Veränderungen reagieren** können. Wichtig ist hierbei zu wissen, dass es nach heutigem Stand keine Universallösung gibt. Die Vorstellung von einer „eierlegenden Wollmilchsau" verkennt die Vielschichtigkeit der fachlichen OSINT-Anforderungen, die sich aus der großen Bandbreite an Deliktsfeldern ergibt. Die Nutzung von frei verfügbaren Internet-Daten im Bereich der Cybercrime-Bekämpfung (z. B. Krypto-Transaktionen, Schadcode-Tracking, Darknet-Recherche) ist gänzlich anders gelagert als im Bereich der Einsatz-begleitenden Internet-Recherche bei den Leitstellen (z. B. soziale Netzwerke, Chat-Verläufe).

Ebenso müssen modulare Lösungen auf die **unterschiedlich ausgeprägten Fähigkeiten der Anwenderinnen und Anwender** eingehen können: Während eine Recherche auf Kleinanzeigen-Portalen für einen einfachen Fahrraddiebstahl auch für einen polizeilichen Sachbearbeiter in der Fläche mit einer einfachen Anwendung möglich sein muss, sind komplizierte Internet-Ermittlungen im Bereich der Kinderpornografie-Bekämpfung OSINT-Spezialistinnen und Profi-Anwendern vorbehalten. Modular aufgebaute Ermittlungsanwendungen müssen den diversen Anforderungen unterschiedlicher Nutzendengruppen und Deliktfeldern gerecht werden.

Das Hauptargument für den Einsatz einer modularen Software im Bereich OSINT ist die dynamische Entwicklung im Internet: Um schnellstmöglich auf **neue Austauschplattformen zugreifen** zu können, müssen **Zugänge und Schnittstellen** umgehend und **einfach aufgebaut oder angepasst** werden können, **ohne die gesamte Software umstellen** zu müssen**.** Diese Dynamik macht es zwingend notwendig, dass Sicherheitsbehörden Veränderungen im Internet, wie etwa die Weiterentwicklung von sozialen Netzwerken und Online-Spieleplattformen zum sogenannten „Metaverse", stets im Blick haben müssen.

Die Internet-Ermittlung muss künftig auch in diesen virtuellen Begegnungsräumen aktiv sein, denn bereits heute werden auf Metaverse-Plattformen Milliardensummen umgesetzt, illegale Aktivitäten beobachtet und am Internet der Zukunft gearbeitet. Das Thema Trend-Monitoring ist daher untrennbar mit der modularen Software-Entwicklung für die polizeiliche Internet-Ermittlung verbunden und muss als solches in den Sicherheitsbehörden verankert werden.

[4] Definition „Modul" in Gablers Wirtschaftslexikon, siehe https://wirtschaftslexikon.gabler.de/definition/modul-40077/version-263472.

Bessere Vernetzung durch Community Building

OSINT-Anwenderinnen und -Anwender brauchen ein **umfassendes und verlässliches Netzwerk Gleichgesinnter**, die Tipps bei der konkreten Ermittlung, Links zu neuen Werkzeugen und Weiterbildungsangeboten oder Ratschläge zu kreativen Ermittlungsansätzen geben können. Genau diese Wünsche und Bedarfe äußern OSINT-Anwenderinnen und -Anwender sowohl im direkten Austausch als auch bei strukturierten Befragungen. Insbesondere auf der Ebene der OSINT-Sachbearbeitung wird die mangelnde Vernetzung beklagt und der Wunsch nach mehr professionellem Austausch im Themenfeld von OSINT geäußert.

Der **aktuell niedrige Vernetzungsgrad** ist vor dem Hintergrund der wachsenden Relevanz und großen Dringlichkeit von polizeilicher Arbeit im Bereich OSINT besonders problematisch. Als **größte Herausforderung** beschreiben die Expertinnen und Experten, dass es **schwierig sei, „am Puls der Zeit“** zu bleiben, weil sich Informationsquellen, Ermittlungspraktiken und Anwendungsbereiche so schnell verändern.

Der Aufbau einer **Gemeinschaft von OSINT-Expertinnen und -Experten** aus den **Polizei- und Strafverfolgungsbehörden (Community Building)** verfolgt das Ziel, die handelnden Akteure über die Behörden- und Landesgrenzen hinaus miteinander in Kontakt zu bringen. Im persönlichen Kontakt und auf gemeinsamen Veranstaltungen kann fachliches, technisches und methodisches Anwendungswissen ausgetauscht und erweitert werden. Über den **Auf- und Ausbau von Tools, Technik und Methoden im Bereich OSINT** erfolgt mittelbar auch eine Vereinheitlichung von Vorgehensweisen zwischen den beteiligten Akteuren, was den zukünftigen Austausch wiederum vereinfacht.

Netzwerk-Veranstaltungen sollten idealerweise **im geschützten Behördenkreis** stattfinden. Bislang waren in derartige Veranstaltungen immer auch Vertreterinnen und Vertreter von Industrie-Unternehmen eingebunden, die über den jeweils aktuellen Stand der Technik informierten. Der Nachteil dabei: Die Anwesenheit von Externen verhinderte den vertrauensvollen Austausch zwischen den OSINT-Expertinnen und -Experten zu konkreten Sachverhalten oder Problemen bei der Internet-Ermittlung.

Fachliche Weiterentwicklung am Beispiel des T-Modells

Neben der Ausstattung mit bedarfsgerechter und modularer Software sowie der besseren Vernetzung der OSINT-Anwenderinnen und -Anwender ist auch eine **längerfristige Perspektive** wichtig: Gerade vor dem Hintergrund der Social-Media-Trends und angesichts der bereits existierenden Herausforderungen muss schon heute Sorge für die zukünftige Aufstellung im Bereich OSINT getragen werden. Im Rahmen der fachlichen Weiterentwicklung ist insbesondere die organisatorische Aufstellung der Polizei bei der Arbeit mit OSINT und im Kontext der Internet-Ermittlung relevant. Mithilfe des **„T-Modells“** kann beispielsweise die **breite Vermittlung** von grundlegenden **OSINT-Kenntnissen Spezialteams entlasten.**

Polizeibehörden, die die Bedeutung von offen zugänglichen Informationen für die Ermittlungsarbeit oder bei der Gefahrenabwehr bereits erkannt haben, fördern die Vertiefung der **Expertise durch bessere Software**, eine **einheitlichere Methodik** und

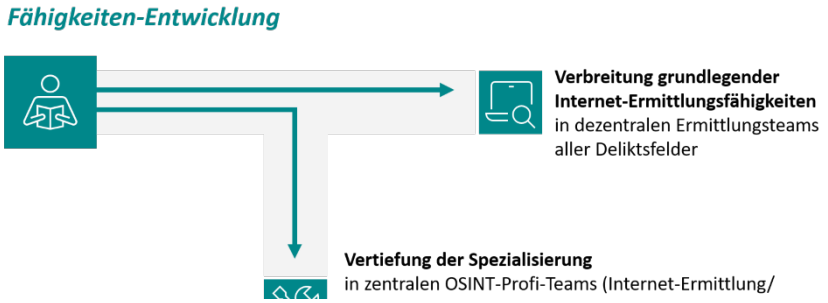


Abbildung 4: T-Modell zur Fähigkeiten-Entwicklung in der Tiefe und Breite (eigene Darstellung)

mehr **Austausch und Vernetzung** (vertikaler T-Strich). Die Expertise ist meistens, aber nicht immer, in Spezialreferaten zur Internet-Ermittlung angesiedelt. Diese bearbeiten die „harten Fälle“ und unterstützen Deliktfeld-spezifische Fachreferate (z. B. Cybercrime, Staatsschutz, Internet-Betrug). Da aber OSINT-Ermittlungen immer mehr an Bedeutung gewinnen und Erkenntnisse zum Beispiel aus sozialen Netzwerken auch in Massen- und Breitenphänomen wie der Kfz-, Einbruchs- oder Diebstahlsermittlung relevant sind, sind **Internet-Spezialreferate häufig überlastet**. Aber nicht alle diese Anfragen benötigen Spezialwissen, sondern könnten bereits mit grundlegenden Internet-Ermittlungsfähigkeiten gelöst werden.

Um diesen Herausforderungen zu begegnen, ist neben der Verstärkung der Spezialteams auch die **Verbreitung allgemeiner Internet-Fähigkeiten in der Breite notwendig** (horizontaler T-Strich). Die Stärkung von OSINT-Fähigkeiten auf Einstiegs- oder Fortgeschrittenen-Niveau in der Breite kann durch einfache Software-Lösungen zur Informationssammlung, Visualisierung und Ausleitung und/oder durch methodische Schulung im Grundrepertoire der Internet-Ermittlungsarbeit erfolgen.

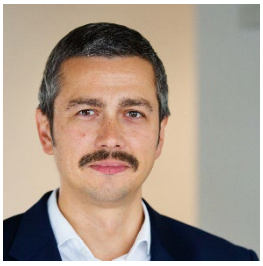
OSINT-Software für Einsteigerinnen und Einsteiger muss **besonders benutzungsfreundlich** sein, da die Komplexität einer Tiefenrecherche Personen ohne Spezialwissen und Erfahrung schnell überfordert. Mit grundlegenden Internet-Fähigkeiten kann die Arbeit in dezentralen Ermittlungsteams aller Deliktfelder beschleunigt werden, da keine Weiterleitung und Abstimmung durch die Beteiligung von Spezialreferaten notwendig ist. Diese werden so entlastet und können sich auf die „wirklich harten Fälle“ konzentrieren.

Mit Open Source Intelligence auf dem Weg zur besseren Internet-Ermittlung bei der Polizei

Das **Internet wächst und entwickelt sich** kontinuierlich weiter – und damit gewinnen **frei zugängliche Informationen** aus sozialen Netzwerken, von Webseiten oder aus offenen Datenquellen zunehmend an Bedeutung.

Diese **Entwicklungstrends** – gepaart mit den fachlichen, technischen und organisationsbezogenen Herausforderungen von Strafverfolgungsbehörden – **zwingen die Polizei zum Handeln.** Damit dies nicht von jeder Behörde alleine geleistet werden muss, sollten Bund und Länder an gemeinsamen Lösungsansätzen arbeiten, um akuten Software-Bedarfen zu begegnen, die Vernetzung der Expertinnen und Experten auszubauen und die Polizei langfristig besser für die Arbeit mit OSINT-Informationen aufzustellen.

Kontakt



Erik Hersemann
Principal Expert
T +49 30 25 76 79-150
M +49 172 355 54 71
Erik.Hersemann@pd-g.de

Johannes Jausen
Manager

M +49 172 729 16 21
Johannes.Jausen@pd-g.de

Louis Jarvers
Senior Consultant

M +49 172 349 03 27
Louis.Jarvers@pd-g.de

PD – Berater der öffentlichen Hand GmbH
Friedrichstr. 149
10117 Berlin
pd-g.de/

Erik Hersemann ist Principal Expert bei der PD – Berater der öffentlichen Hand GmbH und Leiter des Bereichs Öffentliche Sicherheit. Sein Beratungsschwerpunkt liegt auf der Digitalisierung von Polizei und Sicherheitsbehörden. Er ist zudem Leiter des PD-Thinktanks „Öffentliche Sicherheit".

Johannes Jausen ist Manager bei der PD – Berater der öffentlichen Hand GmbH im Bereich Öffentliche Sicherheit. Sein Beratungsschwerpunkt liegt auf den Themen Künstliche Intelligenz und Datenanalyse bei Sicherheitsbehörden.

Louis Jarvers arbeitet als Senior Consultant bei der PD – Berater der öffentlichen Hand GmbH im Bereich Öffentliche Sicherheit. Sein Beratungsschwerpunkt liegt auf dem Thema Datenanalyse bei Sicherheitsbehörden, insbesondere Internet-Ermittlung und Open Source Intelligence. Er ist der Hauptautor dieses Fachbeitrags.

PD – Berater der öffentlichen Hand GmbH

Die PD ist privatrechtlich als GmbH organisiert und liegt zu 100 Prozent in den Händen öffentlicher Gesellschafter. Mit rund 600 Beraterinnen und Beratern in den Geschäftsbereichen Strategische Verwaltungsmodernisierung sowie Bau, Infrastruktur und Kommunalberatung bietet die PD als Inhouse-Beratung der öffentlichen Hand umfassende projektbezogene Beratungs- und Managementleistungen zu moderner Verwaltung und Investitionsvorhaben ausschließlich für Bund, Länder, Kommunen und sonstige öffentliche Auftraggeber an.

Die Expertinnen und Experten des Bereichs Öffentliche Sicherheit bei der PD fokussieren die Themen innere Sicherheit, Polizei und Sicherheitsbehörden. Im Rahmen ihrer Thinktank-Arbeit beschäftigen sie sich mit Lösungsansätzen für die Zukunftsfragen der öffentlichen Sicherheit.