



Expertise hubs and the credibility challenge for open-source intelligence: insights from usage patterns of a web-controlled radio receiver and related Twitter traffic in the Ukraine war

Anne van Harten, Shawn Donnelly, Pieter-Tjerk de Boer & Roland van Rijswijk-Deij

To cite this article: Anne van Harten, Shawn Donnelly, Pieter-Tjerk de Boer & Roland van Rijswijk-Deij (11 Nov 2024): Expertise hubs and the credibility challenge for open-source intelligence: insights from usage patterns of a web-controlled radio receiver and related Twitter traffic in the Ukraine war, *European Security*, DOI: [10.1080/09662839.2024.2421262](https://doi.org/10.1080/09662839.2024.2421262)

To link to this article: <https://doi.org/10.1080/09662839.2024.2421262>



© 2024 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 11 Nov 2024.



[Submit your article to this journal](#)



Article views: 250







[View related articles](#)



[View Crossmark data](#)

Expertise hubs and the credibility challenge for open-source intelligence: insights from usage patterns of a web-controlled radio receiver and related Twitter traffic in the Ukraine war

Anne van Harten ^a, Shawn Donnelly ^{b,c}, Pieter-Tjerk de Boer ^a and Roland van Rijswijk-Deij ^a

^aDesign and Analysis of Communication Systems Group, University of Twente, Enschede, Netherlands;

^bPublic Administration Section, University of Twente, Enschede, Netherlands; ^cInstitute for Political Science, Leiden University, Leiden, Netherlands

ABSTRACT

This article analyses how new open-source intelligence methods democratise and complement traditional signals intelligence while bundling dispersed expertise required to ensure the quality of data and the confidence we can have in analysis. It examines the case of OSINT activity on web-controlled radio receivers since 2022 about Russian military communications in Ukraine. It uses network analysis to show the extent of information leakage, analysis and collaboration by various actors that perform different tasks of crowdsourcing, vetting and interpreting information to make it actionable. We advance the field in knowledge of open-source intelligence gathering, dissemination and use.

ARTICLE HISTORY

Received 19 July 2024

Accepted 22 October 2024

KEYWORDS

National security; human security; open-source intelligence; coordination; expertise

Introduction

Under what conditions, can radio intercepts available through web-based software-defined radio receivers (WebSDR) contribute to trustworthy and informative intelligence gathering and analysis? WebSDR antennas and receivers allow internet users, even if they do not own radio equipment themselves, to listen to radio communications from commercial, government and amateur transmissions, as well as by military establishments and military units in the field (Websdr.org n.d.). Although open-source intelligence specialists, journalists and military veterans discuss this information on the internet, how reliable are their findings for increasing the supply of intelligence through crowdsourcing that state establishments should take seriously? This paper presents original research on the processing of WebSDR radio intercepts by online communities of specialists with divergent but complementary skill sets, concluding that this form of intelligence crowdsourcing can and should be taken seriously.

Listening and analysing radio communications in conflict scenarios is a core function of state intelligence agencies (IAs) as part of the intelligence community (IC), in which signals

CONTACT Shawn Donnelly  s.donnelly@utwente.nl, shawnwdonnelly@gmail.com

© 2024 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

intelligence (SIGINT) and geographical-temporal location intelligence (GEOSINT) play a core role. Since the dawn of radio, non-state actors have also been listening in to such radio communications using receivers and antennas of their own. Web-based receivers, however, have changed this in two major ways: listening and analysis have become available to a broader group, as no own equipment is needed and make it possible to listen via an antenna in another part of the world. Furthermore, listening and analysis can now happen in a coordinated way, often making use of internet platforms to share insights and information about events of interest and analysis surrounding them. Collectively, this alternative ecosystem is known as open-source intelligence (OSINT). We know a considerable amount about the high level of interest in the OSINT community on security issues, but want to push this knowledge further in three areas:

- To what extent has WebSDR, as a specific means of accessing radio intercepts for discussion and analysis, had a noticeable impact on open-source intelligence (OSINT)?
- To what extent has Twitter-based discussion of WebSDR-accessible material led to any changes in the OSINT community and its output that have implications for how trustworthy their findings are for conventional state security institutions?
- Similarly, to what extent has Twitter-based use of WebSDR-accessible material had any impact on the potential for NGOs and UN tribunals to prosecute war crimes and genocide during or after a conflict? In short, does the advent of WebSDR receivers transform discussions and activities surrounding military and human security?

Our analysis starts with a technical introduction into what WebSDR is and does, and then an overview of the broader, online OSINT community that engages with radio intercepts, in particular, those gathered via WebSDR. The body of the paper presents a novel means of identifying specific groups of users that work with WebSDR material and discuss it with each other online via Twitter. It then uses process tracing techniques to determine whether, how and by whom WebSDR-related OSINT output is verified in ways that make it possible to democratise intelligence gathering and analysis without sacrificing quality. We examine a recent crisis where WebSDR activity and subsequent analysis was noticeably strong: Russia's 2022 full-scale invasion of Ukraine. We also outline the (potential) use of WebSDR-leveraged OSINT in genocide trials, using the manner of prosecution at the International Criminal Tribunal for the Former Yugoslavia as an example (ICTY 2017).

Open-source intelligence and ecosystem complexity

OSINT can be understood as a specific technique for gathering, processing and analysing publicly available data related to security and defence outside state intelligence agencies in news reports, official documents made public through freedom of information requests and commercially available data plus photos, videos, social media communications and the metadata attached to them. This information can be used to reveal and confirm events that have happened, timing and location and people involved, whether as direct participants (whether perpetrators or victims), accomplices or accessories. They can also be used in real time to engage in warning intelligence and during conflict. They may be a useful complement to IC institutions that discount information as many European institutions did in the 2022 Russian invasion of Ukraine (Hulnick 2004, Gustafson 2024, Jonsson 2024, Michaels 2024).

Hatfield (2024) and Miller (2018) advocate merging the OSINT concept with traditional intelligence as the IC is using the same methods, but with better resources. However, other authors see potential added value to private sector OSINT as a means of gathering and analysing information, provided quality control is equal to that of intelligence agencies and privacy concerns are respected. Gustafson *et al.* (2024) demonstrate that unsecured radio transmissions and mobile phone communications by Russian soldiers during their invasion of Ukraine served as raw material for useful OSINT analysis.

Further concerns about OSINT's net utility focus on the quality of methods and standards of disclosure. Oerlemans and Langenhuijzen (2024) argue that OSINT can protect or undermine national security, based on who has access to results, making privacy both a national security concern (Sherman 2022) and an enforceable right in the EU through the European Convention on Human Rights, Article 8. To avoid oversharing and disseminating harmful analysis, they suggest OSINT practitioners clearly articulate the goals and parameters of their research and define inappropriate behaviour to establish a perimeter and establish oversight to ensure respect for privacy concerns in both the US and Europe. These calls echo calls to standardise principles, rules and guidelines both across national jurisdictions and between the IC and private OSINT practitioners.

Such concern for quality assurance methods has prompted Robson Morrow's (2022) advocacy of private sector intelligence acquiring a shared identity, training and education, method of knowledge advancement, code of ethics and certification to be contributors to the field. Gioe *et al.* (2024) are even more specific in using the US Intelligence Community Directive (ICD) 203, issued in 2007 by the Director of National Intelligence as a model for private actors. ICD 203 requires analysis to be objective, apolitical, timely and comprehensive in sourcing information, clearly identifying uncertainties, inconsistencies, data quality and credibility issues and considering alternative interpretations. Gioe *et al.* (2024) argue that this critical part of analysis rarely happens in intelligence activity carried out by private enterprises.

In addition to defining what radio- and more particularly WebSDR-leveraged OSINT does and how practitioners do it, this paper can ask to what extent they attempt to act in ways that promote expectations of quality and objectivity. A key difference between this literature and our analysis below is that the literature, to date, focuses on private companies that operate as units, while we investigate independent actors and their interactions, which attempt to reach verifiable results in the process. To set a benchmark for what actors attempt to do, we not only look at interactions but also how they measure broadly in terms of ICD203 expectations. Strong reflection of those standards should be seen in attempts to solicit expertise to interpret and analyse data as they are processed. We hypothesise that online discussion across specialist groups in using WebSDR has a strong commitment to seeking objective flagging of geopolitical events, plus collection and analysis of data surrounding them.

This leaves the question of whether they should. Some will remain concerned that OSINT provides both home and adversarial teams insight into the home team's thinking. While true, OSINT's added value is in the sharing of information, analysis and discussion that might be lost in the soup of available information and filtered through the standard operating procedures and biases of traditional IC agencies. In other words, it can aid in fact-checking groupthink, selection bias and overload, in addition to furthering the work of human rights agencies and NGOs devoted to uncovering and prosecuting abuses using information that IC agencies keep to themselves.

In this article, we analyse OSINT activity surrounding radio transmissions, how that activity has changed with computer technology and how OSINT analysis has changed by the development of networks of organisations and individuals that perform complementary tasks. Radio-based OSINT activity parallels that of state-centric intelligence agencies, but without the illegal breaching of communication infrastructure and databases and without the secrecy regarding the results and methods used to obtain them. Despite the overlaps that these communities have in the material, we have only rudimentary knowledge of whether and how they connect and what role if any OSINT plays in those connections. This paper examines the actors and connections using a novel dataset combined with network analysis of the actors involved and their interactions.

Even OSINT activity can increase the supply of intelligence and combat blind spots, siloed information, information overload and selection bias typical of large state organisations. It also has disadvantages and hurdles, including the confrontation with unstructured information, misinformation and weak reliability of results without close attention to the quality of sources and the analysts who work on them (Cogan 2000, Kelty *et al.* 2013, Pastor-Galindo *et al.* 2020, Rubin 2023). However, a key feature of OSINT's approach to information gathering and processing is that it is conducted by decentralised actors who nevertheless need to share their insights to gain a full understanding of what they are looking at and what it means. Some can be described as OSINT specialists who collect, vet, process and disseminate information. Discussion between OSINT participants can help generate greater insight through information analysis and confidence in the accuracy of the information used. It can, therefore, be used for military intelligence but also increasingly for human rights violations detection, confirmation and intervention (Walker 2018, Dubberley *et al.* 2020).

Radio-based OSINT has historical precedents. The UK used private radio listeners during World War II to listen to and report on radio communications of the adversary. In contrast, modern OSINT radio surveillance involves private individuals outside the perimeter of the state intelligence apparatus. WebSDR users often transcribe and reference transmissions of interest on internet platforms and social media, which makes them searchable and available to actors outside traditional intelligence agencies after the fact. The process is, therefore, potentially democratised in that a wider range of actors is involved. However, there remain serious questions about the quality and usefulness of the output, and how actors with different skillsets can be brought together to do so.

The radio transmissions of most relevance in security-related OSINT are those on shortwave. Shortwave radio, i.e. frequencies between 3 and 30 MHz, can transmit information over thousands of kilometres. Specific parts of the radio frequency spectrum are reserved for and used by military units and facilities as agreed by the International Telecommunication Union at the World Radio Communication Conference, besides a wide range of other uses, from broadcasting and radar to amateur radio and civil maritime and aeronautical communication.

Software-Defined Radio (SDR) is a technique for implementing radio equipment that relies on digitally processing analogue radio signals in software. WebSDR adds a web-based, server-supported platform to allow multiple users to tune in to multiple frequencies simultaneously and is used worldwide with 162 public servers active as of writing. It also hosts a public logbook in which users can enter their findings, as well as a chatroom to discuss findings. This allows anyone to listen to signals and discuss the importance,

meaning and veracity of the information at hand (de Boer 2008). WebSDR, therefore, expands the supply of raw data, users, analysts and networks involved in OSINT, making crowdsourced-enhanced, searchable and verifiable signals intelligence available to a wider audience than traditional state intelligence agencies and private owners of suitable radio equipment, with the potential to substantively increase the volume of actionable intelligence analysis in conflict zones.

Crowdsourced-enhanced WebSDR has not only strengths in the availability of massive quantities of data from a wide variety of sources but also the potential to overcome analytical blind spots and selection bias typical of siloed information in bureaucratic structures that can otherwise hamper insights. Its open nature, the legal methods used and the drive to openness of information not only increase the supply of information and analysis generally but to two other groups interested in the information they provide with their own agendas: journalists and human rights agencies devoted to the documentation and prosecution of war crimes, such as Human Rights Watch, Amnesty International and United Nations International Criminal Tribunals. A contemporary example of use in the Russian attack on Ukraine has been documented by Janovsky *et al.* (2022). Amnesty International also places value on documenting human rights violations with these methods (Koenig *et al.* 2021, MacLean 2023).

Identifying OSINT skill groups and their connections: a network approach

Making sense of radio intercepts is a challenge that requires bundling and networking expertise possessed by distinct groups engaged in intelligence gathering, processing and use outside the perimeter of state intelligence agencies, in the absence of state-led coordination. *OSINT specialists* are a distinct category of users with a specific focus on the methodology that sets them apart from others regarding confidence in the accuracy of the information generated (Glassman and Kang 2012). Other OSINT participant groups identified and discussed in this paper are *veterans* operating in the public realm (ex-military and intelligence officers) with specific expertise in the interpretation and context of verified information, *human rights activists* focused on documenting and prosecuting human rights violations, war crimes and genocide in international criminal tribunals, such as those held for Yugoslavia and Rwanda (O'Brien 1993, Schabas 2006), *law and order specialists* (police and justice institutions) (Sikkink and Kim 2013) and *journalists* (encompassing both investigative journalists that generate intelligence and other reporters who promote awareness, discussion and public interest as part of the daily news cycle).

Do these actors interact on WebSDR radio intercepts, how and can results be treated as reliable and accurate? We argue that WebSDR, as a source and platform, adds to the palette of sources and means of cooperation between different OSINT groups determining what information exists, what it means and whether it can be trusted. Online connections between different practitioners not only generate the potential to share expertise while interpreting data but also subject the findings to review by more than one actor, consistent with quality expectations in ICD203, while allowing it to take place in the open. This potential contribution to OSINT techniques and process is both relevant but underexplored in the extant literature (Marzell 2007, Steele 2007, Schaurer and Störger 2013, Akhgar *et al.* 2017), primarily examined six years ago by Eldridge *et al.* (2018). We want to focus on the nature of online networks to analyse whether and how radio-using

OSINT groups form connections to each other and then to other sub-groups, what kind of output their collaboration generates and with what degree of confidence. This complements studies of how the introduction of artificial intelligence technology can improve the analysis of open-source intelligence (Evangelista *et al.* 2021).

Collaborative OSINT: preconditions and potential

The rise of OSINT activity and its apparent fragmentation raises the question of whether, how and under what conditions they cooperate, and how their output becomes connected to what state intelligence agencies and human rights advocates do. Williams and Blum (2018) argue that while intelligence agencies (IAs) increasingly use OSINT output, communication between the two sides is not visible. This resembles a one-way mirror: with IAs scraping all the publicly available data they can find, including OSINT analysis for their own use, without providing feedback. The necessity of secrecy limits not only direct evidence of OSINT impact on state behaviour; it also makes OSINT participants rely on their own resources to determine how reliable their findings are. We, therefore, focus on how the OSINT community combines specific skills to do this.

Hribar *et al.* (2014)'s discussion about the OSINT community, its methods and output, argues that a key challenge to crossovers between kinds of intelligence communities and actors, including acceptance and interaction between OSINT operatives and IAs, is determining *trust* and demonstrating the *quality of analysis*. OSINT actors face the challenges of sharing specific expertise and establishing *bona fides*, even under anonymity. However, little is known precisely about the degree of connection and cooperation that has the potential to enhance the supply and trustworthiness of crowdsourced information.

We posit that online communication is one factor making it possible for specific actors within the OSINT community to bundle complementary skills and knowledge in ways that make increased production of intelligence analysis possible and effective (Murphy and Salomone 2013). Each group performs a specific task. Listeners and journalists crowdsource raw information, OSINT specialists filter, source and verify information and veterans help them interpret it. Doing this successfully requires cooperation to enhance trust between intelligence actors and confidence in their collective output. Tuinier *et al.* (2023) underline the importance of trust, built on recognised professional standards and shared traits that “socially bind” intelligence professionals into a “community of practice” that shares information and analysis. We posit that the specific combination of crowdsourcing, methodology and interpretive skills is necessary and sufficient for generating an increased supply of trustable, actionable results, provided all three elements are combined. WebSDR receivers support this endeavour by providing the empirical data these experts use and permitting collaborative analysis, while the groups depend on one another before results can be achieved. Once organised, algorithmic solutions can help standardise the process (Yeung *et al.* 2023).

Connecting OSINT groups: OSINT hubs and regime complexity

However, social media and the internet are not sufficient on their own to promote coordination and cooperation. Below, our research uses empirical analysis to define discrete OSINT groups, conducts network analysis to outline the connections between the

actors and looks for patterns of collective action. Referring to coordination mechanisms from international regime theory, we argue that OSINT specialists act as high-profile, community-vetted OSINT hubs (in the case of groups) or linking pins (for individuals), connecting other individuals and organisations with specific skill and knowledge sets. As hubs, they connect the entire OSINT intelligence chain of collecting, deciphering, interpreting and analysing publicly available information and creating a useful, reliable product of interest to defence agencies and human rights organisations.

We take an inductive and data-driven approach to network analysis, examining individuals, government and corporate representatives interacting with one another on a regular basis on the same topic, often in the absence of hard, formal institutional arrangements, but in ways that define, empower and shape the behaviour of the participants (Hafner-Burton *et al.* 2009). We add regime theory's insights into how actors develop trust, cohesion and cooperation across actors working on the same issue, but with diversity in specific policy focus, types of expertise present, types of institution or professional members and epistemic viewpoints on the perimeters of the policy.

A thread of regime theory focused on regime complexity deals with situations where formal institutions are absent and actors organise in networks instead. This suits the situation of OSINT participant groups, who cooperate with others while retaining independence and differing normative visions and goals (Pernice 2018, Anagnostakis 2021) but also between those who are comfortable working with state institutions and others who are not. Within regime complexity, various professions can retain their own practices and values while taking part in a larger ecosystem that is more than the sum of its parts. Quaglia (2020, 2022), Alter and Meunier (2009) and Alter and Raustiala (2018) see regime complexity develop because of specialisation, with different professions taking on distinct roles within a larger policy puzzle in a way that potentially maximises the combination of expertise and differentiation, creating a regime complex of interacting communities and organisations. The key to coordination lies in mutual respect among the various communities regarding their output. This, in turn, requires an agreement on the basic facts of the situation they face, the objectives they have and the principles on which their responses are based. If this mutual respect can be established, then OSINT as a collection of actors specialised in different functions can constitute a supplement to state-centric intelligence agency activity.

Beyond trust, coordination is also essential. A mechanism that coordinates fragmented expertise and enhances trust and confidence in the information provided, is the hub (Quaglia and Spendzharova 2022, 2023) or the linking pin (Organ 1971). Hubs are where independent members of a policy community share their information and expertise, allowing for the discussion of basic concepts, design of possible responses and coordination of different components of a larger whole. They allow participants to engage in policy learning, deal with temporary uncertainty, shape narratives about problems and responses and coordinates. Repeated interaction and sharing allow them to build trust between participants despite different viewpoints. The confidence and trust generated lies in the methodologies used, the thoroughness of the analysis and the sense of integrity with which it is done. Linking pins provide more indirect connections, with the other members interacting through the individual. Organisational hubs can, therefore, foster communication and coordination between OSINT participants.

The new technology of WebSDR potentially democratises access to certain kinds of intelligence information and makes it possible to construct networks that analyse it

and to change how intelligence is derived and used. Hubs connect actors that need each other to find and process WebSDR-accessible data. The empirical study below uses activity and interaction across several sub-groups of the OSINT participant community regarding information derived from WebSDR-enabled radio listening between the 2014 Russian invasion of Ukraine and the present, which includes the 2022 Russian invasion of Ukraine to analyse interaction between actors, to identify key players that both produce widely-used output and vet it from elsewhere by triangulation and to demonstrate the direction in which information flows.

The next section presents the methodology by which we collect, sort and process information from WebSDR server logs and Twitter data about (1) OSINT participants with distinct profiles active on the Twitter/X platform, as well as their links to outside organisations that confirm or strengthen their affiliation with that group; (2) their use and analysis of WebSDR-sourced information (verifying intensity of use, topical focus of use, the level of attention paid to verifying methodologies versus dissemination and discussion) and (3) the patterns of interaction between them (how information is shared between different OSINT participant communities, with what degree of intensity and the presence of actors functioning as information hubs for other users). We look for evidence of cross-checking, vetting, collecting and interpreting radio intercepts. We also look for evidence that coordination occurs due to the affiliation of key actors and hubs that are connected to a single country (the power hypothesis: Drezner 2009). Our starting assumptions, however, are modest and focus on an empirical overview before assessing congruence with one outcome and explanation over another.

Research design, operationalisation and methods in analysing WebSDR use

To get more insight into the WebSDR ecosystem and its relation to OSINT, we conduct two different analyses and combine them into a case study on the Russia's war on Ukraine. The first analysis uses usage data of one highly popular WebSDR server to focus on which actors are present, how they interact with others on the platform and whether they demonstrate sufficient connections to one another to constitute one or more ecosystems. By ecosystem, we mean a cluster of actors interacting collectively to generate a common output, often involving interdependence, specialisation and cooperation across diverse participants (Korhonen 2001).

The second analysis uses Twitter data to determine the credibility of actors. We do this primarily by analysing how information flows between them, with a particular interest in whether certain actors play central roles in collecting, vetting, processing and disseminating information and analysis. We define credibility as trust that other actors have in the accuracy, validity and quality assurance of the information that the actor provides to other members of the information ecosystem. While never perfect, we can speak of higher or lower degrees of confidence and trust in the outcome.

The WebSDR platform has been collecting usage data since 2013 for improving, maintaining, monitoring and troubleshooting the platform's use. As the data were not collected with explicit consent from users to perform this research, we took all possible steps to anonymise data. This includes the anonymisation of IP addresses and usernames in the chatroom and only aggregated results will be discussed. We have purposely

refrained from singling out individual users. This approach has also been discussed with and approved by the ethics committee of the University of Twente.

In addition to the quantitative and network analysis below, we additionally undertook qualitative interviews to collect information from highly credible sources to corroborate the findings. The individuals interviewed provided bona fides through institutional linkages (workplaces with reputations for attention to professional standards of information collection, filtering and analysis), either present or past. The anonymity of the people interviewed, their institutional affiliations and their specific relation to the broader OSINT community in some cases was considered essential, given the nature of the work that they perform.

Identifying actors within the WebSDR ecosystem

To analyse the ecosystem surrounding the WebSDR platform, we constructed a dataset of the actors that use the platform, including details on the interactions they perform with the platform. This involves identifying unique users and sessions from HTTP request data (logged information about the Web connection a user's browser makes to the server) and exact radio frequencies users listened to within their sessions. With this data, we can find networks of frequencies that are listened to in the same session, identify interest in frequencies that users or groups of users have in common, identify cluster(s) of frequencies popular for information gathering during geopolitical events and identify and categorise users searching for information regarding geopolitical events.

Dataset

Our dataset was collected on the WebSDR server of the University of Twente, consisting of (anonymised) HTTP requests made to the platform collected from the web server logs between 2013 and 2024. For every HTTP request, information was available on the user (anonymised IP address), files requested and accessed, browser, website source and cookies set by the WebSDR. Resource requests form the bulk of data analysed. Every time a user adjusts the frequency they listen to in the audio stream, a new request is made, thus making it possible to trace what users tuned in to. Timestamps also make it possible to infer how long they listen or switch to another frequency.

Identifying users and sessions

Log data about HTTP requests on the WebSDR platform were first pre-processed to remove spurious or malformed information, due to server problems, users attempting to inject malicious code or other random activity. We then bundled all actions by session: defined as the start and end of an HTTP connection. Many of these sessions are short-lived and only contain a single request to get an image or other resource from the server. However, the ones we are interested in are sessions that make a resource request to access the underlying audio stream.

With these sessions grouped, it is possible to find unique users across the different sessions that share the same cookie, share the same IP address and user-agent and were made within at most one week of each other. We placed extra restrictions on matching

by an IP address since IP addresses are likely to be rotated to different users after a certain period (Xie *et al.* 2007) and changed through short-lived connections such as WiFi hot spots when a cookie is not present (Mishra *et al.* 2020). Although the same IP address can be used by multiple users in a short time under these conditions, chances are small that this occurs within a period of one week and it has a negligible impact on the resulting users. Using this filter, we could isolate 41.8 million sessions and 13.6 million unique users out of 54 billion original dataset rows.

Extracting radio frequencies and sessions of interest

To further refine these sessions, we extracted which frequencies users listened to and for what duration of time, rounded to the nearest kilohertz (kHz) and duration to the nearest second. To identify sessions that are likely to be from users intending to gather information regarding geopolitical events, we first match each frequency in a session to its corresponding category in frequency purpose categories set by the International Telecommunications Union (ITU). We then identify a category “Conflict” from a list of 229 frequencies crowd-sourced from WebSDR operators, knowledgeable individual users and the WebSDR platform chat that were popular regarding the war in Ukraine.

Profiling users, networks and nodes

WebSDR data show a distinct cluster of users focused on conflict (less than 10% of users, compared to distinct groups for maritime, aviation, broadcasting, amateur radio and “other”), who spend most of their time (92%) listening to conflict-related material. Users in other categories do the same, staying within their areas of interest. Within this category, we filter out short connections caused by users scrolling through frequencies and apply the Pareto principle to use 80% of the data. We filter the remainder to construct the network of interconnected frequencies by selecting

- Node weight: Number of sessions in which a user listens to the frequency for at least 8 s.
- Edge weight: Number of sessions in which a user listens to both frequencies for at least 8 s.
- Edges: Minimum edge weight of 11.

Cluster detection

To isolate which (cluster of) users are listening primarily to frequencies falling within the conflict category, a clustering algorithm is used. The Leiden algorithm by Traag *et al.* (2019) can detect clusters of nodes that are densely connected within the network we previously constructed. As we are interested in frequencies related to the list of conflict frequencies, this algorithm can identify those by looking at which cluster they are a part of. With these clusters it is possible to show which frequencies users are likely to have also listened to in case they listened to a specific frequency, and thus conclude which users have the same listening pattern. The nodes are initially partitioned by the ITU frequency

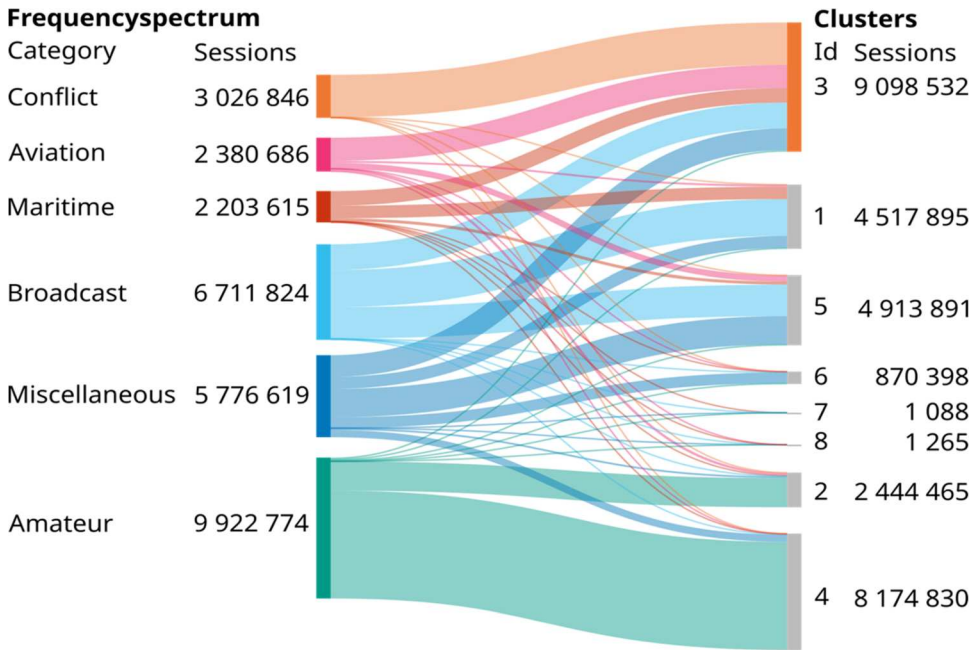


Figure 1. Distribution of the number of sessions categorised by the Dutch frequency spectrum to newly created clusters.

spectrum. The algorithm is then run iteratively until the modularity coefficient, a metric to measure the strength of the newly found clusters, no longer increases. In total, the algorithm detects 8 clusters within our network and reaches a modularity coefficient of $Q = 0.28$. The score, which can range between -1 and 1 , falls just below the range for a typical network with a strong community structure (0.3 – 0.7) by Newman and Girvan (2004). Although our network sits at the lower bound, it is still well above a random network which would have $Q = 0$.

Figure 1, which shows how sessions are distributed across different clusters, demonstrates that the newly constructed conflict cluster consists of sessions from military, aviation and maritime frequencies combined rather than just military-specific communications. The cluster additionally does not overlap much with amateur or broadcast frequencies or users.

Relating WebSDR usage patterns to geopolitical events

To analyse how WebSDR usage has varied over time, in particular, the days on which the number of users displayed a pronounced peak, we look both at the total number of users that listen mostly to the frequencies that are in the newly identified conflict cluster. When the number of those users listening to the conflict cluster peaks, that is a strong indication that the peak is related to a geopolitical event (as opposed to other categories). The data also track how people came to the platform – from the HTTP referrer – and what users discuss in the chat, making it possible to explain what causes these peaks.

Multiple peaks can be observed, as shown in Figure 2. One such case is a peak on November 20th, 2016, when an increase in users was seen on the platform. When

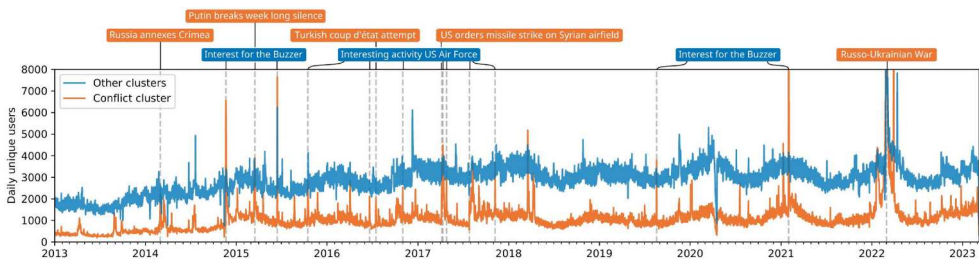


Figure 2. Number of active users per day by cluster.

looking at the top referrers, two forums are found that discuss a tweet. Users then link to the WebSDR platform, causing a spike in users trying to get more information by tuning to frequencies of (in this case) the US Air Force. Another example of a high influx of users was on April 13th, 2022, when a popular Twitter user linked to the WebSDR. As can be deduced from their previous tweets, it was made in relation to the Russian ship Moskva sinking (Madhani *et al.* 2022) and an (unverified) claim was made that it was transmitting emergency Morse code on a frequency that can be received on the WebSDR.

A subset of peaks is labelled similarly, by manually checking the referrer and chatroom data to infer the peak's cause. In cases where no direct cause is found, the peaks are left unlabelled, and thus the final figure likely depicts only a subset of all reasons. Figure 2 shows the difference in peak usage between users in the conflict cluster and other clusters with the inferred events labelled.

Three peaks are cut off at 8,000 users to improve visibility, but in reality, they extend well beyond that point (10,133 on January 31st 2021, 46,980 on February 28th 2022 and 17,975 on March 30th 2022). The lag after the Russian invasion of Ukraine on February 24th is due to the WebSDR server being severely overloaded, serving only a subset of (potential) users until it was upgraded on February 27th.

Analysing information flow between actors on Twitter/X

To determine the credibility of the actors, as well as how the actors potentially share information gathered using the WebSDR receiver, discourse on Twitter is analysed. One method to investigate the affiliations of actors is by analysing Twitter profiles (Pathak *et al.* 2021). From manual inspection, we also observe that users often mention their affiliations to journalistic or state organisations on their profile. Therefore, a systematic search on Twitter can reveal more details on the actors and ecosystem surrounding WebSDR.

Data collection

The dataset we retrieved consists of tweets containing the term “websdr” and related users between January 1st, 2022 and September 22nd 2023. It consists of 2 434 threads of messages, containing 2 689 tweets that use the term “websdr”, as well as 4 243 responses.

To extract users matching the profiles we are interested in, we used a keyword-based approach. These keywords could be matched to either the user's name, handle, affiliation

Table 1. Keywords used to assign a category to a Twitter/X user.

Category	Keywords
Veterans	veteran, NSA, RAF, USAF, USCG, USMC, AIVD, MIVD, NCTV, 16AA, 3PARA
OSINT Specialist	OSINT, open-source intelligence
Journalists	journalist, reporter, foreign editor
Human rights	HRF, FIDH, UNHCR, amnesty, civil rights defenders, human rights watch, human rights foundation, federation for human rights, Freedom House, international humanitarian law

or bio. Where the match was broad and potentially fit different categories, a manual inspection was performed to confirm or deny the fit. The keywords “veteran”, “OSINT” and “journalist” were used for the first three categories, respectively. By manual analysis of the matches and other keywords mentioned in the bio of the matched users, extra keywords were added to match a broader set of users. Furthermore, for the Human rights category keywords were included with relevant organisations from a list by Human Rights Careers (n.d.). Table 1 lists the keywords used.

Of all users who posted tweets relating to WebSDR, only 67 users match any of the profiles in the table above and constitute primary sources of information: 18 veterans, 35 OSINT specialists, 14 journalists and 0 human rights advocates. As we are also interested in the larger ecosystem surrounding these users, they serve as the starting point for further analyses using a snowballing method. We added both their followers and who they are following, placing them in the same categories as secondary sources: 5815 veterans, 3335 OSINT specialists, 17016 journalists and 208 human rights advocates. The entire number of “other” users was more than 1.1 million. Although this means the resulting set of users is likely far from complete, it also means that the keywords used are not too broad.

The network of actors

From Twitter users’ data, we can visualise how information flows between the various categories. To do this, we condense all users in a category to a single node in a graph. For each category, we let the incoming edges represent where they get their information from and what percentage of a user’s feed on Twitter is part of these categories (so the incoming arrows add up to 100%).

Figure 3 visualises the flow of information between categories of users on Twitter. Incoming arrows add up to 100% and represent the source of the information that users in this category receive. It shows that journalists see more than four times more tweets from OSINT users as opposed to veteran users (34.53% as opposed to 8.45%) on average. OSINT specialists are, in turn, double as likely to see content from veteran users compared to journalists (16.99% as opposed to 8.45%). Another noteworthy observation is that the human rights category contributes little to the other categories and follows mostly journalists and OSINT specialists. This is also expected due to the small number of users.

To further tease out relations between different actors on Twitter, and which types of actors they are connected to, the whole network of users in the Twitter dataset was placed using the force-directed placement algorithm ForceAtlas2 (Jacomy *et al.* 2014). The primary sources are more prominent players than the secondary users, with strong connections between them and many followers in common. This suggests that there is a

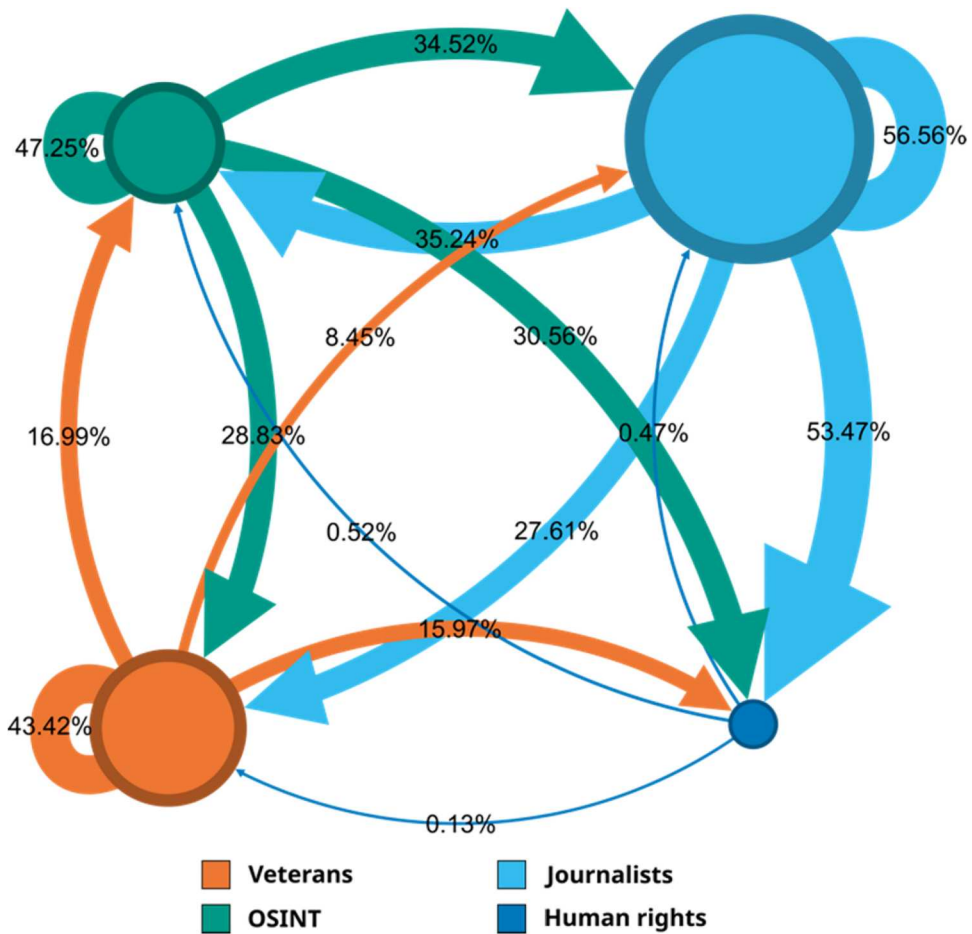


Figure 3. The flow of information on Twitter between OSINT participants.

close-knit community of actors that share information with each other within the WebSDR ecosystem on Twitter.

To find which actors are the most influential within this network, we analysed for each category of primary sources the average number of followers and eigenvector centrality. The latter is a network measure, ranging between 0 and 1, to determine a node’s (user’s) influence based on the reach of the nodes it connects to, and where connections to influential nodes increase one’s own influence. Although this measure does not encompass all aspects to determine a node’s influence, a larger value indicates that it is connected to other more influential nodes.

Table 2 shows that OSINT specialists stand out as the most influential actors in the ecosystem, followed by journalists and then veterans. As can be seen, on average, the influence of veterans scores lowest on both measures. For OSINT and journalists, however, the two differ. Whereas journalists have more than twice as many followers on average, they have less influential actors in their network than OSINT actors. This means that although journalists reach more individuals, OSINT specialists have even more influence in the network surrounding WebSDR on Twitter than the numbers indicate at first glance.

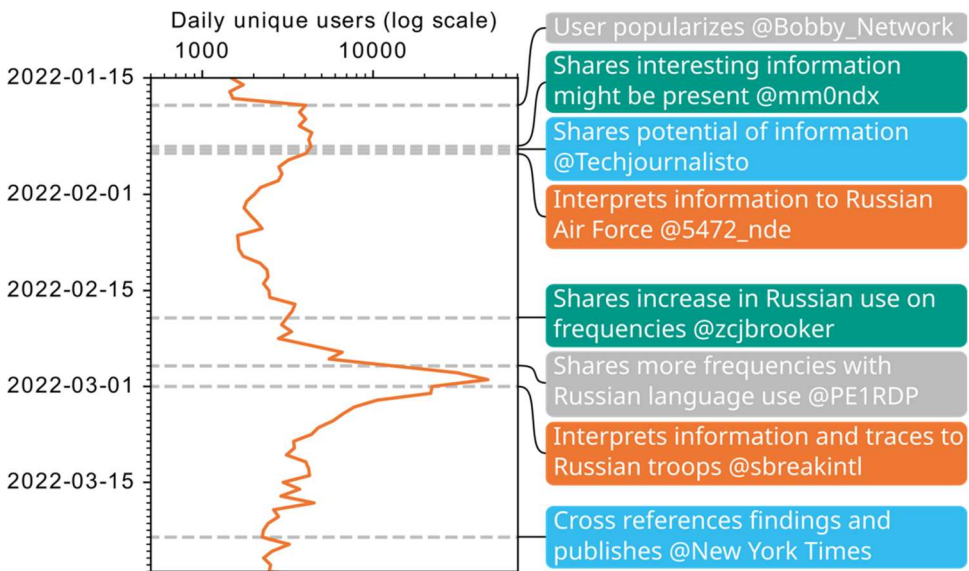
Table 2. Average number of followers and eigenvector centrality per primary source.

Category	Followers	Eigenvector centrality
Veterans	11 541	0.0204
OSINT	15 746	0.0749
Journalists	32 110	0.0457

Case study: the war in Ukraine in 2022

Information gathered on WebSDR and shared on platforms such as Twitter referencing the war in Ukraine in 2022 from 15 January until the end of March 2022 demonstrates information sharing across different actor categories. WebSDR usage is first filtered by sessions taking place during the conflict period. Tweets from the dataset are then manually analysed to determine who shares which information first. Figure 4 presents the resulting overview. It shows WebSDR usage on the left and summaries of tweets related to WebSDR and the war in Ukraine on the right.

In January, rumours emerged that there were interesting radio transmissions being made relating to the war in Ukraine. The first peak of WebSDR usage coincides with a user sharing frequencies related to the US Air Force on January 19th. No new insights are shared in the tweet however from @Bobby_Network (2022). On January 25th, interest on the platform increases in response to new information. A user, who identifies as being involved in OSINT and an amateur radio user (@mm0ndx 2022), shares potentially interesting information related to a Russian transmission on a certain frequency (@mm0ndx 2022). In response, a German journalist specialised in open-source investigations (@Techjournalisto 2022) shared this information with his network (@Techjournalisto 2022). Within a day a British Royal Air Force veteran, who claims to be specialised in Cold War intelligence

**Figure 4.** Information shared on twitter: frequency and key users.

and radio communications (@5472_nde 2022), interpreted the broadcasts to be from a Russian strategic bomber also known as “Bear” (@5472_nde 2022).

Almost a month later on February 19th, close to the full-scale invasion of Ukraine, a user, who mentions they focus on open-source intelligence related to Ukraine and are cited by multiple news organisations (@zsjbrooker 2022), shares they hear interesting Russian language usage on specific frequencies (@zsjbrooker 2022). A week later on February 26th, an amateur radio user (@PE1RDP 2022) shared multiple different frequencies on which they heard Russian voices but offered no information or translations about the broadcasts (@PE1RDP 2022). Then on March 1st, Shadowbreak, an organisation of professionals that specialise in GEOINT and OSINT, shared that it was actually Russian military units who broadcasted on the previously mentioned frequencies (Shadowbreak 2022). This information was later cited and confirmed by the New York Times, which published an article on March 23rd in which they linked the transmissions picked up via WebSDRs to footage made on the battlefield in Ukraine (Stein *et al.* 2022).

In this time period, we observed three types of information that were shared surrounding WebSDR. The first type is mainly sensationalistic, where an actor links the presence of communication over frequencies of the US Air Force to conflicts in the world without further analysis or insight. Apart from bringing a significant number of users to the platform, it does not contain any proven insights. Secondly, we observe two cases where an actor engaged in OSINT information gathering shared the fact that something interesting was being communicated but did not have the expertise to turn this into knowledgeable intelligence. In both cases a (group of) veterans were able to interpret the information and connect it to other knowledge about the conflict in Ukraine. Here we observe the strength of the community on Twitter surrounding WebSDR and other radio receivers.

Although initially, most users that come to the platform are presumably sensationalists who come and go, we observe a large group of actors continuing to interact that are specifically interested in gathering intelligence on geopolitical events. Some of these actors we also observe in the Twitter ecosystem, from which we can confirm that both OSINT and veteran actors are actively using WebSDR for intelligence purposes. Furthermore, the information flow on Twitter suggests that although OSINT actors can pick up interesting information from a WebSDR, often veteran knowledge is needed to interpret those findings before it becomes a claimed finding that would meet the criteria of (attempted) objectivity and pass the challenge of critical analysis. The fact that this appears to happen regarding WebSDR-leveraged information suggests that the network makes a meaningful effort to meet quality expectations surrounding OSINT and IC agencies alike, as well as human rights advocates that depend on reliable information to prosecute abuses. To further assess the patterns unearthed in this study, we spoke to people who were identifiable as veterans and OSINT specialists. They confirmed these findings as accurate, which increase our confidence in them. A final observation about the activity of OSINT participants is that there is no clear link to any particular country, suggesting that the coordination observed is not taking place in the shadow of a particular state’s hierarchy. Nor is there any evidence of direction from a state-led body that ensures they work together. The power hypothesis of coordination is, therefore, not supported.

Discussion and conclusions

We started out asking whether and how information is collected using WebSDR radio receivers and processed across Twitter/X by the broader OSINT community. We envisaged that if such collaboration were possible, it would enhance the quality and quantity of OSINT analysis by bringing complementary knowledge and skill sets together, required to crowdsource and process information outside of established state intelligence agencies. This would mean incorporating OSINT specialists, veterans of military and intelligence agencies, journalists and human security advocates to cover the range of purposes for which this information is valued. We asked this with specific attention to information gathered from radio intercepts and their analysis from WebSDR systems. In the context of military conflicts like Russia's war on Ukraine, the identification, verification and processing of information can be valuable to several interested parties, both during the conduct of a war and afterwards, in the realm of prosecuting war crimes in international tribunals.

We first showed that there is a clearly identifiable OSINT community operating online, with clusters of actors that are involved in searching, vetting and analysing information. They depend on each other, creating a system of checks and quality control in the process of flagging, interpreting and analysing data. We have also shown the links between those clusters and what each cluster does in sharing and analysing information that helps the ecosystem meet basic expectations of objectivity and professionalism. OSINT activity involves a great deal of crowdsourcing information by specialists and non-specialists alike before clusters of actors break that information down and process it. Many *journalists* fall into the category of disseminating information rather than generating it, but investigative journalists contribute information that other clusters use. *OSINT specialists* focus on verification and sourcing specialised information and are highly active in the collection, verification and triangulation of evidence. *Veterans* focus on interpretation of data and are central to providing the broader meaning that OSINT specialists are looking at but cannot always interpret fully without their input. By communicating with each other and sharing expertise, they were able to generate vetted information and analysis outside the halls of state agencies that none of them would have been able to produce alone. While verification through OSINT specialists was confirmed to be a common feature that turned them into coordinating hubs for the broader community, we also showed a surprising result that veterans formed a crucial part of what OSINT specialists are able to do, by interpreting information, allowing specialists to sift through information and separate the most important information from the trivial and to get the big picture over the real meaning behind the data. Despite distinct group identities, coordination emerged with OSINT specialists working as hubs and linking pins. To gain further insight into our findings, two independent journalist teams we spoke with confirmed that there is still future work to do on the methodologies and practices by which information is collected and processed, but that the first steps have already been taken, as outlined in this paper.

The connections formed through OSINT hubs and individuals acting as linking pins are best interpreted as coalitions of convenience between different clusters or groups within the larger OSINT community that have come closer together without forming a collective organisation. These coalitions are supported not only by online communication

but more specifically by the connecting functions that hubs and linking pins fulfil. Hubs allow each of the groups to collaborate on sourcing, sifting, verifying and interpreting information in ways that none of them could do individually while retaining their independence. In addition to other sources of open-source intelligence shared online, radio intercepts from WebSDRs (and other radios) provides a gold mine of searchable, analysable data that OSINT participants are now starting to use and can exploit further in the future.

We also tested for the existence and activity of a *human security* cluster that might be interested in using OSINT. While they exist, we do not yet observe them interacting significantly with the others, despite overlapping interests. This is a topic for future research as they may use the information without being visible. However, if there is a disconnect between human security advocates and other OSINT groups, a better connection could improve the use of OSINT research in prosecution of war crimes, particularly United National International Criminal Tribunals.

The crowdsourcing of signals intelligence is not entirely new, but the democratisation of open-source capacity to filter and analyse information is. We expect these expert ecosystems to persist and even grow in importance over time. As this happens, the quantity of trustable, actionable intelligence information crowdsourced through the OSINT ecosystem will increase as a resource for traditional security establishment actors but also for human security specialists focused on proving and prosecuting war crimes. Not only do we contribute to our understanding of how OSINT works with WebSDR resources, we also have a stronger understanding of how quality control is exercised and confidence is generated in the output produced and how new sources of information can be added to the information and analysis chain. This is something for traditional intelligence agencies and human security advocates as well to take note of, even if they cannot openly acknowledge their use of OSINT material.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Anne van Harten  <http://orcid.org/0009-0005-0406-6394>

Shawn Donnelly  <http://orcid.org/0000-0003-2791-6505>

Pieter-Tjerk de Boer  <http://orcid.org/0000-0002-0818-5295>

Roland van Rijswijk-Deij  <http://orcid.org/0000-0002-0249-8776>

References

- Anagnostakis, D., 2021. The European Union-United States cybersecurity relationship: a transatlantic functional cooperation. *Journal of cyber policy*, 6 (2), 243–261. <https://doi.org/10.1080/23738871.2021.1916975>.
- Akhgar, B., Bayerl, P.S., and Sampson, F. eds. 2017. *Open source intelligence investigation: from strategy to implementation*. Cham, Switzerland: Springer.
- Alter, K.J. and Meunier, S., 2009. The politics of international regime complexity. *Perspectives on politics*, 7 (1), 13–24.

- Alter, K.J. and Raustiala, K., 2018. The rise of international regime complexity. *Annual review of law and social science*, 14, 329–349.
- @Bobby_Network [Malhotra, B.R.], 2022. Imminent risk of war between @NATO/@Ukraine & @Russia could become a sour reality, according to rumors. #SKYKING: [Tweet]. Twitter. 19 January. Available from: https://twitter.com/Bobby_Network/status/1483629968672407553.
- Cogan, J.K., 2000. The problem of obtaining evidence for international criminal courts. *Human rights quarterly*, 22, 404–427.
- de Boer, P.T., 2008. Het WebSDR-experiment. *Electron*, 63, 258–260.
- Drezner, D.W., 2009. The power and peril of international regime complexity. *Perspectives on politics*, 7 (1), 65–70.
- Dubberley, S., Koenig, A., and Murray, D., eds. 2020. *Digital witness: using open source information for human rights investigation, documentation, and accountability*. New York: Oxford University Press.
- Eldridge, C., Hobbs, C., and Moran, M., 2018. Fusing algorithms and analysts: open-source intelligence in the age of “big data”. *Intelligence and national security*, 33 (3), 391–406.
- Evangelista, J.R.G., et al., 2021. Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence. *Journal of applied security research*, 16 (3), 345–369.
- Gioe, D., Parkhurst, J., and Gioe, D.V., 2024. Can private sector intelligence benefit from U.S. intelligence community analytic standards? *International journal of intelligence and CounterIntelligence*, 37 (4), 1145–1163. <https://doi.org/10.1080/08850607.2023.2235078>.
- Glassman, M. and Kang, M.J., 2012. Intelligence in the internet age: the emergence and evolution of open source intelligence (OSINT). *Computers in human behavior*, 28 (2), 673–682.
- Gustafson, K., et al., 2024. Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022. *Intelligence and national security*, 39 (3), 400–419. <https://doi.org/10.1080/02684527.2024.2322214>.
- Hafner-Burton, E.M., Kahler, M., and Montgomery, A.H., 2009. Network analysis for international relations. *International organization*, 63 (3), 559–592.
- Hatfield, J.M., 2024. There Is No such thing as open source intelligence. *International journal of intelligence and CounterIntelligence*, 37 (2), 397–418. <https://doi.org/10.1080/08850607.2023.2172367>.
- Hribar, G., Podbregar, I., and Ivanuša, T., 2014. OSINT: a “grey zone”? *International journal of intelligence and CounterIntelligence*, 27 (3), 529–549.
- Hulnick, A.S., 2004. *Keeping us safe: secret intelligence and homeland security*. London, UK: Bloomsbury Publishing USA.
- Human Rights Careers, n.d. *25 international human rights organisations*. Available from: <https://www.humanrightscareers.com/magazine/international-human-rights-organisations/> (Accessed 20 Oct 2023).
- ICTY, 2017. *International criminal tribunal for the former Yugoslavia*. Available from: <https://www.icty.org/>.
- Jacomy, M., et al., 2014. Forceatlas2, a continuous graph layout algorithm for handy network visualisation designed for the gephi software. *PLoS ONE*, 9 (6), e98679.
- Janovsky, J., et al. 2022. Attack on Europe: documenting Russian equipment losses during the Russian invasion of Ukraine. *Oryx*. 24 February. Available from: <https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html>.
- Jonsson, M., 2024. Swedish intelligence, Russia and the war in Ukraine: anticipations, course, and future implications. *Intelligence and national security*, 39 (3), 443–457. <https://doi.org/10.1080/02684527.2024.2325248>.
- Kelty, S.F., Julian, R., and Ross, A., 2013. Dismantling the justice silos: avoiding the pitfalls and reaping the benefits of information-sharing between forensic science, medicine and law. *Forensic science international*, 230 (1–3), 8–15.
- Koenig, A., et al., 2021. New technologies and the investigation of international crimes: an introduction. *Journal of international criminal justice*, 19 (1), 1–7.
- Korhonen, J., 2001. Four ecosystem principles for an industrial ecosystem. *Journal of cleaner production*, 9 (3), 253–259.

- MacLean, K., 2023. Interactive digital platforms, human rights fact production, and the international criminal court. *Journal of human rights practice*, 15 (1), 84–99.
- Madhani, A., Fox, B., and Merchant, N., 2022. US seeks to downplay role in sinking of Russian warship. *Associated press*. 6 May. Available from: <https://apnews.com/article/russia-ukraine-europe-black-sea-f500930a03ccdfdd32c2ca82082582f0>.
- Marzell, L., 2007. OSINT as part of the strategic national security landscape. In: B. Akhgar, S. Bayerl, and F. Sampson, eds. *Open source intelligence investigation: from strategy to implementation*. Cham, Switzerland: Springer, 33–56.
- Michaels, E., 2024. Caught off guard? Evaluating how external experts in Germany warned about Russia's war on Ukraine. *Intelligence and national security*, 39 (3), 420–442. <https://doi.org/10.1080/02684527.2024.2330133>.
- Miller, B.H., 2018. Open source intelligence (OSINT): an oxymoron? *International journal of intelligence and CounterIntelligence*, 31 (4), 702–719.
- Mishra, V., et al., 2020. Don't count me out: on the relevance of ip address in the tracking ecosystem. *Proceedings of The Web Conference 2020*. 808–815.
- @mm0ndx [McGowan, C.], 2022. Russian Navy frequency (8131Khz) in use. websdr.ewi.utwente.nl:8901/ Lots of other frequencies here. Anyone heard anything else other than 8131? [Tweet]. Twitter. 25 January. Available from: <https://twitter.com/mm0ndx/status/1486019950204665858>.
- Murphy, G. and Salomone, S., 2013. Using social media to facilitate knowledge transfer in complex engineering environments: a primer for educators. *European journal of engineering education*, 38 (1), 70–84.
- nde [@5472_nde], 2022. #RussianAF #BEARNET active ... faint number groups on Moscow Rx via Websdr ... 8131khz HFNet. 0958z [Tweet]. Twitter. 26 January. Available from: https://twitter.com/5472_nde/status/1486277369765801985.
- Newman, M.E. and Girvan, M., 2004. Finding and evaluating community structure in networks. *Physical review E*, 69 (2), 026113.
- O'Brien, J.C., 1993. The international tribunal for violations of international humanitarian law in the former Yugoslavia. *American journal of international Law*, 87 (4), 639–659.
- Oerlemans, J.J. and Langenhuijzen, S., 2024. Balancing national security and privacy: examining the use of commercially available information in OSINT practices. *International journal of intelligence and CounterIntelligence*, 1–19. <https://doi.org/10.1080/08850607.2024.2387850>.
- Organ, D.W., 1971. Linking pins between organisations and environment: individuals do the interacting. *Business horizons*, 14 (6), 73–80.
- Pastor-Galindo, J., et al., 2020. The not yet exploited goldmine of OSINT: opportunities, open challenges and future trends. *IEEE access*, 8, 10282–10304.
- Pathak, A., Madani, N., and Joseph, K., 2021. A method to analyze multiple social identities in twitter bios. *Proceedings of the ACM on human-computer interaction*, 5 (CSCW2), 1–35.
- @PE1RDP, 2022. Now Russian military comms at 5125kHz. Also activity logged at 4397, 4610 and 4649.5 Heard clear at my websdr [Tweet]. Twitter. February 26. Available from: <https://twitter.com/PE1RDP/status/1497672347406508034>.
- Pernice, I., 2018. Global cybersecurity governance: a constitutionalist analysis. *Global constitutionalism*, 7 (1), 112–141.
- Robson Morrow, Maria A., 2022. Private sector intelligence: on the long path of professionalization. *Intelligence and national security*, 37 (3), 402–420. <https://doi.org/10.1080/02684527.2022.2029099>.
- Quaglia, L. (2020). *The politics of regime complexity in international derivatives regulation*. Oxford: Oxford University Press
- Quaglia, L. (2022). *The perils of international regime complexity in shadow banking*. Oxford: Oxford University Press.
- Quaglia, L. and Spendzharova, A., 2022. Regime complexity and managing financial data streams: the orchestration of trade reporting for derivatives. *Regulation and governance*, 16 (2), 588–602.
- Quaglia, L. and Spendzharova, A., 2023. Explaining the EU's uneven influence across the international regime complex in shadow banking. *Politics and governance*, 11 (2), 6–16.

- Rubin, S., 2023. Politicians called them “traitors”. Now they’re manning Israel’s home front. *Washington Post*, 14 October. Available from: <https://www.washingtonpost.com/world/2023/10/14/israel-brothers-in-arms-gaza-border/>.
- Schabas, W.A., 2006. *The UN international criminal tribunals: the former Yugoslavia, Rwanda and Sierra Leone*. Cambridge, UK: Cambridge University Press.
- Schaurer, F. and Störger, J., 2013. The evolution of open source intelligence (OSINT). *The intelligence: journal of U.S. intelligence studies*, 19 (3), 53–56.
- ShadowBreak Intl. [@sbreakintl], 2022. Using publicly available web radio receiver (websDR), call-signs of Russian military units and roles were discovered. Reports of losses, injuries, [Tweet]. Twitter. 1 March. Available from: <https://twitter.com/sbreakintl/status/1498619319730974726>.
- Sherman, J., 2022. The open data market and risks to national security, *Lawfare*, 3 February 2022. Available from: <https://www.lawfaremedia.org/article/open-data-market-and-risks-national-security>.
- Sikkink, K. and Kim, H.J., 2013. The justice cascade: the origins and effectiveness of prosecutions of human rights violations. *Annual review of law and social science*, 9, 269–285.
- Steele, R.D., 2007. Open source intelligence. In: L.K. Johnson, ed. *Handbook of intelligence studies*. London: Routledge, 129–147.
- Stein, R., et al. 2022. Under fire, out of fuel: what intercepted Russian radio chatter reveals. *The New York Times*. Available from: <https://www.nytimes.com/video/world/europe/10000008266864/russia-army-radio-makariv.html> [Accessed 25 Oct 2023].
- @Techjournalisto, 2022. Insanely ingenious conflict #OSINT, listening in on RUSS Navy frequency-move yellow slider: on 8131Khz (via @mm0ndx), didnt pick up: [Tweet]. Twitter. January 25. Available from: <https://twitter.com/Techjournalisto/status/1486046609305739264>.
- Traag, V.A., Waltman, L., and Van Eck, N.J., 2019. From Louvain to Leiden: guaranteeing well-connected communities. *Scientific reports*, 9 (1), 5233.
- Tuinier, P., Zaalberg, T.B., and Rietjens, S., 2023. The social ties that bind: unraveling the role of trust in international intelligence cooperation. *International journal of intelligence and CounterIntelligence*, 36 (2), 386–422.
- Walker, J.R., 2018. The rise of GEOINT: technology, intelligence and human rights. In: S. Ristovska and M. Price, eds. *Visual imagery and human rights practice*. Cham, Switzerland: Springer, 67–88.
- Websdr.org, n.d. Available from: <http://www.websdr.org/>.
- Williams, H.J. and Blum, I., 2018. *Defining second generation open-source intelligence (OSINT) for the defense enterprise*. Santa Monica: RAND Corporation. Available from: <https://apps.dtic.mil/sti/pdfs/AD1053555.pdf>.
- Xie, Y., et al., 2007. How dynamic are ip addresses? *Proceedings of the 2007 conference on applications, technologies, architectures, and protocols for computer communications*, 301–312.
- Yeung, C.M.A., et al., 2023. Decentralisation: the future of online social networking. In: O. Seneviratne, and J. Hendler, eds. *Linking the world’s information: essays on Tim Berners-Lee’s invention of the World Wide Web*. New York: Association for Computing Machinery Digital Library, 187–199.
- @zcyjbrooker [erich_auerbach], 2022. Russian language use on 3675 kHz apparently really picking up. websdr.ewi.utwente.nl:8901/ [Tweet]. Twitter. 19 February. Available from: <https://twitter.com/zcyjbrooker/status/1495181127690211347>.