Enhanced internet investigation through open-source intelligence (OSINT)

Three trends, challenges and solutions for police work using OSINT

Berlin, 07.11.2022

Enhancing internet investigation for the police using open-source intelligence

Remember MySpace, Google+, Second Life? Social media platforms have only recently sprung up as the revolutionaries of internet communication, but a host of them are already exiting the stage. The rapid and regular turnover of devices and internet trends has brought forth new platforms like TikTok, Snapchat, BeReal, Discord or Twitch, while sites like MySpace, Google+ or studiVZ (a networking platform for German students) are no longer part of the show.

These trends present growing challenges to policing work using internet data. Modular software, greater interconnectedness and more training in methods and approaches in the field of **open-source intelligence (OSINT)** gathering can help remedy this. The team from PD's Public Security division is working – in cooperation with security authorities – on solution-based approaches to **enhance police investigation using the internet**.

Three trends in social networks – against the backdrop of a steadily growing flood of information

The fast-paced developments in the social media landscape follow various trends: around 20 years after their introduction, social networks are expanding their reach in Germany year by year – not just in terms of the sheer **number** of users but also when it comes to the **time** they spend each day online.[1]

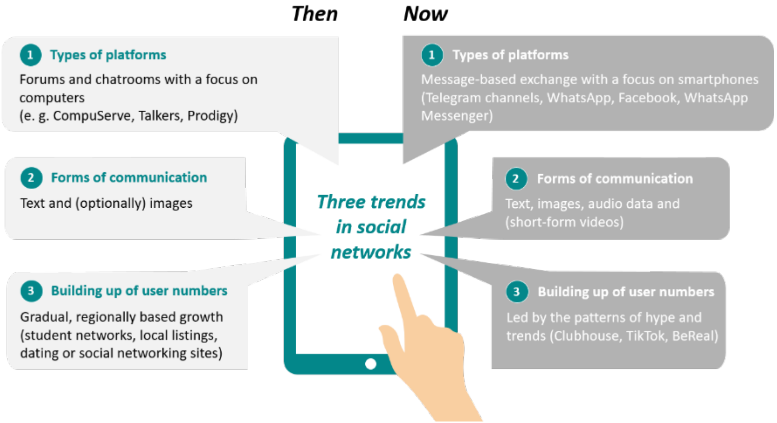

Then
Now
1 Types of platforms
Forums and chatrooms with a focus on computers (e. g. CompuServe, Talkers, Prodigy)
2 Forms of communication
Text and (optionally) images
3 Building up of user numbers
Gradual, regionally based growth (student networks, local listings, dating or social networking sites)
Three trends in social networks
1 Types of platforms
Message-based exchange with a focus on smartphones (Telegram channels, WhatsApp, Facebook, WhatsApp Messenger)
2 Forms of communication
Text, images, audio data and (short-form videos)
3 Building up of user numbers
Led by the patterns of hype and trends (Clubhouse, TikTok, BeReal)

Figure 1: Three trends in social networks (PD's own depiction)

At the same time the way platforms are used is constantly evolving: while the network studiVZ, with roughly 6.2 million users in 2009, was one of the most successful online providers in Germany, this platform has now vanished from our screens.

Alongside this, new providers are continually jostling for market position – in recent years, for example, these have included a range of offerings in the area of direct messaging services (Telegram, Signal, Facebook, WhatsApp Messenger) or so-called 'lip sync' platforms (like TikTok, Snapchat, and Instagram).[2] This has been accompanied by a **dramatic increase in user numbers – making platforms relevant to policing work**. Instagram is a notable example of this: in just a few years it has managed to more than double its number of users. From seven million users at the start of 2017, by the end of 2018 this figure had grown to 17 million.[3]

[1] ARD/ZDF-Onlinestudie 2022 (09.11.2021): Mediale Inhalte verstärken Internetnutzung [Media content increases internet use], https://www.ard-zdf-onlinestudie.de/ardzdf-onlinestudie/pressemitteilung/, accessed on 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, accessed on 26.10.2022.

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

Social media sites represent only one aspect – though an important one – of the way in which freely available data is dealt with on the internet. But we can view the dynamic way it has developed as representative of other areas of the internet landscape, including **rapid changes in platforms** (for example, from traditional forums to Telegram channels), **forms of communication** (the shift from text-based to audio messaging to short-form videos) or **user numbers** (studiVZ in 2010 compared to TikTok a decade later).

This dynamic also presents challenges to policing authorities, because law enforcement or emergency response activity with the aid of data gathered from the internet will only be successful if this 'flood of information' can be managed. The term **open-source intelligence refers to police agencies taking steps towards extracting information from freely available sources**, the most common type of data on the web. From websites and social media networks to technical details about users and site visitors, the internet offers a goldmine of information – a rich seam that can serve as a foundation for police intelligence.

Three challenges for policing work using publicly available internet data

In light of the ever-growing amount of data, changing communications formats and rapid turnover and disappearance of information sources on the net, the demands of police authorities – when it comes to methods of gathering and processing data from the internet – are also increasing. **(1) Up-to-the-minute OSINT software needs to react quickly to this changing landscape.**

However, not even the most state-of-the-art investigation software will help you if you don't know how to put it into practice, or if the ways in which the software is deployed do not evolve just as quickly as the way information itself is distributed across the internet. In other words, successful policing work using the net requires not just effective software; it also calls for a **set of methods – through the professional training and networking of investigators**.

As smartphones have become ever more commonplace, their users have increasingly realised that software doesn't come with detailed 'how to' guides; our default mode is to just fiddle around with a device and see what works. This is *not* the principle that underlies OSINT. **(2) For comprehensive and professional research activities, OSINT users need detailed know-how**, far beyond the 'click it and see' approach. However, this detailed knowledge is developing and refining itself nowhere near as fast as the platforms and information on the internet itself.

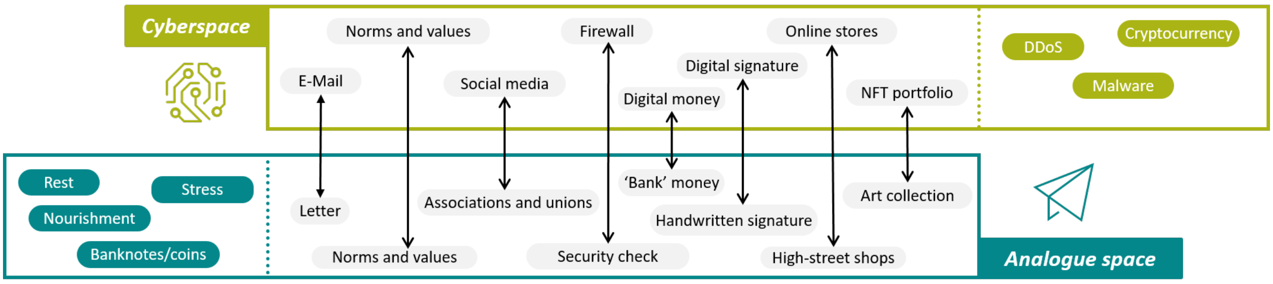


Figure 2: Comparable phenomena in the analogue and digital worlds (PD's own depiction)

The internet pervades every corner of our lives and is a mirror of the analogue world: letters become e-mails, high-street shops become online stores and the money economy gives way to cryptocurrencies. The very diversity of these applications represents another challenge when it comes to policing work using OSINT methods. **(3) The skillsets of internet investigators and OSINT analysts are *not* associated with one**

'traditional' crime domain. Information derived from OSINT relating to fields such as cyber-crime, organised criminality or internet fraud is just as pertinent as it is in police-led public safety measures, missing persons cases or in tackling child pornography.

The multifaceted nature of this challenge means that, in organisational terms, **OSINT-based fields of work are located at different units or departments**. Some policing authorities 'park' their OSINT competencies across different units whose members work particularly intensively with the internet or with freely available digital information (for instance, in units dedicated to cyber-crime or internet fraud) but are not internet investigation units per se. Other agencies centralise OSINT capabilities within **specialist departments** devoted to **internet-based investigation alone**. It's the same story in the field of internet monitoring, with expert investigators either based at central command and control centers, situation rooms or in units specialising in internet monitoring. The **different way in which skills are allocated** has an impact on staff members' sense of belonging and can lead to unnecessary demarcations and distinctions between colleagues, which **can negatively influence efficient investigation**. Because – who knows – maybe the approach that an OSINT analyst is using for a fraud investigation could also be the right path to follow for an officer tackling cyber-crime?

Internet-oriented investigators and OSINT analysts working for policing authorities face a threefold challenge: in the context of internet investigations, the areas of application are **varied** and **organisationally fragmented**, OSINT-related source materials and methodologies are **rapidly evolving**, and more effective software doesn't on its own resolve the problem.

Three solutions for enhancing OSINT competencies in policing work

To improve internet-based policing with open-source intelligence, three solutions in the areas of software, interconnectedness (networking) and further skills training are at hand:

1. **The use of modular software** addresses complex, dynamic and ever-evolving needs of the relevant authorities on the local, regional and national levels.
2. More efficient technical capabilities need to be accompanied by a **'community building' approach to achieve better** interconnectedness and networking among agencies and stakeholders.
3. **Security services and public safety bodies must confront organisational and operational challenges** when it comes to **professional training**, for example with the help of the 'T' model of skills development (see figure 4).

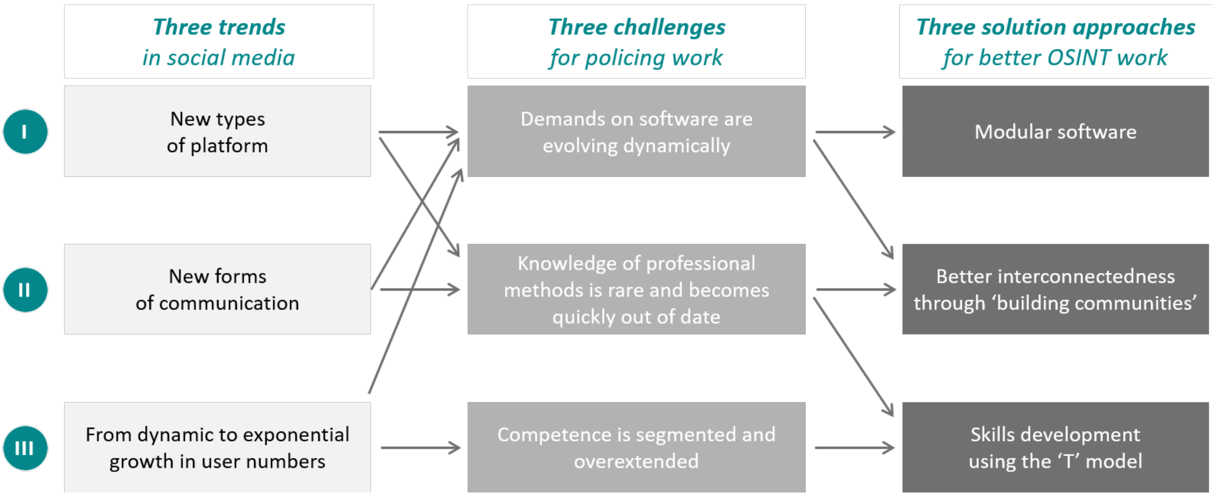


Figure 3: Three trends – three challenges – three solution approaches (PD's own depiction)

Needs-based, demand-driven, and modular software

In terms of software development, a module is a “functionally self-contained unit” that “performs a particular service”.[4] **The application of modules has several advantages**: they’re straightforward to maintain, can be upgraded easily and can be used in a cross-functional way with other applications. In other words, a module can be swiftly adapted to new or altered requirements.

Alongside this, features and functions in a modular system can be activated or disabled – depending on operational necessity and on a case-by-case basis – with the help of a set of parameters defining access privileges and roles. In terms of inquiries relating to constitutional legality or data protection rights, authorities implementing this software have the opportunity to **switch on individual modules on the basis of an array of police regulations governing emergency response and public protection**, and to have these separately outlined and evaluated before an inquiry is initiated or in the case of an ongoing investigation.

Modular, flexible and adaptable applications enhance policing competencies in the realm of internet investigation and ensure that **users can react in an agile way to changing circumstances**. With one important proviso: there is currently no universal solution. Holding to the idea of a universal solution is to fail to acknowledge the multifaceted nature of the specialist requirements of intelligence gathering using openly sourced information, a diversity that arises from the broad range of crime domains. The use of freely available internet-derived data when it comes to tackling cyber-crime (for instance when researching cryptocurrency transactions, tracking malware or tracing activities on the darknet) is drastically different from how internet research (for example into social networks, chatrooms and messaging platforms) is used in central control points to support operations.

Modular solutions also need to be geared towards **users’ distinctive competencies and skills**. Whereas combing through small-ads websites to investigate a straightforward case of bicycle theft needs to be possible for a police support officer using a simple application, more complex internet-based investigation when it comes to tackling child pornography cases are reserved for specialists and expert users in OSINT. Investigative applications that are devised in a modular way must be tailored to the diverse requirements of a wide variety of user groups and crime domains.

The principal argument for putting in place modular software in the OSINT context is based on the way the internet is evolving dynamically. To gain access as quickly as possible to new communications and exchange platforms, **entry points and interfaces** would have to be set up immediately – these should be **easy to implement and adjust**, without the need to reconfigure or reboot the entire software. This momentum of change makes it absolutely essential that security and public safety authorities are constantly alert to the altered digital landscape – for example, with social networks and online gaming platforms starting to extend themselves to the so-called ‘metaverse’.

The internet-based investigation of the future must also be an active player in these virtual meeting places, because billions are already being invested and transacted today on metaverse platforms, to scrutinise illegal activities and continue research into the internet of the future. The theme ‘**trend monitoring**’ is therefore inextricably connected to the development of modular software for internet-based police investigation and also needs to be embedded in the work of security and public safety authorities.

[4] For the definition of ‘module’, see https://dictionary.cambridge.org/dictionary/english/module.

Improving interconnectedness by building communities

OSINT users need a comprehensive and reliable **network of kindred spirits** who can offer and share tips and instances of best practice regarding specific investigations, links to new tools, opportunities for further training or advice on innovative and creative enquiry pathways. OSINT users voice these desires and demands in face-to-face exchanges as much as they do in more formal surveys. They draw attention to this lack of effective networking particularly at the level of OSINT-oriented case processing, speaking often of their wish for more professionally organised forums of exchange in the field of open-source intelligence gathering.

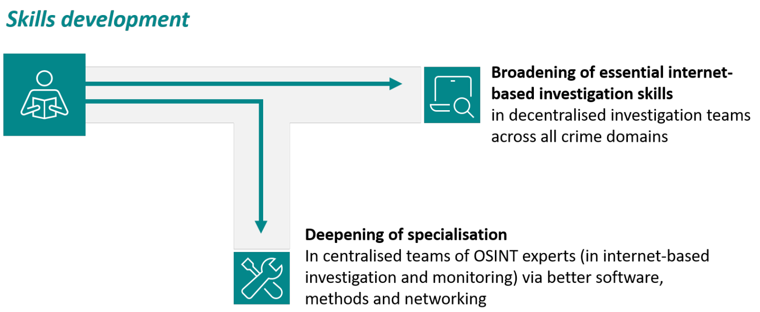
Against the backdrop of OSINT's growing relevance and priority for policing work, this **current low level of interconnectedness** is especially problematic. Experts point out that the greatest challenge is how hard it is to keep abreast of the latest developments because sources of information, investigatory practices and areas of application are changing so rapidly.

Building a community of OSINT experts made up of members of police and law enforcement authorities aims at bringing professionals together beyond the usual demarcations of different authoritative or regional bodies. In this way, they can exchange, broaden and deepen their knowledge and expertise when it comes to professional, technical and methodological know-how via personal contact – in events, get-togethers and conferences. **Developing and expanding the range of OSINT tools, techniques and methods** should also lead to participants agreeing on a standard set of approaches and procedures, which in turn will make future exchanges of know-how easier to coordinate.

Networking events should ideally take place among staff from the relevant authorities in the form of **internal and safeguarded sessions**. Previously, these types of event have often involved representatives from industry and private companies who informed participants about the current state of the art relating to technological solutions on a case-by-case basis. The downside of this is that the presence of external actors has tended to hinder open and confidential exchange between OSINT specialists regarding specific issues, cases or problems arising from net-based investigation.

Professional development – the example of the 'T' model

The third strand to this approach – alongside the provision of needs-based, demand driven, modular software and improvements to how OSINT specialists connect with each other – is the need for a **long-term perspective**. Against the backdrop of trends in social media and in light of existing challenges, care must be taken *now* to ensure how OSINT is to be deployed in future. When it comes to further professional development, of particular relevance will be the nature of the **organisational set-up** of policing authorities in relation to OSINT and in the context of internet-based investigating. As an example, the 'T' model can help, by paving the way to a broad transmission of essential OSINT know-how, to free up specialist teams**.**



Broadening of essential internet-based investigation skills
in decentralised investigation teams across all crime domains

Deepening of specialisation
In centralised teams of OSINT experts (in internet-based investigation and monitoring) via better software, methods and networking

Figure 4: 'T' model for a broadening and deepening of skills development (PD's own depiction)

Policing and risk-prevention authorities, which are already alert to the significance of publicly available information for their investigative work, are encouraging a deepening of expertise by way of **better**

software, a more **integrated and standardised set of methods** and a greater degree of **exchange and networking** (represented by the vertical line of the 'T' model in figure 4). This expertise is generally, though not always, to be found in specialist units tasked with internet-based investigation. These work on the 'hard to crack' cases and act as support for subject-specific divisions dealing with various crime domains (for instance, cyber-crime, national security or online fraud). However, precisely because OSINT-based investigations are becoming ever more important and as insights – derived, for example, from social-media networks – are relevant to the investigation of widespread phenomena like vehicle theft, house burglary or other types of theft, **specialist units dedicated to internet-based investigation are often overstretched**. However, not every enquiry demands specialist knowledge; many can in fact be cleared up by those with the requisite skills in the essentials of internet-based enquiry.

To address these challenges, alongside the strengthening of specialist teams a **broadening of overall internet skills and competences is key** (the horizontal line of the 'T' model in figure 4). A broad-based consolidation of an OSINT skillset, whether at the beginners' or the advanced level, can be achieved by means of user-friendly software solutions for information gathering, visualisation tools and data filtering and/or through methods-based training in the basic repertoire of internet-based investigative work.

OSINT software for beginners needs to be especially user-friendly, as the complex nature of intensive research can quickly overwhelm those who don't have specialist knowledge. Having essential internet skills can speed up the work of staff operating in decentralised teams of investigators, because there's no need to forward enquiries and adjust investigative approaches when specialist units are not involved in the procedure. This helps to free up the time and resources of specialist units, which can then concentrate on 'cracking the tough cases'.

Open-source intelligence as a pathway to enhancing internet-based police investigation

The internet continues to expand and extend its reach – and, as a result, freely accessible information from social networks, websites or publicly available data sources is becoming ever more important.

These **trends** – coupled with the challenges faced by law enforcement authorities in the professional, technological and organisational spheres – **oblige policing agencies to act**. To prevent each individual authority having to 'reinvent the wheel' in isolation, national and regional agencies should work together to arrive at common solutions to address the urgent need for appropriate software, to build up networked communities of experts, and to train and prepare policing staff – much more effectively and on a long-term basis – for mining the rich seams of information generated by open-source intelligence gathering.

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 is a principal expert at PD – Berater der öffentlichen Hand GmbH, and leads the Public Security division. His main area of consultancy expertise is digitalisation with regard to the work of policing and public safety authorities. He is also head of PD's 'Public Security' thinktank.

Johannes Jausen is a manager at PD – Berater der öffentlichen Hand GmbH, in the Public Security division. His consultancy activities focus on the themes of artificial intelligence and data analysis in the context of the work of security and public safety authorities.

Louis Jarvers works as a senior consultant at PD – Berater der öffentlichen Hand GmbH, in the Public Security division. His consultancy work focuses on the topic of data analysis in security authority settings, particularly in the areas of internet investigation and open-source intelligence. He is the main author of this report.

PD – Berater der öffentlichen Hand GmbH (PD – Consultants to the Public Sector)

PD is organised under private law as a GmbH whose ownership is 100% in the hands of public shareholders. With around 600 consultants working in various fields – covering, for instance, strategic administrative modernisation, as well as consulting on construction projects, infrastructure and municipal policy – PD's in-house advisory services for the public sector provide comprehensive and project-related consultancy and management services for modern administration and investment projects exclusively for the German federal government, regional states, municipalities and other public-sector clients.

The experts in PD's Public Security division focus on the topics of internal security, policing authorities and public safety bodies. Their thinktank concentrates on identifying solution pathways for potential issues when it comes to the public safety questions of the future.

Hidden
Champion
2022/23
PUBLIC SECTOR