HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 3. szám 43–53.
DOI: 10.32567/hm.2026.3.3

Ferenc Nyizsnyik[1]

Crowdsourcing Intelligence

Abstract

The widespread nature of privately owned smart equipment, such as cellphones, tablets and computers enables the general public to record virtually any event all over the world. These tools are able to provide text, image or video along with accurate time and location data. They can be considered sensors, and the owners can contribute valuable data on events happening in their vicinity. Several countries, most notably Ukraine is already exploiting this potential. According to the popular term of outsourcing a task for the public, it is called crowdsourcing. Crowdsourcing information gathering is an effective supplement to traditional intelligence methods. It is low cost and widely available, providing a large amount of information. This information must be processed and analysed, which is a time-consuming task. Artificial intelligence can help, but it must be used with caution.

Keywords: crowdsourcing, intelligence, CITINT, information, analysis

Introduction

In traditional warfare, intelligence is a key element of the decision-making process. Knowing the situation and activity of the opposing forces is vital information for the commander and mission planners to develop feasible missions. Traditionally, collecting this type of information is a job for the reconnaissance troops. More recently, as advanced sensors appeared on the battlefield, it is done by the Intelligence, Surveillance and Reconnaissance units, widely known as ISR.

The widespread nature of Internet-enabled devices paved the way for yet another possibility of information gathering: people connected to the Internet can contribute based on their skills and opportunities. This distributed work is called crowdsourcing.[2]

The aim of this paper is to get an insight on the potential incorporation of crowdsourced information into the intelligence gathering process and use the obtained information to support military decision-making. Based on the capabilities of the

[1] PhD student, Ludovika University of Public Service, e-mail: nyizsnyik.ferenc@stud.uni-nke.hu
[2] Dobák 2025.

sensors, the information provided meets the criteria for timeliness, accuracy and completeness; however, the employment of these sensors is completely based on the owners' discretion and cannot be tasked as a traditional sensor can.

Based on the sheer number of available sensors, crowdsourcing intelligence seems to be a viable tool for gathering information and assisting the decision-making process. Among others, this paper investigates the advantages and disadvantages of this method, based on researching the available literature and already existing solutions.

Collaborating citizens usually provide information on events they deem important. These events are usually, but not necessarily valuable for the intelligence community and the decision-makers. Information can be abundant in some cases, and at some point, the selection and categorisation of all the reports can be time-consuming. Artificial intelligence (AI) is a possible tool to accelerate this process. However, artificial intelligence has its own limitations at the time of writing this paper. These limitations need to be taken into consideration when employing AI in decision-making.

Theoretical overview

A definition of journalism crowdsourcing can be found in the book authored by Onuoha et al. in 2015 entitled: *Guide to Crowdsourcing*. Although this is about journalism, the definition fits quite well for intelligence collection activities.

"Journalism crowdsourcing is the act of specifically inviting a group of people to participate in a reporting task – such as newsgathering, data collection, or analysis – through a targeted, open call for input; personal experiences; documents; or other contributions."[3]

The Ministry of Digital Transformation of Ukraine issued an application (DIIA[4]) to manage their documentation, pay taxes and interact with public services.[5] "This app was later repurposed to allow Ukrainian citizens to provide real-rime reporting of Russian military troop dispositions, movements, strengths and equipment."[6]

Although reports by citizens include high-resolution photo or video footage complete with timestamps and geo-reference data, these reports still need to be verified by a trained intelligence specialist. This work is still overwhelming for humans, given the huge amount of raw data coming in. However, verification can be crowdsourced again: multiple reports from different citizens may confirm the event. The same process can be used to do Battle Damage Assessment (BDA), confirming the effectiveness of the strike.[7]

Stottlemyre (2015) further defines the nature of crowdsourced intelligence, and a simple way to tell it apart from OSINT[8] and HUMINT.[9] OSINT collectors acquire

[3] Onuoha et al. 2015: 4.
[4] Держава і Я [The State and I].
[5] Digital Citizen [DÁP, Digitális Állampolgár] is a Hungarian website that implements the same functionality (https://dap.gov.hu/).
[6] Burke 2022: 96.
[7] Burke 2022.
[8] Open Source Intelligence.
[9] Human Intelligence.

information "second hand", as the information was not originally provided to support national security objectives. HUMINT collection involves eliciting information by issuing intelligence questions to the collector. Crowdsourced intelligence requires open calls to enlist the community's assistance.

Stottlemyre (2015) also states three requirements that make crowdsourcing intelligence possible: first, an organisation that wishes to solve a problem. Second, that the organisation solicit the participation of a large, likely online, community to solve the problem. And finally, it is required that individual members of the at-large community choose to participate.[10]

The first requirement can be considered fulfilled; the armed forces is an organisation with constant need for information. The second requirement – when applied to dedicated sensors – is equivalent to tasking. In case of the third one, further investigation is necessary, and it always depends on multiple factors of the theatre and the operation.

Intelligence sensors

From the aspect of this paper, sensors can be classified into three main categories: dedicated sensors, operated by specialised units, sensors carried by the soldiers and crowdsourced sensors. All of the above types have their own advantages and disadvantages, complementing each others' functionality.

In case of dedicated sensors and soldier-mounted equipment, tasking is part of the process and willingness to participate is taken for granted. In case of the civilian population, however, cooperation depends on a variety of circumstances, mainly on how the population perceives the military. Even if the perception is positive, a level of trust is also needed, given the high risk of cooperation.

Dedicated sensors

Traditionally, sensors are dedicated platforms of information gathering with specific abilities, such as detection of electro-optical or electromagnetic signals. These platforms are often very expensive and therefore limited in number. They are critical assets, and as such, high value targets of the opposing forces. Their employment must be coordinated and deconflicted in order to avoid targeting the same area, wasting precious sensor time.

According to the Military Decision-Making Process (MDMP), decision points are points in space and time when the commander or staff anticipates making a key decision concerning a specific course of action. These decision points are often associated with a named area of interest (NAI).[11]

[10] Stottlemyre 2015.
[11] Center for Army Lessons Learned 2015.

As NAIs indicate the occurrence of one course of action or the other, they are often observed thoroughly, using dedicated intelligence platforms. This means that these areas are under observation even when no significant event is happening, and also that due to the scarcity of dedicated platforms, key events may happen unnoticed elsewhere and remain unknown to own forces.

Another disadvantage of these platforms is the limited range. More often than not, these are operated from far behind the front line of own troops in order to protect the high value assets. Therefore, they are unable to take advantage of their full range and can only provide information on a certain depth of the area of interest.

Networked soldiers

Modern technology enables manufacturing communication equipment and sensors in portable sizes. Networked soldiers are equipped with these kind of tools, and are integrated into a digital battlefield. They are not only able to discover the opposing forces from a greater distance than before, but are also able to transfer this information to the command post in real time.[12] The advantages are twofold: situational awareness is maintained at the headquarters at all times, providing vital information to the decision-making process, and virtually all the operational area is covered, since soldiers are present throughout.

Although this seems to be a straightforward method of information gathering, there are several disadvantages. The sensors must be small and light in order to allow soldiers to move and fight undisturbed, but it also decreases the capability and range of the sensors. They also must be autonomous, because operating them may distract the soldier, and in a battle situation the consequences of a distraction may be grave.

Crowdsourced intelligence

There are also very capable sensors and communication devices in the hands of most citizens: cell phones, tablets and other smart devices. These, in the hands of collaborating individuals, can be turned into very powerful intelligence platforms able to provide immediate, accurate and original information. This is crowdsourced intelligence gathering.

A recent example is the e-enemy (eVorog) Telegram chatbot, operated by the Ministry of Digital Transformation of Ukraine.[13] This platform enables any Ukrainian citizen to report on Russian military activities. This way information is obtained from all over the theatre, even if it is controlled by the opposing forces, or even from the rear area of the belligerent country.

Dobák (2025) and Burke (2022) investigated the e-enemy chatbot, so their findings are applicable to the Russo–Ukrainian conflict. Application of a similar

[12] Kollár 2017.
[13] Dobák 2025; Burke 2022.

method in different conflicts may show different outcomes. The key is the population's willingness to cooperate with the military. This depends on a variety of factors, and must be taken into consideration not only for the possibility of crowdsourcing, but for the success of the whole operation. A force entering a hostile environment must be entirely self-sustaining. Members of neutral population may be recruited as contractors, mostly in the field of logistics. In order to fully exploit crowdsourcing, a friendly and supportive community is necessary.

There are, however, several disadvantages of this method. First, the background knowledge of the reporters are very diverse. They may misinterpret events or misjudge actions. They may also misrecognise military equipment. It is also possible that they deliberately provide misleading information. This information is therefore not suitable for immediate processing, thorough validation is necessary. As this method is public, the infrastructure and the participants will be targeted by the enemy in many different ways. This activity is called CITINT, i.e. the intelligence activities conducted by citizens and NGOs.[14]

As it was mentioned before, in order to effectively exploit this method, the community must willingly participate. In case of the Russo–Ukrainian conflict, citizens take a chance to actively counter the occupying forces, so their willingness is evident. Expeditionary forces, however, are already in a disadvantageous situation. The local population is indifferent at best; they may as well consider the troops an occupying force. In this case, crowdsourcing works against the organisation.

To turn the tables, the population has to be convinced to cooperate. There are several methods for doing that, for example, psychological operations, but the success is never guaranteed. These activities are out of the scope of this paper.

The properties of the different sensor types are summarised in Table 1. The table shows that every sensor type has its own field of advantage. Dedicated sensors can be used in multiple intelligence disciplines; however, they are limited in numbers, therefore not able to monitor every possibly important event. Networked soldiers and community contributors can only provide information in the IMINT[15] discipline, but they are present in the battlefield and the rear area of the hostile country, respectively. This supports the theory that they augment each other in the information gathering process and employing all three grants leaders the ability to be aware of as many important events as possible.

Table 1: Properties of different sensor types

	Dedicated sensors	**Networked soldiers**	**Community contributions**
Multiple intelligence disciplines	Yes	No	No
Availability in the decisive locations for planning	Limited	No	Yes
Availability in the decisive locations for engagement control	Limited	Yes	No

Source: compiled by the author

[14] Pietilä et al. 2024.
[15] Imagery Intelligence.

Verification of crowdsourced information

The information gathered must be verified for credibility and genuineness. Comparing the report to the actual ground truth is a complex task. It can be done by cross-cueing using different types of sensors. Based on the presence of sensors throughout the battlefield and the rear area, significant events are likely to be reported either by own forces or citizens. These reports can be considered heads-ups and dedicated sensors may be tasked to monitor the situation.

Identifying the source is a good general method for filtering unusable noise or intentional misinformation out. When using crowdsourced information, extra attention is needed in order to determine the average attitude of the population in the theatre, and also the possible presence of malevolent actors. The general public, given enough congruent reports, can self-confirm any information.

Identification

Sensors must be identified in order to prevent injection of false information. In case of dedicated intelligence platforms and soldier-mounted equipment this is already handled by design. In case of citizens, identification may vary on a wide range of possibilities. The simplest way is registering with an e-mail address, which can be created in a matter of minutes, like in the case of OpenStreetMap.[16] Other applications, like the Viber instant messaging service, require a working phone with an active phone number.[17]

Reporting on enemy troops is subject to cyberattacks. The DIIA system was almost immediately targeted by Russian spambots after the ability to report on enemy movements had been added to it. In response, reporting required logging in using valid Ukrainian identity credentials.[18] This measure successfully addressed the spam issue, but identification allowed reports to be connected with the reporters. Should the enemy acquire this information, it can lead to severe retaliation, therefore protection of this database is essential.

Verification of genuineness

The amount of reports coming in from citizens makes it overwhelming for intelligence analysts to process and exploit the information in a timely manner, especially in case of a highly dynamic battlefield. Spam messages can be avoided if strict login is required, but the remaining reports still need to be verified.[19] Mass confirmation is one of the

[16] The sign-up process for contribution to OpenStreetMap requires only a valid e-mail address, a display name and a password (www.openstreetmap.org/user/new).
[17] Viber Terms of Service (www.viber.com/en/terms/viber-terms-use/#account-and-registration).
[18] Burke 2022.
[19] Burke 2022.

possibilities to verify the existence of the reported activity, but it depends on citizens present in the area. In the vicinity of military movements this may not be enough.

As mentioned earlier, dedicated intelligence platforms are traditionally observing named areas of interest. Due to the limited availability of these sensors, key events may go unnoticed while nothing happens in the designated NAI. A feasible option to increase the efficiency of these platforms is using them to verify citizen-reported information. This would allow mission planners to further accelerate the planning process, giving serious advantage over the opposing forces.

On tactical level, this information can be confirmed by drones, if available at the unit. It can provide targeting information to artillery or other fire units, or it can carry out the strike itself.[20] The aim of the information gathering on the operations level may not be direct targeting, but likely confirmation of one of the enemy courses of action.

Threats to crowdsourced intelligence

Credible and genuine information is necessary for the right decision to be made. Information warfare tactics will be employed by the opposing forces to disrupt the decision-making capability of friendly leadership. Even in case of a cooperative population in the area, threats to the information gathering process may arise.

As all intelligence platforms are high value targets to opposing forces, citizens providing reports are no exception. The reporters themselves and the platform providing the functionality are both vulnerable. Citizens contributing information on enemy activity are risking their freedom or even their life.

The information flow can be disrupted using electromagnetic warfare or cyber-attacks. A malicious reporter may provide false information, confusing the targeting and the mission planning process. A legit reporter may also provide false information due to insufficient knowledge and expertise.

Electromagnetic warfare

Citizens are using their own devices, such as cell phones, tablets or personal computers. They usually access the Internet through their Internet Service Provider (ISP) using mobile Internet or Wi-Fi. These services operate on well specified frequencies, so they are easy targets for electromagnetic jamming.

Global positioning systems can also be targeted by jamming or spoofing, providing false location data to the report. One example of GPS-jamming equipment is the Zhitel (RH–330 Zh).[21] The geotags of the information provided by a source suffering GPS-jamming are still valid, therefore it is very hard to filter out or correct these contributions. One clue may be the image not corresponding to the related coordinates.

[20] Burke 2022.
[21] Clark 2022.

This is a fatiguing and time-consuming work for humans; artificial intelligence may be able to spot and handle these anomalies.

The Starlink service provides Internet access for both Ukrainian troops and civilians. It has proven highly resistant to electromagnetic jamming,[22] even if the Krasukha–4 (1RL257) is able to jam low-Earth orbit satellites.[23] "Starlink has a constellation of thousands of satellites that orbit the planet […] at about 550 km, and cover the entire globe."[24] This redundancy makes the service accessible, even if some of its satellites are being jammed.

Cyberattacks

As it was mentioned, the DIIA service was subject to a high level of spam messages by Russian cyber warfare units. The requirement of logging in with valid Ukrainian credentials significantly reduced the amount of spam.

A malicious contributor may provide false information, of which the confirmation uses up valuable resources. In the worst case, the false information ends up being used in the military decision-making process, resulting in a wrong or suboptimal mission plan. This may have severe consequences regarding to the manpower and equipment of the friendly forces.

A contributor lacking the necessary knowledge, even with a good intent, may also provide false information. From the viewpoint of verification and mission planning, this information must be handled the same way. In both cases, identifying false information is very time-consuming for humans. These are usually single-source, unconfirmed reports, usually, but not necessarily contradicting confirmed information. AI may be able to filter these out, but it is up to the leadership to decide whether just drop it, possibly missing a significant event, or use another sensor to confirm, possibly wasting resources.

Processing and analysis

Until recently, intelligence communities were struggling to acquire enough information to support the requirements of the operations. After the exploitation of social media and crowdsourcing intelligence, information became abundant. The communities are now suffering from the overwhelming amount of data, and struggling to select, confirm and prioritise the information in a timely manner.

Tactical level command structures often lack the necessary personnel and equipment to process the large quantity of acquired information. In addition they are often operating from a makeshift command post, which is often relocated in order to avoid being localised and targeted by enemy fires. Also, units on this level focus on short

[22] Burke 2022.
[23] Clark 2022.
[24] Starlink 2026.

term goals, and may skip over details that otherwise could be used to predict larger scale courses of enemy actions.

Operational level structures are more adequate for this kind of work, as their staff includes a dedicated mission planner element and an intelligence section responsible for supporting the planners. However, the amount of information gathered by crowdsourced intelligence may overwhelm even this group of specialists, as they need to systematically review each piece of information and determine their relevance to the mission. This work is time consuming, and a delay in the decision-making is favourable for the opposing forces.

It is tempting to use the crowdsourcing model again – after all, it was invented for the distributed processing of large amount of data. However, the general public lacks the proper training that intelligence personnel go under in order to be able to fulfil their mission. They also lack the databases and historical data available for mission planners. Also, contributors usually work according to their own time schedule, and are not obligated to follow the battle rhythm of the armed forces. As a consequence, crowdsourced analysis can be considered unfeasible.

Using AI for analysis

Artificial intelligence (AI) has gone through a huge development in recent years. Properly trained models are capable of carrying out increasingly difficult tasks. The question naturally arises: Can AI be used for intelligence analysis?

As of the time of writing this paper, using AI is adequate for many different tasks. However, there are issues with AI: they may seem to be omniscient at first, but they cannot substitute human reasoning. They can be used to process large amount of data, but possible risks must be taken into account in order to operate them safely.

According to Probasco et al. (2025), the scope of the model must be thoroughly understood. A model providing excellent results in its own scope may fail when used outside of this scope. Nevertheless, AI will state the results very confidently, even if they are wrong. Humans tend to be biased toward these results, as computers are considered authentic sources. Confirmation bias is also important to be aware of, as humans tend to believe information supporting their own opinions.

AI can be of great help in categorising and organising large amount of data. However, at the time of writing this paper, they should not be used for the automation of decision-making. Critical thinking is required in the process, and AI lacks critical thinking. Human supervision is therefore essential when AI is involved in the decision-making process.[25]

[25] Probasco et al. 2025.

Dissemination

Every soldier at every level needs to be aware of the surrounding situation. One of the aims of intelligence gathering is providing this situation awareness (SA) for all friendly forces. Carrying out missions is only possible if the units involved are in the possession of this SA.

Situation in military operations are dynamic in nature, both in time and space. The most straightforward way to depict and disseminate dynamic information is using a geographic information system (GIS). A GIS can display the situation in real time for everyone with appropriate equipment. This information, should fall in enemy hands, will cause significant disadvantage for own forces. This system therefore must be considered a high value asset, and must be protected accordingly.

In this paper, the focus is not on the dissemination of SA. This topic has been discussed extensively and the problem is addressed in different ways. The methods of dissemination are outside of the scope of this paper, the focus is on information gathering.

Conclusion

Crowdsourcing intelligence is a proven method for information gathering. It is considered to be a new discipline of intelligence by some: CITINT.[26] It requires little financial investment as the necessary equipment is owned by the contributors. Contributors – given their willingness to cooperate – are present and provide information virtually everywhere, resulting in a multitude of sensors available for the intelligence community.

As a result, traditional sensors can be used for confirmation of events instead of wasting these platforms for continuous observation of NAIs. The sensors becoming available can be retasked for time sensitive operations.

Every intelligence system is a high value target of the opposing forces, crowdsourced intelligence being no exception. The bottleneck of the system is the underlying communication and information infrastructure, so most likely this will be targeted by different ways in order to suppress or destroy this gathering method.

Processing the overwhelming amount of data requires time. Intelligence specialists are under constant time pressure to provide timely support for mission planning. This contradiction can be resolved by utilising artificial intelligence. However, AI has its own drawbacks, so human supervision cannot be avoided.

This paper investigated the feasibility of crowdsourced intelligence among traditional methods and the inclusion of the information obtained this way into the military decision-making process. The final finding is that crowdsourced intelligence is a valuable asset in the hands of modern armed forces. It can be considered a relatively low-cost force multiplier, and employed together with traditional sensors and networked soldiers greatly enhances the decision-makers' situation awareness.

[26] Pietilä et al. 2024.

References

Burke, Paul (2022): The Issues in the Collection, Verification and Actionability of Citizen-Derived and Crowdsourced Intelligence during the Russian Invasion of Ukraine, 2022. *Strategic Panorama,* (Special Issue), 94–103. Online: https://doi.org/10.53679/2616-9460.specialissue.2022.09

Center for Army Lessons Learned (2015): *MDMP Handbook.* Center for Army Lessons Learned. Online: https://apps.dtic.mil/sti/pdfs/AD1018227.pdf

Clark, Bryan (2022): The Fall and Rise of Russian Electronic Warfare: The Ukraine Invasion Has Become an Old-fashioned Slog, Enabling Russia to Unleash Its Electronic Weapons. *IEEE Spectrum,* 30 July 2022. Online: https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

Dobák, Imre (2025): Crowdsourcing for Security in the Age of Hybrid Threats. *Security and Defence Quarterly,* 49(1), 98–111. Online: https://doi.org/10.35467/sdq/197309

Kollár, Csaba (2017): Az IoT katonai felhasználási lehetőségei és a fejlesztés irányai. *Hadmérnök,* 12(4), 146–158. Online: http://hadmernok.hu/174_15_kollar.pdf

Onuoha, Mimi – Pinder, Jeanne – Schaffer, Jan (2015): *Guide to Crowdsourcing.* Columbia Journalism School. Online: https://data.journalism.columbia.edu/sites/data.journalism.columbia.edu/files/content/guide-to-crowdsourcing.pdf

Pietilä, Iikka – Kortesuo, Katleena – Pohjanen, Ulla – Tuominen, Mikko (2024): Shift in Intelligence Issue Ownership: Conceptualizing CITINT – Intelligence Conducted by Citizens. *Frontiers in Political Science,* 6. Online: https://doi.org/10.3389/fpos.2024.1379789

Probasco, Emelia – Toner, Helen – Burtell, Matthew – Rudner, Tim G. J. (2025): AI for Military Decision-Making. Harnessing the Advantages and Avoiding the Risks. *Center for Security and Emerging Technology,* April 2025. Online: https://doi.org/10.51593/20240028

Starlink (2026): *Satellite Technology.* Online: https://starlink.com/hu/technology

Stottlemyre, Steven A. (2015): HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence. *International Journal of Intelligence and Counterintelligence,* 28(3), 578–589. Online: https://doi.org/10.1080/08850607.2015.992760