SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Crowdsourcing for security in the age of hybrid threats

Imre Dobák

dobak.imre@uni-nke.hu

https://orcid.org/0000-0002-9632-2914

Institute of National Security, National University of Public Service, Ludovika tér, H-1083, Budapest, Hungary

Abstract

The study explores emerging forms of crowdsourcing solutions in cyberspace for security and national security purposes. It aims to systematise the main types of crowdsourcing solutions that involve civilian participation and contribute to the overall security of society in an increasingly broader context. The study begins with international examples of crowdsourcing, which can be visible in various areas of security. Identifying their specific features as they appear on open platforms helps to frame and examine the issue. Nowadays, the multitude of international security conflicts and processes indicate that the use of information and communications technology tools available at the individual level can effectively support the (national) security use of knowledge and expertise available in a distributed manner as a concentrated resource. The examples examined in this study indicate that the crowdsourcing approach can play a significant role in security and national security strategies across various areas. However, the adoption and effectiveness of crowdsourcing solutions in the voluntary contribution of individuals to security will undoubtedly be influenced by the nature of security events and the open involvement of members of society.

Keywords:

intelligence, hybrid, cyberspace, information society, national security

Article info
Received: 20 May 2024
Revised: 8 December 2024
Accepted: 12 December 2024
Available online: 31 January 2025

Citation: Dobák, I. (2025) 'Crowdsourcing for security in the age of hybrid threats', *Security and Defence Quarterly*, 49(1). doi: 10.35467/sdq/197309.

http://doi.org/10.35467/sdq/197309

Introduction

Crowdsourcing, conceptually, can be defined as a distributed work process in which tasks are outsourced to participants (the crowd) who contribute based on their skills or opportunities, collaboratively solving tasks to produce a common result. This model can be found across various domains, from economics and engineering to technology and the digital, data-driven fabric of modern society. The relevance of crowdsourcing extends to the security sector, which, in the 21st century's era of hybrid conflicts, is increasingly focused on maximising the potential of cyberspace; in particular, fields such as information warfare, which includes influencing members of society, deceiving adversaries through disinformation, and conducting cyberspace-related intelligence and information gathering. The phenomenon is now present on social platforms, widely used by society. On the one hand, they create an abundance of openly available information; on the other, they serve as platforms for deception and the dissemination of misinformation.

Crowdsourcing is used across a wide range of research areas and is evident in our everyday lives (Castillo, 2013; Gupta and Brooks, 2013, p. 27). Participants contribute their data, knowledge, or resources, such as financial support (e.g. crowdfunding), to the creation, improvement, or refinement of a collective "outcome." It is present in information and communications technology (ICT), including the crowdsourcing of the Internet of things (Anopa *et al.*, 2023) as well as in business and marketing. It is also increasingly significant in the social sciences, where it has driven specific directions of innovation, such as geo-crowdsourcing and crowdfunding (Brovelli *et al.*, 2019, pp. 838–863; Demiray *et al.*, 2019, pp. 115–151).

However, "crowdsourcing" as a model is not a phenomenon unique to the 21st century. From a scientific perspective, crowdsourcing refers to the outsourcing of parts of work processes and human resources in a distributed manner (Stottlemyre, 2015). It involves engaging crowds as distributed resources to perform various "subtasks," which today, thanks to online space and communities, has evolved into a powerful distributed problem-solving capability (Brabham, 2008, p. 76). The logical progression of this development is to obtain solutions or insights from actors in cyberspace who can provide relevant information, whether through professional expertise or their presence in specific contexts. The term "crowdsourcing" is often attributed to Jeff Howe (2006), who introduced it from a business perspective in a 2006 article. Today, however, distributed work based on cooperation is prevalent across various aspects of life, as numerous technological and infocommunication solutions are built upon shared resources. The rise of crowdsourcing has been propelled by the accessibility of infocommunication tools at the individual level, which has expanded the spatial boundaries of the information we can access and share. These tools essentially act as "sensors" of our daily lives.

The opinions and information shared on various social platforms can be particularly valuable in critical security situations, as they often provide more accurate and up-to-date information than traditional sources. However, beyond these ideal scenarios, questions may arise about the value and reliability of the information shared. What is undeniable is that during such periods (e.g. natural disasters or conflicts), there is an increased demand for accurate and credible information from both members of society and public organisations responsible for security. In this context, cyberspace-based crowdsourcing solutions can play a significant role in supporting the work of agencies responsible for ensuring security.

Based on examples from the international literature, the crowdsourcing approach to national security demonstrates the collective power of communities, whether in

information gathering, analysis, or forecasting. In this context, gaining a deeper understanding of the potential applications of the method and continuously seeking ways to further develop it for security purposes is essential. The aim of this paper is to contribute to the scientific discourse on applying crowdsourcing to (national) security by highlighting some of its main directions, as identified in the literature and current international examples. The paper categorises the topic into four key areas: information gathering, cybersecurity, expert analysis, and security foresight. It examines the specifics of these application directions as well as the advantages and limitations of the method.

Methods

A key element of this research is the concept of "collective intelligence", which refers to the shared abilities and knowledge of group members. A fundamental aspect of collective intelligence is the ability and willingness to cooperate, where participants work together towards a common goal and share tasks among themselves. This concept is demonstrated in numerous international examples, which serve as a basis for this study. As an inductive research method, this paper examines the topic by drawing on case studies from the literature and incorporating the findings of other authors in the context of security-related applications. While crowdsourcing is now highly diverse, much of it is not directly related to security. Therefore, during the literature review, document analysis, and selection of examples, a focus was placed on identifying examples that are central and illustrative for security-related applications (e.g. Papapesios *et al.*, 2019). The reviewed sources and examples provided the basis for identifying key characteristics and elements of crowdsourcing in security contexts as well as for outlining its main application directions. The choice of research method reflects the observation that crowdsourcing, as a theory, is often intertwined with security-related activities. This study seeks to explore how the method can be applied within the paradigm of security, rather than treating it as a distinct, clearly delineated category.

Due to a lack of available data, this study did not aim to explore the inner workings and characteristics of crowdsourcing systems. Instead, it aimed to identify specificities along the lines of the categorisation of security-related applications. At the same time, given the broad interpretability of security, it is not possible to draw sharp distinctions between the categories identified in the study. However, the examples examined provide valuable illustrations of how crowdsourcing is applied in these security-related contexts. It is hoped that identifying the main application categories and outlining the advantages and disadvantages of the method will be beneficial for those considering crowdsourcing solutions. Additionally, the study aims to offer ideas that could facilitate the further development and application of crowdsourcing in security-related fields.

This research aligns with the growing research direction in applying crowdsourcing methods to security contexts (Halder, 2014; Hui, 2015; Markowsky, 2013). The global information environment, characterised by the availability of vast amounts of data in various formats and platforms, opens new perspectives for security applications. For instance, during a security incident, the challenge of identifying and selecting relevant information of value becomes significant. This increases the importance of sources that can enable security organisations to act more accurately and quickly. From this perspective, crowdsourcing views crowd members as distributed resources whose significance lies in their skills or geographic location. In critical security incidents, identifying the fastest and most accurate source of information becomes crucial. On the one hand, individuals in the affected geographic area may possess relevant information, and available tools can

facilitate the transmission of that data. However, the accuracy and authenticity of the data cannot be guaranteed, whether due to accidental errors or intentional deception. Therefore, the advantages and disadvantages of crowdsourcing as a method must be considered carefully.

In this regard, as a methodological element, it is important to examine the distinct components of crowdsourcing (the crowd, the crowdsourcer, the crowd-sourced task, and the crowdsourcing platform; Hosseini *et al.*, 2014, pp. 1–12). Additionally, consideration must be given to both advantages and disadvantages of crowdsourcing, including data reliability, as well as the motivation and willingness of participants to participate.

Forms and characteristics of crowdsourcing for security purposes

The conflicts of recent years have increasingly valued crowdsourcing solutions for security purposes. This trend reveals an increasingly complex picture, encompassing areas such as intelligence, analysis, forecasting, cybersecurity, and cyberattacks. One key factor driving this development is the involvement of civil society actors in modern armed conflicts. In today's conflicts, alongside traditional military forces, civilian participants are also engaged—often through invisible networks—on both defending and attacking sides. These actors contribute to the events by providing information and support within cyberspace.

In a national security context, a key objective is to obtain the most accurate and up-to-date understanding of a given event. Achieving this requires human resources capable of contributing their skills, expertise, and information to piece together a more complete picture from mosaic-like elements.

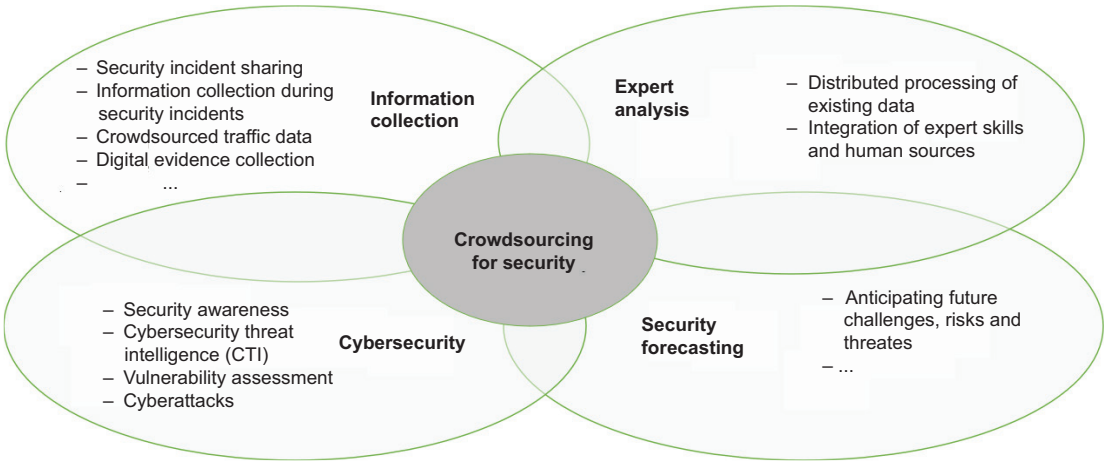
Aligned with these objectives, numerous international examples demonstrate the use of crowdsourcing for security and national security purposes. These efforts use the unique characteristics of the online space to their advantage, including:

- the actors of the information environment engaged in the given task (either information collection or analysis), which can be used to enhance capabilities;
- platforms can be developed to reduce the time required for obtaining or processing information;
- diverse types of information can be systematically and targetedly collected and processed, particularly in connection with security incidents where local human resources possess knowledge. In such cases, the involvement of members of society can significantly improve efficiency.

On the other side of the coin, crowdsourcing also presents challenges and disadvantages, making it unsuitable as a "one-size-fits-all" solution:

- Authenticity and accuracy of data provided by participants as well as the underlying motivations for their contributions.
- Risks of distortion, manipulation, or contamination of the process through data.

Figure 1. Possible main directions of crowdsourcing solutions for security purposes.



- Participant security during conflicts, as their openly shared data or mobile communication devices could be vulnerable to attack, especially due to their physical geo-location.

Based on the international examples reviewed, this study has grouped the main applications of crowdsourcing for security purposes into four clusters and seeks to highlight the relevance of the topic through their main characteristics (Figure 1). The clusters are not rigidly defined, and their boundaries often overlap.

Crowdsourcing for information collection (crowdsource intelligence)

Among the general types of crowdsourcing, the categories of "audience-centric, geocentric, event-centric, and global" crowdsourcing (Erickson, 2010) provide a useful framework for models applicable in today's online environment. The widespread adoption of online tools has significantly accelerated information transmission, which has created a shift in how human resources, ICT tools, and openly available information interact. Infocommunication tools now enable individuals not only to receive information but also to actively participate in shaping processes by contributing their data. By connecting their smartphones to online platforms and social media, people can participate in larger, coordinated efforts to collect and geo-reference data, improving the accuracy of assessments in specific situations, including security-related events (Papapesios *et al.*, 2019). In the national security context, crowdsourced intelligence aligns closely with concepts like Human Intelligence (HUMINT) and OpenSource Intelligence (OSINT) due to the prominence of human involvement and open information (Stottlemyre, 2015). However, the term OSINT may be misinterpreted in this context. Here, it refers to the potential openness of information contributed by the crowd, rather than the process itself. In many cases, the aggregated results of crowdsourcing are no longer openly accessible, such as in open source software development process (Brabham, 2008, p. 81).

The main purpose of the following examples is to demonstrate the types of information-gathering applications of crowdsourcing.

One significant application is during natural or humanitarian disasters and armed conflicts. Data collected by information providers in the affected area—despite the method's

limitations (e.g. inaccuracies or incorrect information)—can directly support coordination efforts, crisis management, and even disaster resilience (Moghadas *et al.*, 2023). The value of such information lies in its immediacy and its origin from the field, offering authorities a more accurate understanding of the size and nature of a security incident. However, in crisis situations, it is evident that reliance solely on this information is not feasible due to its inherent limitations. Factors such as intentional or unintentional deception, panic, misinterpreted knowledge, or inaccuracies arising from irresponsible behaviour linked to a sense of digital anonymity can all compromise the reliability of crowdsourced data.

These application possibilities have long been recognised by researchers and professionals in the field (Halder, 2014). Comprehensive solutions that use the capabilities of crowdsourcing communities include examples such as fire-signalling systems and the visualisation of data on maps. For example, Europol's Stop Child Abuse—Trace an Object (SCATO) is a platform which engages the public to help identify objects in images associated with child abuse cases (Ilbiz and Kaunert, 2023). Such applications support the work of law enforcement and government agencies by providing digital evidence and aiding in the subsequent investigation of incidents by authorities.

Engaging and involving members of society on online platforms during crimes and major security incidents (e.g. terrorist attacks or bombings) is not a new phenomenon. Publicly available information can aid in identifying perpetrators and detecting individual crimes or security-related cases. The relationship between social media and crowdsourcing has been investigated in several studies, with one of the best-known cases being the Boston Marathon bombing in 2013 (Nhan *et al.*, 2017, pp. 341–361; Tapia and LaLone, 2014, pp. 61–77). While crowdsourcing intelligence has clear advantages, the Boston Marathon case also highlighted its errors and contradictions when applied to security purposes. Following the bombings, groups formed on social networking sites to assist in identifying potential perpetrators (Markowsky, 2013, pp. 772–773). The "investigative community" created online provided valuable support to law enforcement and investigative authorities. However, these groups also demonstrated the risks of crowdsourcing, such as the reinforcement of false connections and the wrongful identification of innocent individuals as suspects (McCullagh, 2013). Despite the authorities' calls for voluntary societal cooperation to expand the evidence base, self-organised online groups were able to call innocent people as suspects. This also illustrated the limitations and potential failures of crowdsourcing when used for security purposes. A more recent example of crowdsourcing intelligence (CSI) occurred during the violent events at the United States Capitol in January 2021. Crowds helped law enforcement officers identify insurgents by analysing photos and videos posted on social media (Zegart, 2021).

The Russian-Ukrainian war provides examples of the wide-ranging security-related applications of crowdsourcing. From the outset of the war, Ukraine recognised the value of social media platforms and smartphone-generated information to track and report the activities of Russian forces. However, this example also highlights the disadvantages of crowdsourcing in security contexts, such as concerns about the safety of those sharing information, the potential inaccuracy of data, and deliberate disinformation efforts. Ukrainian security agencies quickly leveraged the crowdsourcing method. For instance, the Ukrainian Security Service created the STOP Russian War chatbot, which enabled citizens to report enemy movements and activities. The Diia (e-governance digital portal) initially played a key role in enhancing the credibility of information and the effectiveness of crowdsourcing efforts. However, the system later became a target for Russian spambots, which required the implementation of additional protective measures (Bergengruen, 2022; Burke, 2022, p. 96). These challenges (data poisoning, cyberattacks, and system overloads during critical periods) point at problematic aspects of crowdsourcing for security purposes.

Other notable Ukrainian initiatives include the Narodnii Mesnik platform, launched by the Ukrainian National Police to collect signals from the public, and the eVorog (e-enemy) Telegram chatbot, launched by the Ministry of Digital Transformation, to detect and monitor Russian military activities. Additionally, the online project Russia Will Pay aims to document and assess war damages (Russia Will Pay, 2024). Organised by the Kyiv School of Economics (KSE Institute), the Office of the President of Ukraine, and several ministries, the project's goal is to control, analyse, and estimate the material damage to Ukraine's infrastructure and provide detailed proof for accountability. According to the KSE Institute's website, the program guarantees the confidentiality of individuals who submit information.

A common feature of the above crowdsourcing solutions is their direct connection to security issues. These solutions rely on the participation of the civilian population, who provide relevant information (human resources), and on the technological environment, which is frequently linked to external infocommunications development efforts. Additionally, they often involve actors from the scientific community.

Crowdsourcing for cybersecurity

In this form, crowdsourcing models rely on the expertise, specific knowledge, and abilities of participants. Their applications in security-related contexts are highly diverse, ranging from the processing and evaluation of specialised data to addressing the rapidly evolving challenges in the field of cybersecurity.

In the field of cybersecurity, the crowdsourcing model is a well-established approach, particularly used by software development companies for activities, such as Crowdsourced Software Testing (CST) (Alyahya, 2020). One prominent application is in business-driven bug bounty programs, where ethical hacker communities (whether public or private) assist in testing software and enhancing information security by identifying vulnerabilities. The primary objective of such programs is to engage individuals with expertise in the field, such as ethical hackers, researchers, and developers, who can identify cybersecurity vulnerabilities either periodically during specific campaigns or on a continuous basis.

In this context, crowdsourcing can be employed by companies and organisations to gather and share information through platforms such as threat exchange systems, thereby contributing to the development of necessary countermeasures (Pawar, 2023). However, despite its advantages, these data-sharing solutions are often not viable due to the sensitivity of the data involved.

Examples of crowdsourced cybersecurity applications include citizen volunteering initiatives, which use the Internet to share information and fight cybercrime and cyber threats. One such example is the CyberPeace Corps (Kumar, 2022). However, crowdsourced methods can also be observed from the perspective of attackers.

In contemporary armed conflicts, such as the Russian-Ukrainian war and the Israel-Hamas war, groups have emerged on both sides to attack their adversaries' systems in cyberspace. These groups often employ crowdsourced Distributed Denial of Service (DDoS) attack methods. Osta's study (2024) provides a detailed account of these activities, describing the actions of entities like the IT Army of Ukraine, NoName057(16), and the Cyber Army of Palestine. The study examines the crowdsourced DDoS attack methods they use and the traceability of their effects for anonymised participants. The study also highlights

that organised solutions for disrupting systems and services in cyberspace are now readily available as open-source tools, the real catalyst of which is the "crowd" that uses them.

The specificity of this category lies in the distributed expertise and the associated involvement of human resources, often complemented by additional motivating factors, such as financial incentives, beyond mere volunteering. However, the level of expertise required for participation can be reduced through supportive interfaces (e.g. for cyber-attacks or analysis), which can facilitate the involvement of a broader range of participants.

Crowdsourcing for expert analysis

The use of crowdsourcing for expert purposes is also evident in the field of security. One notable example is the case of Malaysia Airlines flight MH370, which disappeared in 2014 during its journey from Kuala Lumpur to Beijing. Millions of participants joined the platform Tomnod to review over 1 million square kilometres of high-resolution satellite images in the search for clues. Another example comes from Germany's Every Name Counts project, based on the Arolsen Archives. Citizens contributed to the expert processing of digitised records related to the victims of Nazi persecution by indexing them into a searchable database. As a result of social media engagement, 7,000 volunteers joined the project in 2020 (Ghert-Zand, 2020). A further example is the Texas Virtual Border Watch program, a government-led web-based monitoring solution developed by the US law enforcement agencies. This initiative allows citizens to participate in monitoring the US–Mexico border, aiding efforts to combat illegal activities, smuggling, and unauthorised immigration (Tewksbury, 2012, p. 250).

As in the preceding category, the crowd's skills are used, but the distinction lies in participants being tasked with analysing already available information. The rationale for using this model stems from two key factors: the substantial volume of data that needs to be processed and the necessity to accomplish this within a constrained timeframe. Meanwhile, the range of applications for this method continues to expand. For instance, recent research (Jia *et al.*, 2024) examines the role of collaborative groups in identifying online misinformation through the "wisdom of crowds," where the aggregate opinion of the group proves more accurate than that of individuals (Simoiu *et al.*, 2019).

Crowdsourcing for security forecast purposes (crowdsourced forecasting or CSF)

The "ability to predict" is an important focus in defence and security planning that can be enhanced through the use of large datasets or by using the knowledge and skills of individuals and organisations. Crowdsourced forecasting is gaining importance as a method for anticipating future events by aggregating the opinions and expertise of the crowd, such as in technology assessments. Scientific research on CSF for national security purposes seeks to support policy-making by predicting future challenges and risks. While open solutions are commonly applied to security issues, the literature suggests that national security forecasting research increasingly leans towards closed, internal systems (Samotin *et al.*, 2023). However, the true power of crowdsourcing lies in its capacity to engage the widest possible range of participants who can make meaningful contributions to the success of a programme. In many cases, this potential justifies extending the reach of such programmes and opening them up to other contributors.

A study examining the relationship between the US Intelligence Community (IC) and crowdsourcing (Samotin *et al.*, 2023) highlights the development of two significant

crowdsourcing platforms over the past decade: the Intelligence Community Prediction Market (ICPM) and the Aggregative Contingents Estimation Program (ACE). These platforms have demonstrated the potential to provide effective forecasting solutions. However, as the study explains, despite their promise, the two programs have not had a substantial impact on the US intelligence reporting. To address this, the research explores several possible reasons for their limited influence. According to the study, the Intelligence Advanced Research Projects Activity (IARPA) launched the US Intelligence Community's classified network prediction market, which has been cited in another study (Stastny and Lehner, 2018) as being "more accurate than predictions made in traditional intelligence reports" (Samotin *et al.*, 2023, p. 558).

The George Mason University SciCast project, funded by IARPA and launched a decade ago, serves as another example of research into the potential for predicting security threats. According to SciCast, 2024, the funding for this research has ended, and the website is currently inactive. The project aimed to explore the use of group-level collective wisdom to predict future events related to national security. As explained in an article by Tucker (2014), participants in the project used their expertise and knowledge to bet on the likelihood of future events.

Other programs fall into this category, such as the US Integrated Forecasting and Estimates of Risk (INFER) program, which enhances government forecasting capabilities by using crowdsourced sources to predict future scientific, technological, and national security trends and processes. Since 2023, INFER has collaborated with the Cosmic Bazaar program, led by the UK's Professional Head of Intelligence Assessment (Siegel, 2023).

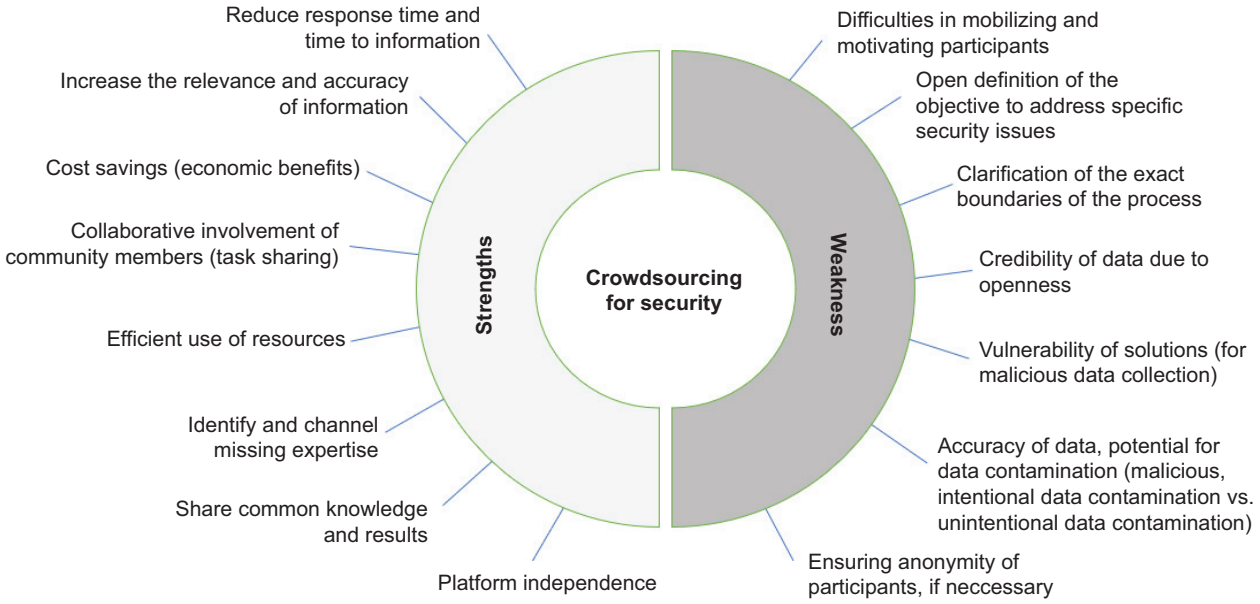
The specificity of this category lies in the fact that it does not rely on existing data or information as a starting point. Instead, it is based on the crowd's intuitions, opinions, and predictions about future developments. In this context, inaccuracies in the input provided by participants cannot be classified as data pollution.

Results

The examined examples suggest that the crowdsourcing approach has potential applications in various aspects of security and national security thinking. However, both limitations and advantages of the method must be considered (see Figure 2). While national security thinking is often "closed" in many areas, critical events, such as terrorist attacks or open military conflicts, create a need for information flows that extend to society. These information needs are particularly apparent in the areas where communication and collaboration with broader social groups can support security interests. Examples include assistance during natural and man-made disasters, law enforcement efforts, or the dissemination of accurate information during armed conflicts (Moghadas *et al.*, 2023; Papapesios *et al.*, 2019).

Regarding the advantages of the crowdsourcing method, several general benefits can be identified. These include a reduction in reaction time, an increase in the volume of information (and the anticipated accuracy), and economic, social, and human advantages. Other authors highlight the power of the crowd, emphasising the utilisation of human resources and expertise, the potential for discreet work, cost savings, and even fostering innovation (Hui, 2015, p. 5). However, crowdsourcing is not a universal solution for addressing security issues. Applications for security purposes raise specific questions, such as whether participant anonymity is necessary or how to ensure data authenticity and accuracy (Ilbiz and Kaunert, 2023). By definition, it depends on the purpose of the

Figure 2. Limitations and benefits of crowdsourcing solutions for security.



crowdsourcing application, whether it is necessary to ensure the anonymity of the individual contributing by solving partial tasks and providing partial information as part of the "anonymous" crowd. In one case, for example, we can think of using a route planner, where we contribute with our efforts to determine the amount of traffic, while in another case we want to contribute to increasing security by handing over digital evidence ("anonymous reporting").

Another critical aspect is that many security-related applications are connected to public organisations and tasks, which often raises concerns about personal data protection and privacy. These issues can significantly influence public motivation and willingness to participate (Kumar and Faisal, 2024). For example, the COVID-tracking applications faced resistance due to fears about potential privacy violations, which acted as a restraining force (Németh and Magyar, 2021). Similarly, the open use of social media platforms for security purposes, as seen during the Russian-Ukrainian war, has highlighted similar concerns regarding data privacy and user anonymity.

Social platforms offer a viable medium for expanding crowdsourcing initiatives. However, in security-related topics, it is crucial to ensure both authenticity of the information and safety (including anonymity) of the participants. Due to their openness, such platforms are particularly vulnerable to influence, manipulation, and the dissemination of disinformation, which can undermine the authenticity of "community" knowledge. Community-sourced data also raises concerns about accuracy and credibility. While inaccuracies may result from innocent errors, they can also stem from deliberate actions, such as intentional deception.

The phenomenon of data poisoning, where malicious participants deliberately contaminate data collection with misleading information, poses a significant challenge, particularly in security applications. This contamination can negatively impact the accuracy of aggregated results, potentially leading to erroneous conclusions and decisions (Tahmasebian *et al.*, 2020). In security-related contexts, where the data collected may directly influence societal safety, the intentional manipulation of information is especially concerning. Such malicious and intentional actions can lead to erroneous conclusions and decisions and can undermine trust in these applications. In today's world, where data analysis and evaluation

are increasingly reliant on artificial intelligence solutions, the importance of "authentic" data is crucial, as inaccurate data can distort the entire analysis process.

As a potential solution, double-checking smaller and refined datasets that emerge as valuable during the crowdsourcing process (e.g. through expert validation) can help mitigate inaccuracies. Additionally, leveraging the collective effect of mass confirmation (where multiple participants validate the same information) can neutralise the impact of inaccurate data. While this solution is more feasible in crowdsourcing intelligence applications, where data can be verified against existing facts or expert analysis, it presents a challenge in crowdsourcing forecasting. In forecasting scenarios, the accuracy of predictions can only be verified retrospectively after the predicted event has occurred.

Conclusions

Crowdsourcing has become an integral yet often invisible part of our daily lives. Its relevance to security has been amplified by several factors. First, the evolution of information technology (IT) tools and environments has expanded the potential for crowdsourcing applications. Second, security authorities have recognised the value of mobile communication tools, which are essential for individuals to share information globally. These tools can generate relevant security-related information, which makes them a valuable asset for public authorities. Mobile devices can serve as a vital data feed. However, when designing and implementing such targeted applications, there are also a number of other aspects to consider.

The study identified four areas of application (namely information collection, expert use, cybersecurity, and security forecasting) where the crowdsourcing model is already demonstrating practical relevance to national security. These areas provide valuable examples and insights that can help shape the future use of crowdsourcing and contribute to the broader discourse on the subject.

The common elements underlying these types of applications include:

- the necessity for involvement and voluntary participation,
- the motivated engagement of participants,
- the utilisation of cyberspace platforms, and
- the requirement for a central organising role.

However, alongside the advantages of the method outlined in the study, there are several limitations that must be acknowledged. These challenges may stem from the participants themselves (e.g. the need for anonymisation, the reliability and credibility of data contributors) or from the datasets generated through their participation (e.g. data accuracy, credibility, and the security of the systems). It is therefore essential for developers of crowdsourcing-based applications to be mindful of these constraints and to address them during the design process. Ensuring robust safeguards and mechanisms to mitigate these challenges is critical to the effective applicability of the method. Failure to do so could result in cumulative community knowledge producing erroneous results.

What can be expected of the future? The nature of future security incidents and the associated open involvement of societal actors will undoubtedly shape the evolution of

crowdsourcing security applications. The capacity to disseminate information through communication channels—whether in the context of ongoing conflicts, unforeseen natural or man-made disasters, or the complex domain of cybersecurity—will increasingly highlight the value of human involvement organised through crowdsourcing processes. Nevertheless, the role of civil society members as observers or external experts opens up numerous research avenues worthy of further exploration.

Funding

This research received no external funding.

Data Availability Statement

Not applicable.

Disclosure Statement

No potential conflict of interest was reported by the author. The author read and agreed to the published version of the manuscript.

References

Alyahya, S. (2020) 'Crowdsourced software testing: A systematic literature review', *Information and Software Technology*, 127, p. 106363. doi: 10.1016/j.infsof.2020.106363.

Anopa, S., Salim, A. and Pankaj, D.S. (2023) 'Crowdsourcing of Internet of things: Applications, trends in technology and the future', in Conference Proceedings: *2023 International conference on power, instrumentation, control and computing (PICC)*, IEEE, Thrissur, India, pp. 1–6. doi: 10.1109/PICC57976.2023.10142617.

Bergengruen, V. (2022) *How Ukraine is crowdsourcing digital evidence of war crimes*, 18 April. Available at: https://time.com/6166781/ukraine-crowdsourcing-war-crimes/ (Accessed: 10 May 2024).

Brabham, D.C. (2008) 'Crowdsourcing as a model for problem solving: An introduction and cases', *Convergence*, *14*(1), pp. 75–90. doi: 10.1177/1354856507084420.

Brovelli, M.A., Delipetrev, B. and Zamboni, G. (2019) 'Free and open source tools for volunteer geographic information and geo-crowdsourcing', in Information Resources Management Association (ed.) *Crowdsourcing: Concepts, methodologies, tools, and applications*. Hershey, PA: IGI Global, pp. 838–863. doi: 10.4018/978-1-5225-8362-2.ch041.

Burke, P. (2022) 'The issues in the collection, verification and actionability of citizen-derived and crowdsourced intelligence during the Russian invasion of Ukraine', *Strategic Panorama*, Special Issue, pp. 94–103. doi: 10.53679/2616-9460.specialissue.2022.09.

Castillo, M. (2013) 'The wisdom of crowds', *American Journal of Neuroradiology,* 34(10), pp. 1863–1865. doi: 10.3174/ajnr.A3417.

Demiray, M., Burnaz, S., and Aslanbay, Y. (2019) 'The crowdfunding market, models, platforms, and projects', in Information Resources Management Association (ed.) *Crowdsourcing: Concepts, methodologies, tools, and applications*. Hershey, PA: IGI Global, pp. 115–151. doi: 10.4018/978-1-5225-8362-2.ch007.

Erickson, T. (2010) 'Geocentric crowdsourcing and smarter cities: Enabling urban intelligence in cities and regions', position paper presented at the *1st Ubiquitous Crowdsourcing Workshop, UbiComp*.

Ghert-Zand, R. (2020) *You can help Nazi victims' families learn their fates in online archive project*, 22 July. Available at: https://www.timesofisrael.com/you-can-help-nazi-victims-families-learn-their-fates-in-online-archive-project/ (Accessed: 5 June 2024).

Gupta, R. and Brooks, H. (2013) *Using social media for global security*. Indianapolis: John Wiley. Available at: Inchttps://books.google.co.in/books?id=Fm0uWf9EL7cC&printsec=frontcover#v=onepage&q&f=false (Accessed: 10 April 2024).

Halder, B. (2014) 'Crowdsourcing collection of data for crisis governance in the post-2015 world: Potential offers and crucial challenges', in *Proceedings of the 8th international conference on theory and practice of electronic governance* (ICEGOV '14). New York, NY: Association for Computing Machinery (ACM), pp. 1–10. doi: 10.1145/2691195.2691208.

Hosseini, M., Phalp, K., Taylor, J. and Ali R. (2014) 'The four pillars of crowdsourcing: A reference model', in Conference Proceedings: *2014 IEEE eighth international conference on research challenges in information science (RCIS)*, IEEE, Marrakech, Morocco, 2014, pp. 1–12, doi: 10.1109/RCIS.2014.6861072.

Howe, J. (2006) 'The rise of crowdsourcing', *Wired*, 1 June. Available at: https://www.wired.com/2006/06/crowds/ (Accessed: 10 April 2024).

Hui, J.Y. (2015) *Crowdsourcing for national security*. Policy report. Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University. Available at: http://www.jstor.org/stable/resrep05853

Ilbiz, E. and Kaunert, C. (2023) 'Crowdsourcing to tackle online child sexual exploitation: Europol's "stop child abuse—trace an object" platform', *Policing: A Journal of Policy and Practice*, 17 paad009, doi: 10.1093/police/paad009.

Jia, C., Lee, A.Y., Moore, R.C., Decatur, C.H.-S., Liu, S.X. and Hancock, J.T. (2024) 'Collaboration, crowdsourcing, and misinformation', *PNAS Nexus*, 3(10), p. 434. doi: 10.1093/pnasnexus/pgae434.

Kumar, V. (2022) 'Crowdsourcing cyber peace and cybersecurity', in Shackelford, S.J., Douzet, F. and Ankersen, C. (eds.) *Cyber peace: charting a path toward a sustainable, stable, and secure cyberspace*. Cambridge: Cambridge University Press, pp. 230–235.

Kumar, S. and Faisal, M. (2024) 'A comprehensive examination of digital privacy in crowdsourcing applications', *2024 International conference on automation and computation (AUTOCOM)*, Dehradun, India, pp. 352–357. doi: 10.1109/AUTOCOM60220.2024.10486102.

Markowsky, G. (2013) 'Crowdsourcing, big data and homeland security', in *IEEE international conference on technologies for homeland security* (HST) 2013, pp. 772–778. doi: 10.1109/THS.2013.6699101.

McCullagh, D. (2013) *FBI seeks crowdsourcing help in Boston bombing case*: *ID these two men!* ,18 April. Available at: https://www.cnet.com/tech/tech-industry/fbi-seeks-crowdsourcing-help-in-boston-bombing-case-id-these-two-men/ (Accessed: 05 May 2024).

Moghadas, M., Fekete, A., Rajabifard, A. and Kötter, T (2023) 'The wisdom of crowds for improved disaster resilience: A near-real-time analysis of crowdsourced social media data on the 2021 flood in Germany'. *GeoJournal,* 88, pp. 4215–4241. doi: 10.1007/s10708-023-10858-x.

Németh, A. and Magyar, S. (2021) 'An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application (part 2)', *National Security Review*: *Periodical of the Military National Security Service*, 1(14), pp. 218–231.

Nhan, J., Huey, L. and Broll, R. (2017) 'Digilantism: An analysis of crowdsourcing and the Boston Marathon bombings', *The British Journal of Criminology*, 57(2), pp. 341–361, doi: 10.1093/bjc/azv118

Osta, Z. (2024) *Crowdsourced DDoS attacks amid geopolitical events*. 16 January. Available at: https://flare.io/learn/resources/crowdsourced-ddos-attacks-amid-geopolitical-events/ (Accessed: 10 May 2024).

Papapesios, N., Ellul, C., Shakir, A. and Hart, G. (2019) 'Exploring the use of crowdsourced geographic information in defence: Challenges and opportunities', *Journal of Geographical Systems,* 21, pp. 133–160. doi: 10.1007/s10109-018-0282-5.

Pawar, S. (2023) *The power of collective intelligence: Leveraging threat intelligence to protect against cyber threats,* 30 May. Available at: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/leveraging-threat-intelligence-to-protect-against-cyber-threats/ (Accessed: 28 November 2024).

Russia Will Pay (2024) *Kyiv School of Economics*. Available at: https://kse.ua/russia-will-pay/ (Accessed: 15 May 2024).

Samotin, L.R., Friedman, J.A. and Horowitz, M.C. (2023) 'Obstacles to harnessing analytic innovations in foreign policy analysis: A case study of crowdsourcing in the US intelligence community', *Intelligence and National Security*, 38(4), pp. 558–575. doi: 10.1080/02684527.2022.2142352.

SciCast (2024) *SciCast is on vacation*. Available at: https://scicast.org/ (Accessed: 15 May 2024).

Siegel, A. (2023) *UK's cosmic bazaar and US' INFER forecasting collaboration is launched*, 20 February. Available at: https://www.cultivatelabs.com/posts/uk-and-us-government-forecasting-collaboration-is-launched (Accessed: 10 March 2024).

Simoiu, C., Sumanth, C., Mysore, A. and Goel, S. (2019) 'Studying the "Wisdom of Crowds" at Scale', *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing*, 7(1), pp. 171–179. doi: 10.1609/hcomp.v7i1.5271.

Stastny, B.J. and Lehner, P.E. (2018) 'Comparative evaluation of the forecast accuracy of analysis reports and a prediction market', *Judgment and Decision Making*, 13(2), pp. 202–211. doi: 10.1017/S1930297500007105.

Stottlemyre, S.A. (2015) 'HUMINT, OSINT, or something new? Defining crowdsourced intelligence', *International Journal of Intelligence and CounterIntelligence*, 28(3), pp. 578–589. doi: 10.1080/08850607.2015.992760.

Tahmasebian, F., Xiong, L., Sotoodeh, M. and Sunderam, V. (2020) 'Crowdsourcing under data poisoning attacks: A comparative study', in Singhal, A. and Vaidya, J. (eds.) *Data and applications security and privacy XXXIV.* vol. 12122. Cham: Springer, pp. 310–332. doi: 10.1007/978-3-030-49669-2_18.

Tapia, A.H. and LaLone, N.J. (2014) 'Crowdsourcing investigations: Crowd participation in identifying the bomb and bomber from the Boston Marathon bombing', *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, 6(4), pp. 60–75. doi: 10.4018/IJISCRAM.2014100105.

Tewksbury, D. (2012) 'Crowdsourcing homeland security: The Texas virtual BorderWatch and participatory citizenship', *Surveillance & Society*, 10(3–4), pp. 249–262.

Tucker, P. (2014) 'This is how America's spies could find the next national security threat – A recent breakthrough in online prediction markets promises a better glimpse of the future – paid for by US intelligence', *Defense One*. Available at: https://www.defenseone.com/technology/2014/02/long-overdue-return-crowd-sourced-intelligence/79094/ (Accessed: 10 March 2024).

Zegart, A. (2021) 'Spies like us: The promise and peril of crowdsourced intelligence'. *Foreign Affairs*, 22 June. Available at: https://www.foreignaffairs.com/reviews/review-essay/2021-06-22/spies-us (Accessed: 15 May 2024).