CHAPTER 4

Open-Source Intelligence in the Russia-Ukraine War

Hannah van Beek & Sebastiaan Rietjens*

Abstract

Since the Russian invasion of Ukraine in February 2022, a steady flow of information has allowed audiences to watch the Russia-Ukraine war unfold in real-time. In contrast to earlier conflicts, the role of amateur analysts as well as open-source organisations stands out. On a large scale, they collect and process publicly available information and subsequently disseminate open-source intelligence analyses. This chapter explores the open-source community in the Russia-Ukraine war with a specific emphasis on these amateur analysts and open-source organisations. Based on numerous news articles, social media posts and reports on open-source intelligence in the Russia-Ukraine War, the chapter identifies four main functions of open-source intelligence, namely 1) debunking and refuting false narratives, 2) reshaping perceptions, 3) informing military troops, and 4) documenting potential war crimes and human rights violations. The main issues the open-source community in the Russia-Ukraine war face include 1) information verification being time-consuming and complicated, 2) ethical and legal problems and 3) the vulnerability of the community and its network infrastructure.

Keywords: Open-source intelligence, OSINT, social media, Bellingcat

1. Introduction

A steady flow of information allows audiences to watch the Russia-Ukraine war unfold in real-time. The information available is very diverse and consists of video feeds, photographs, reports and satellite imagery amongst others. However, in contrast to earlier conflicts, amateur and semi-professional intelligence analysts play a great role in disclosing this information. They produce intelligence analyses based solely on open-source information. One of these amateur intelligence analysts, Justin Peden, was a 20-year-old sophomore from the University of Alabama. He searched through satellite images, TikTok video and security feeds and shared his

* This author uses a pseudonym.

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

findings on troop movements and aircraft models with more than 220,000 followers on Twitter.[2] In addition to individual researchers, several organisations such as the Institute for the Study of War (ISW) and Bellingcat concentrate on generating intelligence solely based on open sources. The ISW, for example, provides a daily update covering the key events of the conflict, including street level assessments and interactive mapping. As such, these individuals and organisations conduct the type of work that intelligence agencies do behind closed doors. And in many cases, these newcomers seem to outperform governmental intelligence agencies.[3]

There is a growing body of literature addressing open-source intelligence (OSINT), which is generally defined as the process of collecting, processing and analysing public information from open data sources to generate knowledge and produce actionable intelligence.[4] Recent publications address the history of OSINT,[5] the role of social media,[6] as well as ethical issues[7] amongst others. This chapter builds upon this literature and explores the open-source community in the Russia-Ukraine war. The chapter emphasises amateur analysts as well as open-source organisations such as ISW but largely excludes intelligence agencies and their use of open sources.

To meet this objective, this study adopts a case study approach. The data included in this study contains numerous news articles, social media posts and reports on open-source intelligence in the Russia-Ukraine War. These data have been collected through keyword searches via university libraries and digital libraries, such as Google Scholar, ResearchGate and JSTOR, as well as a plethora of news and social media websites. Keywords included combinations of e.g. 'open-source information,' 'public data,' 'Russia,' 'Ukraine,' 'OSINT' and 'satellite imagery.' Content analysis was conducted to identify patterns in the data. To this effect words, themes and concepts within the texts were categorised and subsequently analysed.

This paper is structured as follows. Section 2 presents the main function of open-source intelligence. Section 3 subsequently addresses the main issues the individuals and organisations of the open-source community face. Section 4 discusses the results and concludes the chapter.

[2] Schwartz, "Amateur open- Source researchers went viral unpacking the war in Ukraine."

[3] Rietjens, "The future of NLDISS," 12-23.

[4] European Commission, *Open-Source Intelligence*.

[5] Block, "The long history of OSINT."

[6] Dover, "SOCMINT: a shifting balance of opportunity," 216-232.

[7] Bean, "Is open source intelligence an ethical issue?" 385–402.

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

2. Functions of open-source intelligence

Early 2023, the Economist published the article 'Open-source intelligence is piercing the fog of war in Ukraine.'[8] This is generally seen as the main function of OSINT: to provide insight in a complex and cluttered environment. The story of open-source intelligence in the Russia-Ukraine war, however, begins long before Russia's invasion of Ukraine on February 24th, 2022. As early as April 2021, digital evidence, such as social media posts by Belarusian, Russian, and Ukrainian civilians as well as commercial satellite imagery showed the mobilisation of Russian troops along the Russia-Ukraine border[9] This prompted graduate student Steven De La Fuente to scour commercial satellite imagery.[10] His search led to the main road from Belgorod, Russia, to Ukraine's Kharkiv, where he saw the build-up of armored personnel carriers, mobile missile launchers, and other military vehicles. The videos were not the only direct indication of an invasion. Hours before Putin announced the start of 'special military operations,' analysts at the Middlebury Institute of International Studies saw a 'traffic jam' appear at 3:15 a.m., at the same spot where De La Fuente had seen the build-up.

Since the invasion in February 2022, the open-source community has been shedding light on the Russia-Ukraine conflict and offering it in real-time.[11] The information used comes from a variety of sources, including mapping data, metadata, smartphone footage posted on social media, as well as high-resolution overhead images captured by commercial satellite companies.[12] Unlike during most previous major conflicts, nearly everyone, military or civilian, carries a phone with a camera and can upload footage in a matter of seconds.[13] The Ukrainian population, in particular, has grown to become 'a gigantic, distributed, open-source sensor network,' providing details on Russian troops via social media.[14]

As a result of this, using open sources has enabled analysts to gain insight into on-the-ground events; document materiel losses, targets, and casualties; track military infrastructure; and determine the impact of an attack[15] OSINT analysts on Twitter, for example, have kept tallies of verified major equipment losses on both

[8] The Economist, "Open-source intelligence is piercing the fog of war in Ukraine."

[9] Burgess, "If Russia invades Ukraine, TikTok will see it up close"; For instance in*:* Visontay et al.; Woodruff, Swan, and McLeary.

[10] Aldhous and Miller, "How open-source intelligence is helping clear the fog of war in Ukraine."

[11] For instance in: Lippert, "Open-source methods, the cyber weapon anyone can use in Ukraine War."

[12] Aldhous and Miller, "How Open-source intelligence is helping clear the fog of war in Ukraine."

[13] Puiu, "How open-source intelligence (OSINT) is exposing the Ukraine war in real-time."

[14] Abdalla, Davies, Gustafson, Lomas, and Wagner, "Intelligence and the war in Ukraine: Part 1."

[15] Datta, "OSINT comes of age for near real time coverage of Ukraine conflict"; Moran, "Open-source intelligence: how digital sleuths are making their mark on the Ukraine war."

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access -

sides, and social media footage has indicated structural problems with the quality of parts and maintenance of Russian equipment.[16] In addition, automated air-traffic data and similar online tools have allowed journalists and analysts to track yachts of Russian oligarchs against whom international sanctions have been imposed.[17]

An excellent example of the coordinated use of open-source intelligence is *Eyes on Russia.* Within this project, leading open-source organisations, as well as amateurs, have been collaborating to provide a live picture of the ongoing conflict. The project's database contains thousands of entries that can be used to create a timeline which can be filtered on multiple categories, including military presence, bombings, civilian casualties, and military losses.[18] The above made an open analyst conclude: 'there will always be a fog of war, but I think it is the thinnest veil of war we've ever had.'[19] When we unravel the general notion of piercing the fog of war, we identify four functions of OSINT: debunking false narratives, reshaping perceptions, informing military troops and documenting potential war crimes and human rights violations. These are now elaborated on.

2.1 Debunking false narratives

The first function is debunking and refuting false narratives. Propaganda and erroneous narratives have been trusted strategies to win hearts and minds, and the Russia-Ukraine war is no exception. Both Russia and Ukraine engage in a rhetorical conflict in an attempt to sway international sentiment.[20] OSINT serves as a crucial line of defense in favour of the truth, by determining what did and what did not really happen.[21] To this effect, OSINT researchers, (mainly) Western governments and long-established news organisations have played a key role. Several traditional media outlets have started developing their in-house OSINT capabilities, establishing teams tasked with incorporating open sources and OSINT techniques into their investigative journalism activities.[22] Examples include the New York Times Visual Investigations team, France 24 Observers, and the NOS OSINT team in The Netherlands.

[16] Puiu, "How open-source intelligence (OSINT) is exposing the Ukraine war in real-time"; Janovský, "How open-source data got the Russia-Ukraine War right."

[17] Duncan, Blood, McIntyre, and Davies, "Jets linked to Russian oligarchs appear to have kept flying despite sanctions."

[18] Strick, *Eyes on Russia – Mapping Russia's War on Ukraine #* [Video]. YouTube.

[19] Puiu, "How open-source intelligence (OSINT) is exposing the Ukraine war in real-time";

[20] O'Brien, "Open source intelligence may be changing old-school war"; GlobalData, "The role of OSINT in the war in Ukraine."

[21] Freear, "OSINT in an age of disinformation warfare."

[22] Moran, "Open-source intelligence: how digital sleuths are making their mark on the Ukraine war."

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

Perhaps the most notorious example of the use of OSINT to counter an inaccurate narrative comes from the town of Bucha, where photographs show widespread wreckage and corpses in civilian clothing strewn across streets.[23] Russia denounced the images as 'another hoax' and in an effort to influence the narrative, Russian Foreign Minister Sergey Lavrov asserted that Ukrainians had staged the scene after Russian forces withdrew.[24] Using commercial satellite photos and video footage to cross-reference, the Visual Investigations team of The New York Times debunked these claims. The images showed that the bodies had been laying on the ground for weeks before Russian forces had retreated and Ukrainian forces arrived.[25]

Although most cases concern pro-Russian dis- and misinformation, there have also been several examples of debunked pro-Ukrainian claims. A famous example is the 'Ghost of Kyiv,' a story which emerged within the first days of Russia's attack. Several Ukrainian news sites and official Ukrainian government Twitter accounts spread the news that a Ukrainian jet pilot had taken down six enemy aircrafts in the first 30 hours of Russia's invasion.[26] Soon after photos and a video allegedly portraying the pilot had started circulating, OSINT analysts proved these were fake and that the clip was created with a video game.[27]Although the Ukrainian Ministry of Defence first promoted the tale, its Air Force later admitted that it was a myth, 'created by Ukrainians.'

2.2 Reshaping perceptions

The second function of OSINT in the Russia-Ukraine war is to reshape perceptions amongst the general public as well as amongst the troops. The Centre for Emerging Technology and Security (2022) underlines the importance of public perceptions: 'Wars are won by human actions and human decisions. Some decisions are taken on the battlefield–to stand and fight, or to flee. But many crucial decisions are taken elsewhere: by foreign political leaders, who must decide how far to go in defence of their values and interests in supporting either side. In democracies, politicians cannot go further than the public will support, so individual citizens' beliefs count, too.'

OSINT has a prominent role in this conflict and some even argued it represents an entirely new chapter of the political and diplomatic use of intelligence

[23] Higgins, "Russia's Bucha 'facts' versus the evidence."

[24] Salerno-Garthwaite, "OSINT in Ukraine: civilians in the kill chain and information space."

[25] Browne, Botti, and Willis, "Satellite images show bodies lay in Bucha for weeks, despite Russian claims."

[26] Romansky, Boswinkel, and Rademaker, *The Parallel Front: An Analysis of the Military Use of Information in the First Seven Months of the War in Ukraine*.

[27] Eisele, "Fact check: The "Ghost of Kyiv" fighter pilot."

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

in international affairs.[28] There are two main reasons for this. First, by exposing the horrors of the war (such as the bloodshed in Bucha and the Russian use of unguided munitions against civilian targets) and refuting official Russian government narratives, OSINT revelations have swung the international opinion in favour of Ukraine.[29] The discoveries of potential human rights violations and war crimes have proven politically damning for the Russian government as they have horrified Western society as a whole and have become part of the wider public discourse, thereby reaching diplomats and foreign policy decision-makers at the state level.[30] This has put tremendous political pressure on Western governments to sanction Russia and arm Ukraine.[31] As a result, an increasing number of countries have provided Ukraine with (military) support.[32]

2.3 Informing military troops

The third function of OSINT is to inform military troops. There are few reports addressing the use of OSINT for military purposes by (pro-)Ukrainian troops, and even fewer about (pro-) Russian troops. Juliette Kayyem, former Assistant Secretary of the U.S. Department of Homeland Security, argues that this is 'a war where the crowd is essentially helping to make tactical decisions. People are making decisions about where they want to attack, [and are establishing] where the Russian tanks are, or what we are seeing in the skies, based on the [man or woman] on the street with an iPhone.'[33]

As such, social media platforms and mobile phones are a force multiplier.[34] This is especially true when it comes to coordinating OSINT collection for targeting activities, as civilians share coordinates with their smartphones. Identifying the location of military targets has traditionally been a task that military personnel execute, but now it is also entrusted to civilian information infrastructures. In an effort to crowdsource intelligence, the Ukrainian government asked citizens to help

[28] Abdalla, Davies, Gustafson, Lomas, and Wagner, "Intelligence and the war in Ukraine: Part 1."

[29] GlobalData, "The role of OSINT in the war in Ukraine"; Smith-Boyle, "How OSINT has shaped the war in Ukraine."

[30] Lahmann, "Ukraine, open-source investigations, and the future of international legal discourse," 810–820.

[31] GlobalData, "The role of OSINT in the war in Ukraine"; Smith-Boyle, "How OSINT has shaped the war in Ukraine"; Hockenhull, *How open-source intelligence has shaped the Russia-Ukraine war*.

[32] Smith-Boyle, "How OSINT has shaped the war in Ukraine."

[33] O'Brien, "Open source intelligence may be changing old-school war."

[34] O'Brien and Toubman, "Open source intelligence combats disinformation on Russia's war against Ukraine."

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

them locate Russian troops.[35] Standardised chatbots in the government's public services app, Diia, allow them to report Russian units and locations and geotag pictures and videos of Russian troop movements.[36] In this respect, the Ukrainian Security Service tweeted: 'Your messages about the movement of the enemy through the official chatbot [...] bring new trophies every day.'

Another example of the use of social media information for military purposes is the images taken on August 8th, 2022 by a pro-Russian journalist, who shared them on the messaging app Telegram.[37] The photos supposedly show the local headquarters of the Russian Wagner paramilitary group. The nameplate on the building was apparent in the images, effectively revealing the group's location as it indicated the address.[38] Ukrainian forces reduced the headquarters to ruins a few days after the photographs were published online.[39]

Likewise, a pro-Russian OSINT organisation allegedly utilised video footage from a Ukrainian news channel to locate and launch a missile at a munitions factory in Kyiv, killing three civilians.[40] Although these examples seem indicative of the use of OSINT for targeted killing, it is most probable that OSINT was combined with various other sources to provide the intelligence required for armed forces to target enemy forces.[41]

2.4 Documenting potential war crimes and human rights violations

Since the early days of the invasion of Ukraine in February 2022, openly available content has become a tool for online investigators and NGOs to search for evidence of war crimes and human rights violations.[42] Cases include the systematic and pervasive bombing of Ukrainian medical institutions, the bloodshed in Bucha, and a cluster munition strike on a kindergarten outside of Kharkiv, which resulted in the deaths of three civilians.[43] To prosecute potential war crimes or human rights violations, OSINT may serve as lead evidence. It can provide concrete proof of violations,

[35] Abdalla, Davies, Gustafson, Lomas, and Wagner, "Intelligence and the war in Ukraine: Part 2."

[36] O'Brien and Toubman, "Open source intelligence combats disinformation on Russia's war against Ukraine."

[37] Burgess, "Their photos were posted online. then they were bombed."

[38] Salerno-Garthwaite, "OSINT in Ukraine: civilians in the kill chain and information space."

[39] Burgess, "their photos were posted online. then they were bombed."

[40] Idem.

[41] Salerno-Garthwaite, "OSINT in Ukraine: civilians in the kill chain and information space."

[42] Lippert, "Open-source methods, the cyber weapon anyone can use In Ukraine War."

[43] E.g.: Sabbagh, "Researchers gather evidence of possible Russian war crimes in Ukraine"; Oxendine, "Open-source data documents war atrocities in Ukraine"; Higgins, "Russia's Bucha 'facts' versus the evidence."

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

and can be used in addition to field investigation and testimonies collected on site.[44] Gabriela Ivens, the Head of Open Source Research at Human Rights Watch, states: 'We look for nearby military targets which could have been a legitimate target, or evidence that the attack was disproportionate. We look for the type of weapons used, the chain of command, the affected buildings and the human toll.'[45]

Normally, evidence used in war crime cases consists of witness testimonies and forensic evidence, yet these can be difficult to collect. As the types of accessible open sources and the number of OSINT tools are expanding, it seems highly likely that open-source investigation methods and evidence may fill in crucial gaps.[46] Although trials have yet to take place, prosecutors of the International Criminal Court appear willing to use OSINT as evidence of atrocities committed in Ukraine.[47]

However, for evidence to be admissible in court, verified open-source information needs to be gathered, documented, and made accessible to accountability.[48] In response, the OSINT community has been documenting and studying evidence that could be useful in the future. Initiatives such as *Eyes on Russia*, for instance, not only map, document and verify significant incidents for the purpose of conveying to the public the events of the conflict, they also document these actions to hold potential human rights violators accountable. Likewise, the U.S. Department of State has announced the establishment of the Conflict Observatory, a hub site that employs open sources to create reports for upcoming civil and criminal legal processes and assist victims in seeking compensation and restitution.[49] Unsurprisingly, collecting evidence from online sources to meet the standards of a criminal court necessitates painstaking work.[50] As a reported MIT Technology Review states: 'It's not enough to just see a video of an attack or a photo of dead bodies.'[51]

[44] Lippert, "Open-source methods, the cyber weapon anyone can use In Ukraine War."

[45] Lippert, "Open-source methods, the cyber weapon anyone can use in Ukraine War.'

[46] Idem. Simonite, "The race to archive social posts that may prove Russian war crimes."

[47] International Criminal Court, *Ukraine*.

[48] Freear, "OSINT in an age of disinformation warfare"; Bacchi and Reuters, "Ukraine invasion played out online as web sleuths trawl intelligence."

[49] Vick, "Bellingcat's Eliot Higgins explains why Ukraine is winning the information war."

[50] Simonite, "The race to archive social posts that may prove Russian war crimes."

[51] Basu, "The online volunteers hunting for war crimes in Ukraine."

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access -

3. Issues related to open-source intelligence

In addition to the different functions of OSINT, the findings of this study show that the OSINT community faces many issues in the Russia-Ukraine war. These issues include the verification of information, ethical and legal issues and the vulnerability of the network. Each of these issues is elaborated on in this section.

3.1 Verification is time-consuming and complicated

Historically, the main issue of OSINT has been the vast amount of information which needs verification.[52] This is also prevalent in the Russia-Ukraine war. The verification of information is complicated due to a variety of factors and no longer solely due to information overload. More than any prior conflict, the Russia-Ukraine war has been plagued by mis- and disinformation, and it is no longer a question *if*, but *which* social media posts contain fabricated stories and erroneous narratives. TikTok, especially, has become a platform for fake videos and livestreams about the conflict, combining dramatic footage of military videogames, computer-generated imagery and videos of old conflicts. Coincidentally, according to research funded by the United Kingdom, the Russian government has been employing a so-called 'troll factory' to disseminate false information on social media and in online comment sections, with the intention of manipulating international public opinion on Russia's actions in Ukraine.[53] As a result, the amount of open-source information which necessitates fact-checking and verification has increased.

Information verification is further complicated by images and videos spread by pro-Russian social media and fake fact-checking channels.[54] These posts claim to refute 'fakes' made by the Ukrainians that depict damaged Russian military units or Russian air strikes destroying civilian infrastructure. Except, the posts 'debunk' non-existent, fake posts and videos.[55] Researchers at Clemson University's Media Forensic Hub and ProPublica have identified over twenty such posts, but it is likely that many more exist, and although the videos have over a million views, it is not clear who has created them. According to ProPublica: 'The videos combine with propaganda on Russian state TV to convince Russians that the "special

[52] Hatfield, "There is no such thing as open source intelligence."

[53] Foreign, Commonwealth & Development Office, Truss and Dorries, *UK Exposes Sick Russian Troll Factory Plaguing Social Media with Kremlin Propaganda.*

[54] Idem.

[55] Centre for Emerging Technology and Security, *The Information Battlefield: Disinformation, Declassification and Deepfakes: CETaS Expert Analysis.*

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

operation" in Ukraine is proceeding well, and that claims of setbacks or air strikes on civilian areas are a Ukrainian disinformation campaign to undermine Russian confidence.'[56]

Social media companies are urged to moderate the content users post on their platforms and they could, in theory, lessen the burden that information overload has placed on the OSINT community.[57] In practice, however, some social media platforms seem either unable to moderate content, or are simply unwilling to do so. Several platforms have been labelling false or misleading viral videos about the conflict, but the amount of information posted seems to be too much for content moderators employed by social media platforms to handle.[58] In addition, researchers have expressed dissatisfaction with the way TikTok is handling this problem, as the platform does not provide transparency or analytic tools to academics, researchers and journalists, which misinformation experts have long since requested. As one researcher notes: 'When TikTok fails to ensure the accuracy of information receiving millions of views on its platform, that burden is falling on outside researchers and everyday TikTok users.'[59]

Instead of trusting TikTok and other companies to verify the content posted to their platforms, independent fact-checkers have been manually researching that content themselves – an incredibly time-consuming process.[60] The process of confirming sources and information is necessary in order to counteract the majority of risks associated with reflexive control: the control someone has over their opponent's decisions by imposing presumptions that influence how they act. Like other intelligence collection disciplines such as human intelligence, OSINT runs the risk of being used as so-called 'chickenfeed.' This necessitates rigorous validation. Varzhanskyi[61] furthermore criticises the use of OSINT and states it is often the result of a 'serendipitous discovery' and at times analysts mistake the quantity of evidence to support a claim for the quality of that claim.

[56] Silverman and Kao, "In the Ukraine conflict, fake fact-checks are being used to spread disinformation."

[57] Oremus, "Social media wasn't ready for this war. It needs a plan for the next one."

[58] NOS, "Meta verwijdert Russische desinformatie over Oekraïne, gericht op Europa"; Bacchi and Reuters, "Ukraine invasion played out online as web sleuths trawl intelligence."

[59] Sardarizadeh, "Ukraine war: False TikTok videos draw millions of views."

[60] Varzhanskyi, "Reflexive control as a risk factor for using OSINT: Insights from the Russia–Ukraine conflict,"1–31.

[61] Idem.

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

3.2 Ethical and legal issues

Professional open-source initiatives and collectives have ethical and legal standards they hold themselves to.[62] Twitter group chats, for example, have developed informal behavioural rules when sharing and verifying information.[63] These rules include a ban on sharing graphic videos of dead bodies and keeping Ukrainian troop movements under wraps. When members of these collectives unintentionally release inaccurate or misleading information, they are supposed to remove their tweets and 'issue corrections.' The informal atmosphere and communication between analysts help them avoid making mistakes. While these informal ethical guidelines and verification techniques have been honed over the last decade, the ethical and legal issues of open-source intelligence within the Russia-Ukraine conflict have, however, all but been resolved.

The OSINT community consists of 'all types of people.'[64] Numerous anonymous internet users have earned recognition as a result of the reliability of their open-source investigations. However, as more individuals become interested in the hobby of sharing and dissecting information online – a hobby which has no professionally enforced norms or ethical codes of conduct – there is concern that their activities may endanger lives or unintentionally contribute to sharing false narratives.[65] When social media accounts with many followers post information, this information spreads rapidly, regardless of whether or not it is correct.[66]

OSINT has also generated criticism since its community serves as investigator, judge, juror, and executioner in 'the court of public opinion.'[67] Freear[68] argues that some open-source organisations receive government funding, but act more as activists than as journalists. In a similar line, Lahmann[69] argues that the biases and prejudices of individuals or open-source organisations may wittingly be incorporated. Furthermore, they might, wittingly or unwittingly, publish information that originates from a malicious source or disclose classified or otherwise secured

[62] Schwartz, "As grisly images spread from Ukraine, open-source researchers ask what's too gory to share."

[63] Perrigo, "How open source intelligence became the world's window into the Ukraine invasion."

[64] Lippert, "Open-source methods, the cyber weapon anyone can use in Ukraine war."

[65] Verma, "The rise of the Twitter spies."

[66] The Week, "What is open-source intelligence – and how is it helping to map the Ukraine war?"

[67] Freear, "OSINT in an age of disinformation warfare."

[68] Idem.

[69] Lahmann, "Ukraine, open-source investigations, and the future of international legal discourse, 810–820.

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

information. Lahmann[70] therefore concludes that 'we should not naively take civil society actors engaging in open-source investigations as neutral arbiters of truth by default.'

The international community of volunteers InformNapalm illustrates this dilemma well.[71] The goal of this community is to 'debunk myths and expose secrets of the Russian hybrid war' and it has been described as a 'Ukrainian activist website'[72] as well as a 'volunteer activist group.'[73] On several occasions InformNapalm published correspondence of Russian state officials[74] and personal information about Russian military officers,[75] that hackers had provided them. Although this information might have great value, few would consider InformNapalm to be a 'neutral arbiter of truth.'

Finally, the use of facial recognition raises a whole slew of ethical concerns.[76] Firstly, mismatches could make it harder for civilians to stay hidden in battle zones or could even lead to civilian deaths.[77] Second, the use of facial recognition is prone to questions about privacy, racism and other technological and cognitive biases. In fact, Clearview AI, the company whose services both Ukraine and the United States use, is facing lawsuits in the U.S., accusing it of violating privacy rights by taking people's images from the Internet without their consent.[78] Even those who do not have social media accounts and only appear in the background of a photo uploaded to the Internet, may appear in databases used by facial recognition software.[79] Third, the use of such software to identify dead soldiers and civilians may appear to be the least harmful way to use the technology in conflict, but oversight experts are worried that 'once you introduce these systems and the associated databases […], you have no control over how it will be used and misused.'[80]

[70] Idem.

[71] According to its website, InformNapalm does not receive any governmental funding.

[72] The Guardian, "Ukrainian bloggers use social media to track Russian soldiers fighting in east."

[73] BBC, "Ukraine conflict: Hackers take sides in virtual war."

[74] For instance at Inform Napalm, "Hacking Andrey Lugovoy, member of the Russian State Duma, First Deputy Head of the Security Committee."

[75] For instance at Inform Napalm, "Hacking Lieutenant Colonel Kasatkin, Russian war criminal, head of Combat Training of A-50 early warning aircraft, military unit 41520."

[76] Dave and Dastin, "Exclusive: Ukraine has started using Clearview AI's facial recognition during war."

[77] Hill, "Facial recognition goes to war."

[78] Dave and Dastin, "Exclusive: Ukraine has started using Clearview AI's facial recognition during war."

[79] Hill, "Facial recognition goes to war."

[80] Dave and Dastin, "Exclusive: Ukraine has started using Clearview AI's facial recognition during war."

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

3.3 Vulnerability of the network

In 2012, Omand et al.[81] wrote that passive bystanders can now 'become active citizen journalists, providing and relaying information from the ground.' They regarded this as a positive development, as it could improve communication between the government and its citizens. The Russia-Ukraine war, however, has made it clear that 'letting civilians partake' in collecting information to create intelligence does not only have upsides. We highlight two underlying issues: the vulnerability of the network and the blurring between civilians and combatants.

First, although the OSINT community's use of online networks has made it reasonably resilient to physical targeting,[82] online networks are not immune to inference or attacks. In February 2022, for example, Ukrainian government websites and online services like the government app Diia faced cyberattacks, such as DDoS attacks.[83] Similarly, several researchers who posted footage of the war on social media found their Twitter accounts being suspended.[84] Some of them received a message saying their activity on the platform violated the Twitter rules, yet the exact violation was not specified. Although a Twitter spokesperson later announced that these suspensions were an error and not part of a coordinated campaign intended to disable OSINT accounts, the OSINT community became painfully aware of how easily their voices can be silenced.[85]

When Ukrainian data servers and cell towers were under attack from physical missiles, the Ukrainian government sought solutions to protect its internet infrastructure.[86] This led them to Elon Musk's company Starlink, which connects mobile internet terminals to a satellite and establishes a dispersed communications network. Although Starlink's network is less susceptible to being jammed or otherwise interfered with, its satellites could become targets of cyberattacks, physical attacks and spoofing, which is the term for when a radio is used to fake a GPS signal.[87] This could have grave consequences for the OSINT community. Although such a scenario has yet to occur, Russia has openly demonstrated its ability to destroy satellites, and Konstantin Voronstov, Russia's senior foreign ministry official, told the United Nations that 'quasi-civilian infrastructure may be a legitimate target for

[81] Omand, Bartlett, and Miller, "Introducing Social Media Intelligence (SOCMINT)," 801–823.

[82] Freear, "OSINT in an age of disinformation warfare."

[83] Tett, "Inside Ukraine's open-source war."

[84] Faife, "Twitter accounts sharing video from Ukraine are being suspended when they're needed most."

[85] Albon, "How commercial space systems are changing the conflict in Ukraine."

[86] Tett, "Inside Ukraine's open-source war."

[87] Meaker, "High above Ukraine, satellites get embroiled in the war."

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

a retaliatory strike.'[88] The matter of satellite security is further complicated by the fact that neither a procedure for reporting cyberspace attacks nor a procedure for cooperation on a joint response to such an attack have been established.[89]

As a second issue, observers have expressed their worry about the increasingly blurred lines between civilians and combatants.[90] Civilians are under protection of international humanitarian law, so long as they avoid participating in military conflicts.[91] When open-source analysts and citizens share intelligence online that critically informs or otherwise supports hostile military actions, would that cause them to lose their civilian status and potentially be tried for espionage under the law of war? If so, would they thereby become legitimate targets for retaliation and attacks? Such questions have started a debate amongst OSINT analysts on whether to publish videos taken by citizens from their homes, for example, given that these individuals might be identified and geolocated.[92]

4. Discussion and conclusion

The significance of information from open sources has long been acknowledged, but especially in the last few decades, this topic has garnered great attention.[93] 'With the coming of the information age in particular, the rise of the Internet and the digital domain for production and storage of information, the nature and volume of publicly available information has changed fundamentally,' Block remarks. However, while most research on OSINT in intelligence studies emphasises its use by intelligence agencies, this chapter highlights the role of individuals and open-source organisations to generate OSINT in the Russia-Ukraine war. The chapter argues that the increasing availability and accessibility of open-source information has largely democratised the field of intelligence. As a result, individuals and open-source organisations increasingly challenge traditional intelligence agencies as the main intelligence provider on war and conflict. By generating OSINT, these individuals and organisations contribute to debunking false narratives, reshape perceptions, inform military troops and document potential war crimes and human rights violations.

[88] Idem.

[89] Albon, "How commercial space systems are changing the conflict in Ukraine."

[90] Aldhous and Miller, "How open-source intelligence is helping clear the fog of war in Ukraine."

[91] O'Brien, "Open source intelligence may be changing old-school war."

[92] Aldhous and Miller, "How open-source intelligence is helping clear the fog of war in Ukraine."

[93] Block, "The long history of OSINT."

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

In doing this, the open-source community and its network infrastructure display many vulnerabilities. The community lacks guidelines on how to verify information and protect itself from harm, whilst part of this community at the same time unjustly regards its analyses as comprehensive. Furthermore, the use of open sources is associated with many ethical and legal issues, including the use of standards and dealing with the biases and prejudices of the actors involved.

Finally, to better understand the role of OSINT in the Russia-Ukraine war, it is recommended that future studies address declassified sources, for instance on the military use of OSINT, and focus on the relationship between OSINT and other intelligence collection disciplines such as geographical intelligence and human intelligence.[94]

Hannah van Beek

Hannah van Beek is a master student in the field of security studies. During her internship at the Netherlands Defence Academy she conducted research into the role of open source intelligence in the Russia-Ukraine war.

Sebastiaan Rietjens

Sebastiaan Rietjens is a full professor of Intelligence & Security as well the director of the War Studies Research Centre at the Netherlands Defence Academy. He also holds a special chair of Intelligence in War and Conflict at Leiden University. Sebastiaan has done extensive fieldwork in military exercises and operations (Afghanistan (ISAF), Mali (MINUSMA), Poland and the Baltic States (NATO), Greece (FRONTEX)) and has published accordingly in international books and journals including the European Journal of International Relations, International Journal of Intelligence & Counterintelligence, Intelligence & National Security, Human Relations, Armed Forces & Society, Disasters, and Public Management Review. His main research focus is on intelligence during military operations, peacekeeping intelligence, warning for hybrid threats and future developments that confront intelligence organisations.

[94] Hatfield, "There is no such thing as open source intelligence."

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

Bibliography

Abdalla, N. S., Davies, P. H. J., Gustafson, K., Lomas, D., and Wagner, S. "Intelligence and the War in Ukraine: Part 1." *War on the Rocks*, May 11, 2022. https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-1/.

Abdalla, N. S., Davies, P. H. J., Gustafson, K., Lomas, D., and Wagner, S. "Intelligence and the War in Ukraine: Part 2." *War on the Rocks*, May 19, 2022. https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-2/.

Albon, C. "How Commercial Space Systems Are Changing the Conflict in Ukraine." *C4ISRNet*, April 25, 2022. https://www.c4isrnet.com/intel-geoint/2022/04/25/how-commercial-space-systems-are-changing-the-conflict-in-ukraine/.

Aldhous, P., and Miller, C. "How Open-Source Intelligence is Helping Clear the Fog of War in Ukraine." *BuzzFeed News*, March 3, 2022. https://www.buzzfeednews.com/article/peteraldhous/osint-ukraine-war-satellite-images-plane-tracking-social.

Bacchi, U., and Reuters. "Ukraine Invasion Played Out Online as Web Sleuths Trawl Intelligence." *National Post*, February 25, 2022. https://nationalpost.com/pmn/entertainment-pmn/ukraine-invasion-played-out-online-as-web-sleuths-trawl-intelligence.

Basu, T. "The Online Volunteers Hunting for War Crimes in Ukraine." *MIT Technology Review*, March 16, 2022. https://www.technologyreview.com/2022/03/16/1047322/ukraine-russia-war-crimes- evidence/.

BBC. "Ukraine Conflict: Hackers Take Sides in Virtual War." BBC, December 20, 2014. https://www.bbc.com/news/world-europe-30453069

Bean, H. (2011). "Is Open Source Intelligence an Ethical Issue?" *Government Secrecy: Research in Social Problems and Public Policy* 19 (January 2011): 385–402. DOI:10.1108/S0196-1152(2011)0000019024.

Block, L. "The Long History of OSINT." *Journal of Intelligence History* (June 2023). https://doi.org/10.1080/16161262.2023.2224091.

Browne, M., Botti, D., and Willis, H. "Satellite Images Show Bodies Lay in Bucha for Weeks, Despite Russian Claims." *The New York Times*, April 4, 2022. https://www.nytimes.com/2022/04/04/world/europe/bucha-ukraine-bodies.html.

Burgess, M. "If Russia Invades Ukraine, TikTok Will See It Up Close." *WIRED*, February 17, 2022. https://www.wired.com/story/russia-ukraine-military-photos-video/.

Burgess, M. "Their Photos Were Posted Online: Then They Were Bombed." *WIRED UK*, August 26, 2022. https://www.wired.co.uk/article/wagner-group-osint-russia-ukraine.

Centre for Emerging Technology and Security. *The Information Battlefield: Disinformation, Declassification and Deepfakes. CETaS Expert Analysis*. 2022.

Datta, A. "GeoInt, OSINT Comes Of Age For Near Real Time Coverage of Ukraine Conflict." *Geospatial World*, March 7, 2022. https://www.geospatialworld.net/blogs/geoint-osint-comes-off-age-of-ukraine-conflict/.

Dover, R. "SOCMINT: A Shifting Balance of Opportunity." *Intelligence and National Security* 35, no. 2 (2020): 216-232.

Dave, P., and Dastin, J. "Exclusive: Ukraine Has Started Using Clearview AI's Facial Recognition During War." *Reuters*, March 14, 2022. https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/.

Duncan, P., Blood, D., McIntyre, N., and Davies, R. "Jets Linked to Russian Oligarchs Appear to Have Kept Flying Despite Sanctions." *The Guardian*, March 31, 2022. https://www.theguardian.com/world/2022/mar/31/jets-linked-to-russian-oligarchs-appear-to-have-kept-flying-despite-sanctions.

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

Eisele, I. "Fact check: The 'Ghost of Kyiv' Fighter Pilot." *DW*, May 4, 2022. https://www.dw.com/en/fact-check-ukraines-ghost-of-kyiv-fighter-pilot/a-60951825

European Commission. "Open-Source Intelligence. data.europa.eu." *European Commission* May 2, 2022. https://data.europa.eu/en/publications/datastories/open-source-intelligence.

Faife, C. "Twitter Accounts Sharing Video from Ukraine Are Being Suspended When They're Needed Most." *The Verge*, February 23, 2022. https://www.theverge.com/2022/2/23/22947769/twitter-osint-russia-ukraine-invasion-suspended-error.

Truss, E., and Dorries, N. "UK Exposes Sick Russian Troll Factory Plaguing Social Media with Kremlin Propaganda." *Foreign, Commonwealth & Development Office*, May 1, 2022. https://www.gov.uk/government/news/uk-exposes-sick-russian-troll-factory-plaguing-social-media-with-kremlin-propaganda.

Freear, M. "OSINT in an Age of Disinformation Warfare." *RUSI,* March 14, 2022. https://rusi.org/explore-our-research/publications/commentary/osint-age-disinformation-warfare/.

GlobalData. "The Role of OSINT in the War in Ukraine." *Army Technology*, May 6, 2022. https://www.army-technology.com/analyst-comment/osint-war-in-ukraine/.

Hatfield, J.M. "There Is No Such Thing as Open Source Intelligence." *International Journal of Intelligence and CounterIntelligence* (March 2023). DOI: 10.1080/08850607.2023.2172367

Higgins, E. "Russia's Bucha 'Facts' Versus the Evidence." *Bellingcat*, April 4, 2022. https://www.bellingcat.com/news/2022/04/04/russias-bucha-facts-versus-the-evidence/

Hill, K. "Facial Recognition Goes To War." *The New York Times*, April 7, 2022. https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html.

Hockenhull, J. *How Open-Source Intelligence Has Shaped the Russia-Ukraine War*. (n.d.). https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war.

International Criminal Court. *Ukraine*. 2022. https://www.icc-cpi.int/ukraine

Inform Napalm. "Crowdfunding for Targeted Assistance to Informnapalm." https://informnapalm.org/en/donate/.

Inform Napalm. "Hacking Andrey Lugovoy, member of the Russian State Duma, First Deputy Head of the Security Committee." *Inform Napalm*, May 3, 2023. https://informnapalm.org/en/hacking-andrei-lugovoy/.

Inform Napalm. "Hacking Lieutenant Colonel Kasatkin, Russian War Criminal, Head of Combat Training of A-50 Early Warning Aircraft, Military Unit 41520." *Inform Napalm*, July 31, 2023. https://informnapalm.org/en/a-50-kasatkin/.

Janovský, J. "How Open-Source Data Got the Russia-Ukraine War Right." *New Lines Magazine*, April 7, 2022. https://newlinesmag.com/argument/how-open-source-data-got-the-russia-ukraine-war-right/.

Lahmann, H. "Ukraine, Open-Source Investigations, and the Future of International Legal Discourse." *American Journal of International Law* 116, no. 4 (October 2022): 810-820. https://doi.org/10.1017/ajil.2022.52.

Lippert, A. "Open-Source Methods, The Cyber Weapon Anyone Can Use in Ukraine War." *Worldcrunch*, April 29, 2022 https://worldcrunch.com/tech-science/open-source-investigation-war-ukraine.

Meaker, M. "High Above Ukraine, Satellites Get Embroiled in the War." *WIRED UK*, March 4, 2022. https://www.wired.co.uk/article/ukraine-russia-satellites.

Moran, M. "Open-Source Intelligence: How Digital Sleuths Are Making Their Mark on the Ukraine War." *The Conversation*, March 18, 2022. https://theconversation.com/open-source-intelligence-how-digital-sleuths-are-making-their-mark-on-the-ukraine-war-179135.

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

Murray, D., McDermott, Y., and Koenig, K. A. "Mapping the Use of Open Source Research in UN Human Rights Investigations." *Journal of Human Rights Practice* 14, no.2 (2022): 554-581. https://academic.oup.com/jhrp/article/14/2/554/6573245.

NOS. "Meta verwijdert Russische desinformatie over Oekraïne, gericht op Europa." *NOS.nl*. September 27, 2022. https://nos.nl/artikel/2446226-meta-verwijdert-russische-desinformatie-over-oekraine-gericht-op-europa.

O'Brien, A. "Open Source Intelligence May Be Changing Old-School War." *WIRED UK*, May 24, 2022. https://www.wired.co.uk/article/open-source-intelligence-war-russia-ukraine.

O'Brien, M., and Toubman, W. "Open Source Intelligence Combats Disinformation on Russia's War Against Ukraine." *PBS NewsHour*, April 13, 2022. https://www.pbs.org/newshour/show/open-source-intelligence-combats-disinformation-on-russias-war-against-ukraine.

Omand, D., Bartlett, J., and Miller, C. "Introducing Social Media Intelligence (SOCMINT)." *Intelligence and National Security* 27, no. 6 (2022): 801–823. https://doi.org/10.1080/02684527.2012.716965.

Oremus, W. "Social Media Wasn't Ready for This War: It Needs a Plan for the Next One." *The Washington Post*, March 25, 2022. https://www.washingtonpost.com/technology/2022/03/25/social-media-ukraine-rules-war-policy/.

Oxendine, C. "Open-Source Data Documents War Atrocities in Ukraine." *Esri*, June 14, 2022. https://www.esri.com/about/newsroom/blog/ukraine-open-source-intelligence/.

Perrigo, B. "How Open Source Intelligence Became the World's Window Into the Ukraine Invasion." *Time*, February 24, 2022. https://time.com/6150884/ukraine-russia-attack-open-source-intelligence/.

Puiu, T. "How Open-Source Intelligence (OSINT) Is Exposing the Ukraine War in Real-time." *ZME Science*, March 15, 2022. https://www.zmescience.com/science/news-science/open-source-intelligence-ukraine/.

Rietjens, S.J.H. "The Future of NLDISS." *Militaire Spectator* 191, No. 9 (2022): 12-23.

Romansky, S., Boswinkel, L., and Rademaker, M. *The Parallel Front: An Analysis of the Military Use of Information in the First Seven Months of the War in Ukraine*. The Hague: The Hague Centre for Strategic Studies, 2022. https://hcss.nl/report/the-parallel-front-military-use-information-ukraine/.

Sabbagh, D. "Researchers Gather Evidence of Possible Russian War Crimes in Ukraine." *The Guardian*, March 2, 2022. https://www.theguardian.com/world/2022/mar/02/researchers-gather-evidence-of-possible-russian-war-crimes-in-ukraine.

Salerno-Garthwaite, A. "OSINT in Ukraine: Civilians in the Kill Chain and Information Space." *Global Defence Technology*, 2022. https://defence.nridigital.com/global_defence_technology_oct22/osint_in_ukraine.

Sardarizadeh, S. "Ukraine War: False TikTok Videos Draw Millions of Views." *BBC News*, April 25, 2022. https://www.bbc.com/news/60867414.

Schwartz, L. "As Grisly Images Spread from Ukraine, Open-Source Researchers Ask What's Too Gory to Share." *Rest of World*, May 2, 2022. https://restofworld.org/2022/osint-gore-ukraine/.

Silverman, C., and Kao, J. "In the Ukraine Conflict, Fake Fact-Checks Are Being Used to Spread Disinformation." *ProPublica*, March 8, 2022. https://www.propublica.org/article/in-the-ukraine-conflict-fake-fact-checks-are-being-used-to-spread-disinformation.

Simonite, T. "The Race to Archive Social Posts That May Prove Russian War Crimes." *WIRED*, April 11, 2022. https://www.wired.com/story/open-source-russia-war-crimes-ukraine/.

Smith-Boyle, V. "How OSINT Has Shaped the War in Ukraine." *American Security Project*, June 22, 2022. https://www.americansecurityproject.org/osint-in-ukraine/.

Strick, B., [Bendobrown]. "*Eyes on Russia – Mapping Russia's War on Ukraine #russiaukrainewar*." Posted December 8, 2022, Video, 14:15. YouTube. https://www.youtube.com/watch?v=xaXz-EwU0WOs.

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

Tett, G. Inside Ukraine's Open-Source War. *Financial Times*, July 22, 2022. https://www.ft.com/content/297d3300-1a65-4793-982b-1ba2372241a3.

The Guardian. "Ukrainian Bloggers Use Social Media to Track Russian Soldiers Fighting in East." *The Guardian*, June 3, 2015. https://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine.

The Week. "What Is Open-Source Intelligence – And How Is It Helping to Map the Ukraine War?" *The Week UK*, March 10, 2022. https://www.theweek.co.uk/news/technology/956029/what-is-open-source-intelligence-ukraine-war.

Varzhanskyi, I. "Reflexive Control as a Risk Factor for Using OSINT: Insights from the Russia–Ukraine Conflict." *International Journal of Intelligence and Counterintelligence* (2023): 1–31. https://doi.org/10.1080/08850607.2023.2228489

Verma, P. "The Rise of the Twitter Spies." *The Washington Post*, March 23, 2022. https://www.washingtonpost.com/technology/2022/03/23/twitter-open-source-intelligence- ukraine/.

Vick, K. "Bellingcat's Eliot Higgins Explains Why Ukraine Is Winning the Information War." *Time*, March 9, 2022. https://time.com/6155869/bellingcat-eliot-higgins-ukraine-open-source-intelligence/.

Visontay, E., Bartholomew, J., Siddique, H., and Lock, S. "Satellite Images Show New Deployments of Russian Troops – As It Happened." *The Guardian*, February 21, 2022. https://www.theguardian.com/world/live/2022/feb/20/ukraine-crisis-russia-plans-biggest-war-since-1945-says-johnson-zelenskiy-calls-for-sanctions-now-live

Woodruff Swan, B., and McLeary, P. "Satellite Images Show New Russian Military Buildup Near Ukraine." *Politico*, November 1, 2021. https://www.politico.com/news/2021/11/01/satellite-russia-ukraine-military-518337.

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-NC-ND

https://doi.org/10.24415/9789400604742 https://www.inlibra.com/de/page/agb - Open Access - BY-NC-ND