frontiers | Frontiers in Political Science

TYPE Original Research
PUBLISHED 09 September 2024
DOI 10.3389/fpos.2024.1379789

Shift in intelligence issue ownership: conceptualizing CITINT—intelligence conducted by citizens

Iikka Pietilä[1]*, Katleena Kortesuo[2], Ulla Pohjanen[3] and Mikko Tuominen[4]

[1]Finnish Defence Forces, Helsinki, Finland, [2]Independent Researcher, Hämeenlinna, Finland, [3]Independent Researcher, Tornio, Finland, [4]Independent Researcher, Kempele, Finland

Check for updates

OPEN ACCESS

EDITED BY
Mikko Hiljanen,
University of Jyväskylä, Finland

REVIEWED BY
Łukasz Jureńczyk,
Kazimierz Wielki University of Bydgoszcz, Poland
Dries Putter,
Stellenbosch University, South Africa

*CORRESPONDENCE
Iikka Pietilä
✉ iikka.pietilae@gmail.com

RECEIVED 31 January 2024
ACCEPTED 28 May 2024
PUBLISHED 09 September 2024

CITATION
Pietilä I, Kortesuo K, Pohjanen U and Tuominen M (2024) Shift in intelligence issue ownership: conceptualizing CITINT—intelligence conducted by citizens. *Front. Polit. Sci.* 6:1379789. doi: 10.3389/fpos.2024.1379789

This article elaborates on the conceptualization of CITINT, i.e., the intelligence activities conducted by citizens and NGOs. This article is a preliminary attempt to establish foundation and perspectives for future research and to provide for initial conceptualization of CITINT. Moreover, this article elucidates CITINT's implications from legislative perspective within the Finnish context. A semi-systematic, limited literature review incorporating academic literature, governmental outlets, and news was executed to explore the contexts and definitions regarding CITINT. Interviews with a journalist, an active CITINT individual, and a detective superintendent of the Finnish National Bureau of Investigation were conducted to clarify and provide backrest for conceptualization. The key contributions of this article are further elucidation of CITINT as a concept and its implications. Moreover, this article discusses the shift in power relations from centralized issue ownership of intelligence activities toward a more fragmented scene in which individuals and non-governmental organizations (NGOs) have more relevance, possibilities, and weight. Within CITINT, this article points out the differentiation between governmentally facilitated CITINT and the bottom-up CITINT conducted by individuals and NGOs on their own terms and tools. One key contribution of this article is connecting CITINT to societal participation through the CCSCM framework. Although the interviews comprise an empirical component, support contextualization, and provide tangible examples, this article's focus is on the theoretical and conceptual aspects of CITINT. The article concludes with a discussion on the outlook, possibilities, and challenges of CITINT and provokes questions for further discussion on the matter.

KEYWORDS

CITINT, intelligence, civic intelligence, citizen intelligence, societal participation

1 Introduction

The concept of CITINT has been introduced to describe intelligence conducted by citizens. The acronym consists of the words *citizen* (or alternatively civic[1]) and *intelligence* (see, e.g., Steele, 2002; Teti, 2012; Pešek, 2023). In this article, the term intelligence is used in a broad sense to denote intelligence activities such as organizational, governmental, and sub-process of decision-making (e.g., McDowell, 2008). Moreover, in this article, intelligence refers to the sensor-level data produced by intelligence organizations, the processed and analyzed information, and the conclusions and recommendations for courses of action produced by the intelligence process.

Furthermore, in the context of this article, the term intelligence can also refer to military, forensic, and industrial intelligence or, for example, information produced in support of disaster and crisis management. It is noteworthy that this article discusses the strategic, operational, and tactical levels of intelligence, as the conclusions and inferences elaborated on CITINT may emphasize these different levels. In this article, the strategic level is particularly linked to, for example, national decision-making and the longer term, the operational level to regional activities and the medium term, and the tactical level to the grassroots and individual actors, and the short term in decision-making (see, e.g., Kerttunen, 2007).

This article discusses CITINT in terms of methods, platforms, legislation, social power relations, and issue ownership. In the context of this article, power relations are viewed similarly to those outlined by Meriläinen (2014, p. 38) as "an attribute needed in getting attention for a topic, and on a different level, influencing how it is seen […] Power is also connected to the position an actor has in the network." Moreover, issue ownership is regarded as how actors set themselves or are externally set to be more reliable, credible, and able to operate and decide on a matter, phenomenon, or an event, than others (e.g., Meriläinen, 2014). This article asserts that responsible facilitation of CITINT and participation through CITINT activities may contribute to empowerment of citizens, enhance cohesion, and provide a possibility to have a societally impactful voice for individuals and non-governmental organizations such as third sector and voluntary organizations. Through CITINT, the potential of citizens may be better recognized, and the disparity of formative power relation and ownership regarding intelligence issues may be attenuated.

To explore CITINT in societal participation and power relations contexts, this article analyzes the literature review and interview findings through the citizen-centric socio-cognitive model (CCSCM) for societal participation (Pietilä et al., 2021; Pietilä, 2022). CCSCM is a transdisciplinary integrative framework for analyzing and exploring societal participation. It recognizes different epistemological viewpoints in a citizen-centric manner and regards societal participation as a complex set of interconnected processes, including cognitive and social domains. Considering CCSCM, societal participation can be conceptualized at the external, activity, and internal layers in relation to a citizen. In the discussion section, this article explores various aspects and implications of CITINT through these CCSCM layers (*Ibid.*).

The disambiguation of the term CITINT and more precise definition are needed, as it will assist to improve the definition of the roles, responsibilities, and obligations of non-state intelligence actors. It is expected that legislation will not be revised expediently in the CITINT field. In addition, the responsibilities related to CITINT may not be recognized by the industry, NGOs, or individuals. CITINT, or citizen intelligence, is not yet a well-established term. Thus, this article aims to elaborate and discuss the concept, to justify the need for its use, and to compare the practical implementations and differences of CITINT in comparison to government and centralized intelligence. More concisely, this article seeks to answer the questions:

1. How should CITINT be conceptualized and defined?
2. How is CITINT positioned in the overall field of intelligence?
3. What are the implications of CITINT in the perspectives of societal participation, power relations, and (Intelligence-) issue ownership?

Additionally, this article identifies and discusses the possibilities and challenges of CITINT.

In this introduction, the main problematics underlying and the goals steering this article are introduced. After the introduction, an overview of the limited literature review follows. This article continues by reviewing the definition of the term CITINT and discussing its relationship to other intelligence concepts. Moreover, the need for this term and its more concise conceptualization are rationalized. The differences between government intelligence and citizen intelligence in terms of goals, resources, training, and roles are explored. Furthermore, this article discusses the relevant legislation applicable to citizen intelligence in the Finnish context, which is followed by introduction of the various third-sector actors and commercial companies that conduct CITINT as examples, as well as two tools developed for use by government-facilitated CITINT and non-governmental CITINT actors. We continue to describe the interview settings and summarize the findings from the interviews. Finally, the reader's attention is drawn to the expansion of CITINT activities and the identified threats, weaknesses, and opportunities. Additionally, the research questions are briefly revisited, and future research topics are proposed.

2 CITINT in literature and Finnish legislation: an exploration

2.1 Semi-systematic limited literature review process

The semi-systematic limited literature review was conducted in four steps, and characteristics of the applied PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method (Moher et al., 2009; Pietilä, 2022; Henrico and Putter, 2024) can be identified. Additionally, snowballing was applied, i.e., references identified in the articles that were found in initial search were further explored. Steps to decide on the inclusion of the item in the review

[1] To avoid ambiguities, it is noteworthy that a certain form of societal and political participation can be denoted by the expression civic intelligence (see, e.g., Pietilä, 2022). These activities may include, for instance, solving collaborative political problems through deliberative means. However, this kind of civic intelligence is outside the scope of this article.

were the following: (1) Title level appraisal, (2) Abstract level appraisal, (3) Appraisal through skimming, and (4) Full item appraisal. If the item was considered to explain or elaborate on the term CITINT or to reflect similar phenomena, the item appraisal was continued in the next step. If the item was considered to be irrelevant, i.e., not to explain or elaborate on the term CITINT or to reflect similar phenomena at any appraisal stage, it was excluded. The literature search was conducted in databases of Scopus and Google Scholar with keywords "CITINT," "Civic intelligence," "Citizen intelligence," and "Intelligence by citizens." These databases were selected for their wide coverage and indexing of journal and conference publications as well as their convenience. These keywords were defined on the basis that they were identified to reflect CITINT, and snowballing was applied to broaden the possible findings. The first step was limited to including 200 items in Scopus and Google Scholar with each string, and overlapping items were removed at the first step. Additionally, more specific inquiries with similar search strings were conducted in the web resources of intelligence services, ministries, and university publications, as well as on the Google search engine. Thus, the research is characterized as semi-systematic and limited in the scope of reviewing available literature. In addition, news outlets and papers were not excluded from the results, although anecdotal, due to the novelty and ambiguity of the term CITINT. The relevant academic sources and databases are listed in more detail in Table 1.

TABLE 1 Main targets and databases for the literature review.

Service/ repository name	Publisher	Link	Category
Intelligence and National Security	Taylor & Francis	https://www.tandfonline.com/journals/fint20	Academic journals
The International Journal of Intelligence, Security, and Public Affairs	Taylor & Francis	https://www.tandfonline.com/journals/usip20	Academic journals
Journal of Intelligence Studies in Business	Halmstad University	https://ojs.hh.se/index.php/JISIB/about	Academic journals
International Journal of Intelligence and Counter Intelligence	Taylor & Francis	https://www.tandfonline.com/journals/ujic20	Academic journals
Scopus	Elsevier	https://www.scopus.com	Publication database
Google Scholar	Google	https://scholar.google.com/	Publication database/Search engine

2.2 Pursuing disambiguation—how has the term CITINT been used previously?

The term CITINT has been used, for instance, in Burke's (2022) article, but no precise definition is given. CITINT also appears in the article by Laulajainen, Taivalmaa, Vilén, and Virtanen, where they divide non-state intelligence activities into five sub-areas: (1) commercial intelligence companies, (2) criminal and terrorist organizations, (3) NGOs and aid organizations, (4) researchers, investigative journalists, citizen journalists, and citizen intelligence, and (5) intelligence as part of the normal business operations of companies (Laulajainen et al., 2023, pp. 7, 14–17). According to this division, CITINT is categorized under unorganized volunteering, the fourth category, with Burke as their source. This categorization excludes, among others, remote intelligence agencies, criminal organizations, registered associations, and non-governmental organizations (*Ibid.*).

The five-part division can be disputed because the status of the categories of actors listed in the article is quite open to interpretation and partly overlapping. It could be argued that many terrorist organizations can, at the same time, be NGOs, albeit unethical ones. For example, does the Irish Republican Army (IRA) conform to the description of a terrorist organization or as an NGO? The IRA has a history of both years of physical violence as well as more peaceful years of influence (Arthur and Cowell-Meyers, 2023). The question then arises—does the status of CITINT switch back and forth depending on the disposition of the group? Malkki (2014) also notes that the definition of terrorism is still blurred and there is no consensus. One may also wonder whether it is clear from a CITINT perspective if the same person can alternately be or not be a CITINT actor. For example, if an individual CITINT practitioner sets up a company or if a free CITINT group registers as an association, will its activities fall outside CITINT? If an entrepreneur carries out an individual intelligence operation as a hobby, would the result again be CITINT?

2.3 CITINT as part of the intelligence taxonomy

The sub-categories of intelligence can be classified according to different criteria. One criterion for classification is the channel, technique, or means of obtaining information (source) used in the intelligence activity. This is used in the five-part classification presented by Lowenthal and Clark: HUMINT, GEOINT, MASINT, SIGINT, and OSINT, where HUMINT refers to personal intelligence, GEOINT to geospatial intelligence, MASINT to measurement and sensor intelligence, SIGINT to signal intelligence, and OSINT to open-source intelligence (Lowenthal and Clark, 2015; Althoff, 2015). Moreover, Henrico and Putter (2024); see also Putter and Henrico (2022) recognize SOCMINT (social media intelligence) similarly. For all of these, the type or technique used to obtain the information determines the name of the intelligence category.

Another criterion for defining the sub-categories of intelligence is the subject of the intelligence. For example, counterintelligence (CI) refers to activities directed at the intelligence of an adversary (Lowenthal and Clark, 2015; Isokangas, 2023). Business intelligence, on the other hand, is focused on the business environment, competitors, and market situation (Isokangas, 2023). Similarly, financial intelligence (FININT) focuses on economic information and monetary transactions (Walton, 2013, p. 393).

The third criterion for classifying the types of intelligence is the social role and legal status of the person conducting it. In Finland, for example, military intelligence is an activity for which the Defence Forces are responsible. Security intelligence, on the other hand, is the responsibility of the Finnish Security Intelligence Service (Suojelupoliisi, n.d.). Criminal intelligence is carried out by a law enforcement authority, the police, and in serious cases also by the Finnish Security Intelligence Service (Sisäministeriö, 2017, p. 11).

CITINT is best defined by the third criterion, the social role of the implementer. If CITINT is, by definition, intelligence conducted by a non-state actor, it would therefore be a parallel concept to military, civil, and criminal intelligence. It should be noted that there has, in fact, been a gap in the concept of intelligence. There is no standard term for intelligence by lay people, associations, companies, and free collectives.

2.4 CITINT vs. governmental intelligence activities

The starting points for intelligence collection by citizens and by states are different. For the state intelligence organization, the motivation and obligation to produce intelligence is often to support state-level decision-making and to guarantee national security (Finnish Security Intelligence Service, n.d.). The state trains intelligence professionals to meet its own needs. For example, at the National Defence University, one of the cadets' fields of study is intelligence, and the Defence Forces Intelligence Institute also operates an Intelligence School (Maanpuolustuskorkeakoulu, 2019; Puolustusvoimat, n.d.). In contrast, open academic studies in intelligence have only been possible since autumn 2019 at the University of Jyväskylä (Vähätalo, 2019). Thus, it can be assumed that citizen intelligence has largely been a skill learned through experience in the Finnish context (see also Mitrovich, 2016).

Intelligence collection from citizens and government is different in several respects. The state has secret intelligence sources that citizens generally do not have in the same way. Citizen intelligence is largely based on the use of OSINT data, although overall Western intelligence is estimated to be based on approximately 80–90% OSINT data (Ghioni et al., 2023).

States have more human and technical resources to carry out their own MASINT, SIGINT, GEOINT, and HUMINT reconnaissance, to which citizens usually have very limited access. Some satellite imagery and radiation measurement data from mapping services and public agencies are shared on the public web and can be freely accessed by citizens. In addition, SIGINT and COMINT data can be collected and published by, e.g., amateur radio operators with proper equipment.

Attributed to their networks, citizen investigators could theoretically have even more human resources for intelligence than the state. However, government activities may be better organized and managed with clearer shared motivation and objectives. The state also has legal means of coercion to produce intelligence within its own administration, for example, by intercepting the telephone calls of private individuals. In contrast, state organizations are notoriously bureaucratic, which makes them less agile in their ability to collect intelligence. As noted further in the article on the legal aspects of the paper, state actors may, where necessary, obtain confidential information from other authorities to which a private individual does not have legal access.

Commercial companies' intelligence collection is partly based on the same principles as for private individuals, as the legislation and the means of collecting intelligence are very similar. However, some companies may have significant intelligence-related sources at their disposal other than the public. This is the case, for example, with Wagner, a private military company (PMC) used by the Russian state, which is in principle a commercial entity but in practice a state arm. In addition, a company may have more resources to purchase, for instance, OSINT or IMINT material than a private citizen and thus have better access to paid information.

2.5 CITINT and legislation in Finland

In Finland, the authorities have their own intelligence legislation, which allows intelligence to be used in the activities of the authorities as required by law. In contrast, when a citizen considers intelligence, either as an organized network or as an individual actor, there is no separate legislation or individual governing law, and the individual needs to adhere to various bodies of legislation. The more intelligence information a citizen collect in their private capacity, the greater the risk of getting into legal issues (Mäki-Kuhna, 2023).

The laws presented in this section are those that should be considered when engaging in CITINT-related activities. This is not an exhaustive list, but it covers various situations where it is expected that a legal aspect will also need to be taken into account. Primarily Finnish legislation is considered here, but the reader is also invited to consider the EU human rights treaties (EU, 2021) and, for example, the Geneva Conventions relative to the Protection of Civilian Persons in Time of War (Ulkoasiainministeriö, 2015). Although important, further jurisprudential explorations and research through, e.g., precedents are outside the scope of this article and left for later studies.

2.5.1 The constitution of Finland and the Data Protection Act

Chapter 2 of the Constitution of Finland 791/1999 (Perustuslaki 731/1999, 2018) promulgates the fundamental rights of every Finnish citizen or legal resident. These include equality (section 6), freedom of movement (section 9), the right to privacy (section 10), freedom of expression and right of access to information (section 12), and protection of property (section 15). The list is not exhaustive, but the most relevant for the purposes of this inquiry have been selected. Derogations from the provisions of the Constitution may only be made in the manner specified in other legislation, but otherwise, all activities must take account of the provisions of this Act. It is also important to bear in mind the principle of criminal legality laid down in section 8 of the Constitution: no one may be held guilty of a crime that is not punishable by law at the time it is committed (Perustuslaki 731/1999, 2018). This article is linked to the presumption of innocence in Chapter 4, section 2, of the Criminal Investigation Act (805/2011) (Esitutkintalaki 805/2011, 2024). Thus, if the involvement of a person in the course of events is only being investigated, he cannot be referred to as a criminal but is always a suspect. Only when the perpetrator has been convicted in court under Finnish law can he or she be referred to as a criminal.

Already, when planning the collection of data, it should be considered in a legal sense whether the collection will result in the creation of content and/or artifacts (text, voice, or image) that may contain stored personal data. There are specific legal requirements for the storage of personal data. The Finnish Data Protection Act (1050/2018) (Tietosuojalaki 1050/2018, 2024) regulates the collection, storage, and processing of personal data in order to ensure the reliability, integrity, and availability of the data. Data must be collected only for the necessary purposes; it must be stored and processed in such a way that no third party has access to it to modify or read it, and the stored data must be disclosed to the data subject at his or her request (Tietosuojalaki 1050/2018, 2024).

Data protection law focuses more on data collected by organizations and businesses than on data collected by individuals. Individuals are in principle free to use the data for their own purposes and do not have to compile a register, but the emphasis is on the purpose of the data and its publication. The collection and dissemination of private data are governed, *inter alia*, by the constitutional article on freedom of expression (Perustuslaki 731/1999, 2018). The dissemination of information is affected by the penalties laid down in the Criminal Code for the dissemination of private or confidential information, so that the dissemination of information and opinions of individuals in the name of freedom of expression is not completely free. The restrictive provisions will be discussed in more detail later.

2.5.2 Public Order Act and Criminal Code

The intelligence-gatherer is also likely to face the question of whether they can take pictures or videos and listen to or record audio. In principle, filming in public places is allowed under the Public Order Act 612/2003 (Järjestyslaki 612/2003, 2022). Public places are areas that are accessible to the public, including roads, parks, squares, swimming pools, and public transport. Public places also include buildings that are open to the public during an event or during the opening hours of a business. These include public offices, public areas of transport stations and shopping centers, and restaurants (Järjestyslaki 612/2003, 2022). Filming cannot be prohibited on these premises if the activity is not otherwise disruptive. However, in areas protected by public peace and domestic peace, filming requires the permission of the owner or operator of the area. Places protected by public order are parts of public places closed to the public, as well as parts and places, buildings, and areas to which access is restricted (Criminal Code 39/1889) (Rikoslaki 39/1889, 2024).

There are more issues to consider regarding the publication of a stored document, even for a private enquirer. If a recorded document contains information about private life or if the document in question offends the honor of the person identifiably appearing in the document, the publication may constitute a criminal offense. For example, an individual citizen can record all his or her own telephone calls and take videos and photos in public places, and to some extent even on private property, if the conditions are met. However, what matters is how the recording is used: whether it is made available to others in a way that is offensive to the privacy of the person recorded, or whether it is used, for example, as evidence in court, where it has a more limited view. The latter is permissible, as a document containing private life can be presented as evidence in court.

The Criminal Code (39/1889) lists all the penalties that can be imposed if the law is not respected. Chapter 24 of the Criminal Code (39/1889) provides for violation of privacy, peace, and personal reputation. These provisions, together with other legislation, provide very strong protection for individuals and, to some extent, organizations, so it is likely that the first thing a citizen making an enquiry will need to do when seeking information is to consider the provisions of this chapter. The provisions of the chapter include, *inter alia*, violation of domestic privacy (section 1), violation of privacy relating to public premises (section 3), eavesdropping (section 5), illicit observation (section 6), the preparation of the above (section 7), defamation (section 9), dissemination of information violating personal privacy (section 8), and other similar acts. In Chapter 25, offenses against liberty, section 7a, stalking, which could be committed by means of surveillance. If, on the other hand, a citizen informer requires someone to disclose some information against his will, this is a case of coercion under section 8. The Criminal Code also prevents the use of so-called "targeting" by prohibiting extortion in Chapter 31, section 3.

Among other things, Criminal Code 39/1889 provides for secrecy offenses (section 1), violation of the secrecy of communications (section 3), interference with communications (section 5), interference with an information system (section 7), unlawful access to an information system (section 8), offense involving a protection decoding system (section 8b), data protection offense (section 9), and identity theft (section 9a) (Rikoslaki 39/1889, 2024). These provisions also apply to legal persons, i.e., organized organizations. Chapter 15, section 10 of the Criminal Code (Rikoslaki 39/1889, 2024), on the other hand, imposes an obligation on every citizen to give prior warning to the authorities or to the person threatened by the crime of certain serious crimes if he or she becomes aware of such a crime or of its preparation. This does not apply where the person who is preparing the offense happens to be a close relative.

In terms of business intelligence, Chapter 30 of the Criminal Code (Rikoslaki 39/1889, 2024) provides for business offenses, the most significant of which for the informer are section 2, unfair competition offense, and section 4, business espionage. Chapter 30 also contains provisions on violation of a business secret (section 5) and their misuse (Article 6) (Rikoslaki 39/1889, 2024).

The Criminal Code also has its own provisions for offenses against the Finnish state, and these are offenses subject to general prosecution. Several other articles of the Criminal Code, already mentioned earlier in this chapter, reserve the right to act on the part of the prosecutor when the public interest so requires, although in the main the offenses are otherwise crimes against the person concerned. Of the offenses against the Finnish State, offenses of treason are provisions that are worthy of attention from an intelligence point of view. These are set out in Chapter 12 and, in particular, in section 9, unauthorized intelligence activities.

"Unauthorized intelligence activities: A person who, for the purpose of causing damage to a foreign state or benefiting another foreign state, acquires information on the national defense or national security of a foreign state or on matters with direct relevance to these, and in doing so causes damage or danger to Finland's foreign relations, shall be sentenced for unauthorized intelligence activities to imprisonment for at least 4 months and at most 6 years" (Chapter 12, section 9 of the Criminal Code). This imposes restrictions on the publication of information. If information under this section becomes public in such a way that Finland's relations with the rest of the world deteriorate, the perpetrator must be punished. The section on treason also covers any crime that is considered to be international in nature and that has a negative impact on Finland or on Finland's position (see Chapter 13. Offenses of High Treason, Criminal Code 39/1889).

2.5.3 Summary of legislation on citizens' enquiries

In April 2023, the KRP opened an investigation into the disclosure of a security secret (Poliisi, 2023). Crimes of this type are rare in Finland, and the case received much of national media coverage when it was revealed; after all, the suspects were also candidates in the parliamentary elections. It has not been revealed exactly where the suspects' criminal investigation originated, but the suspects have been promoting the so-called tunnel war theory on their website and YouTube channel and have kept a map of the tunnels in Finland alongside it. From the videos, which have now been removed, it can be seen that the suspects have gone into areas where, by law, movement is subject to authorization (Vapa, 2023).

The case is a good example of failed intelligence-related activity by citizens. If you do not know the law, you can be accused. Information collected by a private individual is not necessarily criminal, but how it is collected, how it is published, and to whom it is available, are factors worthy of particular attention and possible legal sanction.

If the definition of CITINT includes all non-governmental intelligence activities, then, depending on the way the activities are organized and carried out, the number of laws and guidelines to be considered will only increase. For example, journalists and the media are governed by specific legislative prescripts and professional codes of ethics, while a private investigator must consider the provisions of the Private Security Services Act (765/2003).

3 Actors, operators, tools, and platforms—who conducts CITINT and how?

There are a few CITINT groups, groupings, and sectors in Finland. The article provides a (non-finite) overview of the Finnish CITINT domain and its actors and operators. Moreover, two CITINT tools are presented to elucidate a more practical aspect of CITINT. The selected tools, Ukrainian Delta and Blackbird, were selected as they represent different paradigms in CITINT.

3.1 CITINT actors and operators

3.1.1 CITINT groups emerging from civic action, such as the black bird group

The Black Bird Group is probably the best-known CITINT group in Finland. It started shortly before the start of the war in Ukraine, when OSINT enthusiasts Eerik Matero, John Helin, and Emil Kastehelmi decided to prepare for frontline surveillance in February 2022, even before the war started. The group's profile grew rapidly. The Black Bird Group went for more than a year without a name, until foreign actors asked the group to come up with a name for itself. The Black Bird Group has since registered as an association, and the aim is to continue to produce commercial intelligence products for sale. There are other similar loose groupings, but he could not directly name others. At least in the free OSINT network Bellingcat, the Finnish Veli-Pekka Kivimäki has been active (Higgins, 2021; Interview #1).

3.1.2 Society for Investigative Journalism

The Society for Investigative Journalism was founded on 24 November 1992 (Tutkivan journalismin yhdistys, 2011, 1). In investigative journalism, both OSINT and HUMINT techniques are used for data collection and analysis (Nelliyullathil, 2020, p. 61; Scott, 2023, p. 1). In addition, economic intelligence methods, or FININT analysis, are used (Scott, 2023, p. 2).

The source material included an interview with an investigative journalist who wishes to remain anonymous. The interviewee confirmed that OSINT, HUMINT, and FININT are used. The journalist described the massive volume of work that is done with the datasets. Often, data leaks contain a large amount of data, which may include data from multiple data nodes, virtual machines, and servers. Deciphering this requires the author to have ICT skills to process the raw data into a usable format (Interview 1, 2023). Thus, similarities with governmental workflows may be identified where data are processed into information (Isokangas, 2023).

The interviewee (Interview 1) said that an important source of information in the work of an investigative journalist is the "deep corner," the "deep informant," with whom one may stay in contact for years. The interviewee stressed that this is not a friendship but a professional relationship of trust. In practice, the use of a deep throat is fully comparable to that of a HUMINT agent of state intelligence, who is recruited from another state, for example (Isokangas, 2023). The interviewee said that in the field, such a source is considered worth a diamond, and therefore an investigative journalist might contact the source every 6 months to ask him or her for news (Interview 1, 2023).

In the field of investigative journalism, international conferences are often held to educate people on the methods, story processes, and legislation of different countries. Intelligence techniques are therefore developed and shared with colleagues on a regular basis, thus keeping intelligence skills in a continuous cycle of development (Interview 1, 2023; GIJN, n.d.; Tutkivan journalismin yhdistys, 2023).

3.1.3 Finnish association of private detectives and law firms

The Finnish Association of Private Detectives and Law Firms was founded in 1972 (SYL, n.d.-a). The industry strives to acquire, handle, and store information responsibly, as the association's code of ethics sets out guidelines such as data security, proper storage of information, compliance with the law, impartiality, and confidentiality (SYL, n.d.-b).

In his blog, Jyri Paasonen, PhD in Law, considers the sources of information for private investigators. These are public sources (OSINT) and information from the client (HUMINT). Paasonen also mentions observation in public places and, for example, acting as a client of a competing company, which represents both OSINT and HUMINT activities (Paasonen, 2023).

3.1.4 Other commercial CITINT operators

There are numerous commercial CITINT operators, some of which have intelligence as their main activity and others where it is only one aspect of their services, for example, in consultancy or recruitment.

For example, Iceye Ltd. is a commercial intelligence company that produces satellite imagery, analysis, and reports (Iceye, n.d.). It is therefore reasonable to conclude that Iceye's main business is intelligence, even though Statistics Finland does not recognize such an industry category (Tilastokeskus, n.d.). According to the business directory Finder, Iceye's main activity is 71,121 Urban Planning (Finder, n.d.). Of course, another possible main business activity of an intelligence company could be in the category of other information service activities (Tilastokeskus, n.d.).

Many consultancies and direct search companies use enquiries as part of their range of services. For example, the recruitment company Inhunt explains on its website that the stages of the direct search process include finding the right person, onboarding, selection, suitability assessment, decision support, and follow-up (Inhunt, n.d.). The model is thus very close to HUMINT's recruitment method, which first targets a suitable target, investigates his background, establishes contact, develops the target, recruits him as an agent, and finally moves the agent to the processing stage (Isokangas, 2023).

3.1.5 Criminal CITINT operators

Not all CITINT operators act legally. According to a detective superintendent of the Criminal Investigation Department of the Finnish Criminal Police, there are criminal individuals and groups in Finland that carry out intelligence activities. The detective superintendent points out that criminals are not prevented (nor seemingly deterred) by legal constraints, so their tools include threats of violence, illegal technical intelligence equipment, data breaches, and the purchase of information obtained through breaches. Of course, an individual can also fall into the trap of using an illegal device, such as a radar detector, without criminal intent. According to interviewee #2, the weak point of criminal groups is often operational security (or defensive CI), which allows the police to apprehend the perpetrators while transgressing the legal prescripts (Interview #2, 15 November 2023).

An YLE news article also suggests that the 2002 transport robbery in Turku (Finland) required intelligence at the time. Those who attempted the robbery had not only the schedule of the transport but also the interior drawings of the van. The robbery failed because the van was a different model than the drawings (Collin, 2020).

3.2 CITINT platforms and tools

In the introduction, CITINT was preliminary outlined at a high level as intelligence collection by citizens. However, especially in the light of the dichotomy of governmentally facilitated CITINT and bottom-up (tactical) CITINT conducted by individuals and NGOs, the tools and platforms have a significant role in enabling data collection, analysis, and intelligence dissemination. Here we consider two tools used in CITINT: the Delta tool is a means of governmental CITINT facilitation, and Blackbird is an open search tool. These tools were selected for introduction as they represent the extreme ends of the proposed dichotomy.

3.2.1 Ukrainian delta

The Ukrainian Armed Forces have a situational awareness[2] tool and platform called Delta (Figure 1). Delta enables integrative situation awareness and situation picture production and maintenance, combining data from aerial imagery, satellites, cameras, radars, chatbots, etc. (Lozovenko, 2023). The system is real-time, and its geospatial map functionality is one of its key features. In addition, Delta has been developed to be platform-agnostic from the client end, i.e., it should be accessible on PCs, smartphones, and tablets.

Delta has been developed by the Centre for Innovation and Development of Defence Technologies, part of the Ministry of Defence of Ukraine (Militarnyi, 2023a). According to Borger (2022), at least Delta's operating principles have included a less military department feeding OSINT data into the system. The development of Delta has considered NATO compatibility and integration with, for example, Link 16, a tactical data link system used by several NATO countries (Fornusek, 2023). The tool has been designed with a modern approach to allied doctrine and considers multi-domain operations (Militarnyi, 2022).

3.2.2 Blackbird tool

The Blackbird[3] tool allows you to search for users by nickname on a variety of internet services, including many social media services, streaming services, gaming platforms and stores, blogs, and repository platforms. According to the documentation, the tool targets 581 different services. The Blackbird tool is available for download from the GitHub repository on the p1ngul1n0 account for running in a standalone environment, but as of 2 November 2023, the service was also available in a browser at https://blackbird-osint.herokuapp.com/. The tool can be accessed from the command line interface (CLI), but the repository package also includes a web server that allows the tool to be accessed in a browser.

CSV and PDF export capabilities have been implemented in the tool (see p1ngul1n0, 2023; Soeiro, 2023). The Blackbird is probably named after the Lockheed SR-71 reconnaissance aircraft; the tool's logo features this aircraft (Figure 2). Figure 2 also shows the user interface of the Blackbird.

4 Interviews

To provide further elaboration on the concept of CITINT, three interviews were conducted (Table 2). The set of interviews should be regarded as an initial effort to elucidate the concept from a professional point of view. All interviewees are recognized professionals in their industries, and the aim was to collect up-to-date expert perspectives from interviewees active in the CITINT domain and industry in Finland. During the interviews, the interviewer took notes. Moreover, the analysis of the interview data is straightforward, as concrete findings are used at anecdotal level to support the elaboration of the concepts. More advanced synthesis and analysis are left for later stages, as this article is a preliminary exploration of the discussed phenomena and problematics.

[2] Endsley (1995) dissects the concept of situational awareness into perception, comprehension, and projection. These mean the observation of a situation, understanding it, and evaluating the possible developments. By situational picture tools, this article denotes such software, tools, and platforms that enable the production and dissemination of situational awareness products and representations through, e.g., timelines and maps.

[3] Not to be mixed up with the Finnish CITINT NGO with the same name.

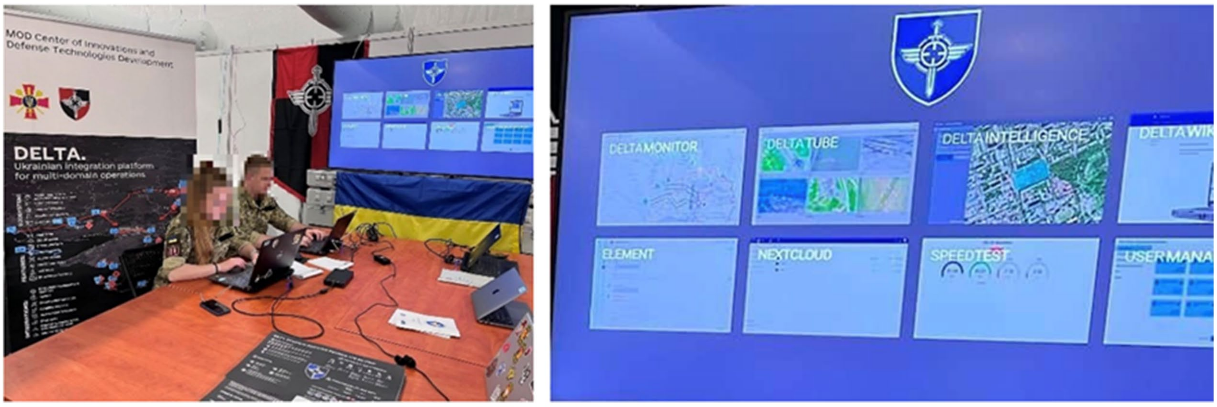
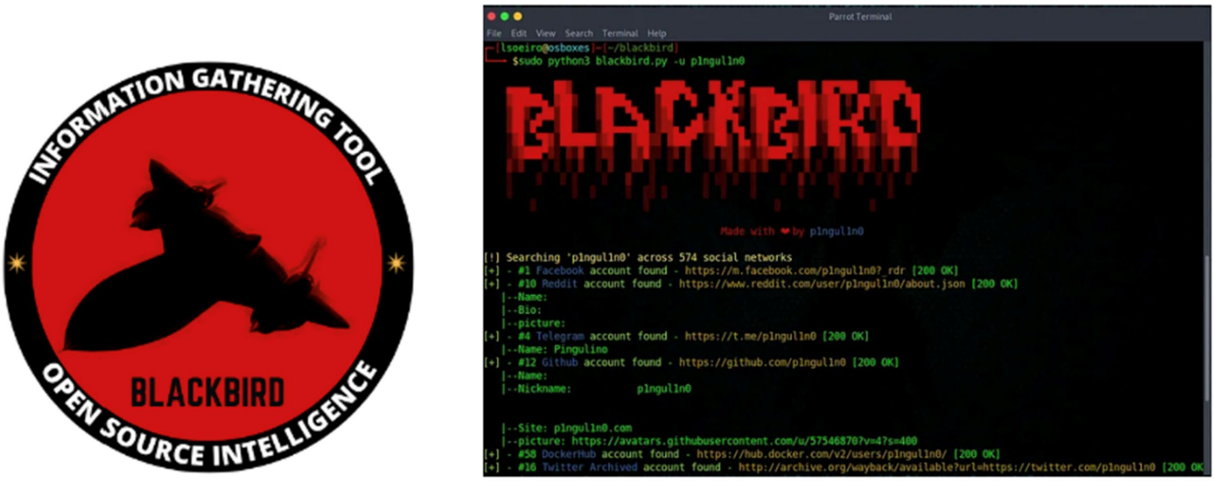

MOD Center of Innovations and Defense Technologies Development
DELTA.
Ukrainian integration platform for multi-domain operations
DELTAMONITOR
DELTATUBE
DELTAINTELLIGENCE
DELTAWIK
ELEMENT
NEXTCLOUD
SPEEDTEST
USERMANA

FIGURE 1
Delta system (Borger, 2022).


INFORMATION GATHERING TOOL
BLACKBIRD
OPEN SOURCE INTELLIGENCE
Parrot Terminal
File Edit View Search Terminal Help

```
┌─[lsoeiro@osboxes]─[~/blackbird]
└──╼ $sudo python3 blackbird.py -u p1ngul1n0

BLACKBIRD

                    Made with ❤ by p1ngul1n0

[!] Searching 'p1ngul1n0' across 574 social networks
[+] - #1 Facebook account found - https://m.facebook.com/p1ngul1n0?_rdr [200 OK]
[+] - #10 Reddit account found - https://www.reddit.com/user/p1ngul1n0/about.json [200 OK]
   |--Name:
   |--Bio:
   |--picture:
[+] - #4 Telegram account found - https://t.me/p1ngul1n0 [200 OK]
   |--Name: Pingulino
[+] - #12 Github account found - https://github.com/p1ngul1n0 [200 OK]
   |--Name:
   |--Nickname:          p1ngul1n0


   |--Site: p1ngul1n0.com
   |--picture: https://avatars.githubusercontent.com/u/57546870?v=4?s=400
[+] - #58 DockerHub account found - https://hub.docker.com/v2/users/p1ngul1n0/ [200 OK]
[+] - #16 Twitter Archived account found - http://archive.org/wayback/available?url=https://twitter.com/p1ngul1n0 [200 OK
```

FIGURE 2
Blackbird tool logo and Blackbird CLI interface (Soeiro, 2023).

4.1 Interviewees and the topics

The interviewees were selected on the basis of relevance, sample coverage, and availability. All the interviewees were estimated to be very relevant due to their expertise and experience on the matter. Selection of the interview sample aimed to enable acquisition of different kinds of perspectives. Thus, the selected interviewees represent different subfields. The first interview was conducted face-to-face with a CITINT operator (Interviewee #1), who also later checked the notes of the interview for errors. This interview was recorded, and a transcript was produced. The other two interviews were carried out by telephone and video call, as the aim was to briefly check the perspectives of different actors on CITINT activities. The interviews were used for collecting data about CITINT scene and operators since the academic literature on CITINT is yet thin. The interviewer was the same person in every interview to maintain a similar level and approach in the conversations. Moreover, the experiences acquired during the three initial interviews contribute to designing future studies and broader interviews.

4.2 Interview approach and method

The Grounded Theory approach was used in the interviews to support the explorative aims. Grounded Theory is a data-oriented method of qualitative research, the goal of which is to build a descriptive theory based on the data (Oktay, 2012, p. 4; Glaser and Strauss, 1967). The interviewees represented different roles and actors, so uniformly structured questions would not have been useful. The interviews were conducted with a low regard to structure due to the explorative approach chosen to provide for the conceptualization of CITINT. The interview method was more specifically a focused interview, where the researcher had defined the themes in advance, but the discussion was free (Hirsjärvi and Hurme, 2000). There were four main themes:

1 What kind of methods are used in CITINT? (Among intelligence enthusiasts, in commercial intelligence, among criminals, and in investigative journalism.)
2 Has CITINT become more common or more professionalized?

TABLE 2 The interviewees, dates, and themes of the interviews.

Interviewee #	Title/role and organization	Criteria for selecting the interviewees	Special sub-theme	Date and recording
1	• The Founder of a CITINT group • Special Journalist in one of the Finland's biggest newspapers	• Interviewee #1 is the most known civilian OSINT operator in Finland. • The research team needed to find out about the process and customers in CITINT field, so expertise was necessary.	• CITINT scene in Finland • Founding of the CITINT group • Commercial CITINT clients in Finland	• 17 October 2023 at Lahti • Face-to-face • Recorded • Transcript produced
2	• Detective Superintendent at the Finnish National Bureau of Investigation • Main Investigator of a large-scale data breach case	• Interviewee #2 is an experienced crime investigator who has an everyday viewpoint on criminal CITINT activities. • Interviewee #2 is highly ranked in the Finnish National Bureau of Investigation and oversees especially complicated cases.	• CITINT used by criminals in Finland	• 15 November 2023 • Via telephone • Not recorded • Notes produced
3	• Investigative journalist	• Interviewee #3 is an active and well-known investigative journalist with an international network and CITINT-related scoops. • Interviewee #3 has attended international seminars concerning CITINT. The interviewee has wide experience on the matter.	• CITINT in the work of investigative journalists	• 15 November 2023 • Via video call • Not recorded • Notes produced

3 What are the differences between CITINT and official intelligence conducted by the authorities?
4 How do the CITINT operators approach their field? (desire for development, ambition, going pro-CITINT, etc.)

In addition to this, each interviewee was asked additional questions related to their special fields (sub-themes in Table 2).

4.3 Summary of the interview key findings

Interviewee #1 elaborated that since the Russian attack on Ukraine in February 2022, there has been a rising interest toward citizen-made OSINT. Interviewee #1 had not heard of the acronym CITINT, but he acknowledged the need for a new term. Moreover, the interviews reflect that, in terms of methods and quality, CITINT strongly approaches the traditional intelligence conducted by the authorities. Technical and technological aids are more common and cheaper than before, and on the other hand, there is also more open data available. In addition, business opportunities increase CITINT, when customers are ready to pay for information and analyses. All this reflects CITINT becoming more relevant and common as an activity in the overall sphere of intelligence.

All the interviewees agreed that CITINT operators are systematically aiming for skill and method development. For instance, investigative journalists attend international seminars in the field, and even criminals exchange action tips with each other. New equipment and technologies are also adopted quickly. Criminals order illegal radar detectors and signal jammers from abroad. Correspondingly, legal operators and entrepreneurs buy high-quality satellite imagery material, and investigative journalists can use various programs to unpack or decode data breach materials.

Other aspects identified in the interviews involved phenomena such as individual motivations, networking, and collaboration with the state through subcontracting. The findings elicited through the interviews are further synthesized with the literature review remarks and set in a dialogue within the citizen-centric socio-cognitive model in the next chapter.

5 Discussion and conclusion

5.1 Making sense of CITINT through CCSCM lens

Various implications of CITINT can be identified within the citizen-centric socio-cognitive model for societal participation at the internal, activity, and external layers in relation to an individual, as highlighted in Figure 3. At the internal layer, CITINT activities may be affiliated with various processes such as motivations, enhanced subjective experience of resilience, self-actualization, and information appraisal and consolidation. At the activity layer, in the two perspectives, manifesting and non-manifesting participation, multiple CITINT-related activities can be pointed out. Non-manifesting activities include, for instance, information search and consumption, collation, and analysis. Manifesting activities consist of, e.g., networking, contacting sources, information dissemination such as publications, blogs, and providing statements and interviews for news outlets, in addition to the use of various social media services. Additionally, at the external layer, in which external artifacts, actors, and phenomena reside according to CCSCM, various facets can be affiliated with CITINT. Artifacts include tools and services, such as the ones discussed in Chapter 3, and processes and structures. Actors encompass, for instance, other individuals, organizations, decision-makers, and governmental roles. External phenomena may include events and other abstract constructs.

One of the identified motivators behind CITINT is the ambition to improve citizen consultation. According to Interviewee #1, the OSINT group has been motivated by the mistakes made by the media and the desire to produce better information. It can also be assumed that there are academic motivators for conducting intelligence in the context of research. Civic intelligence can also be motivated by ideology if one's own intelligence activities are seen to support one's own ideology in some way. The intelligence product may then be colored by support for one's own ideology. Thus, CITINT activities may also be interpreted as societal participation, as outlined by Pietilä et al. (2021) and Pietilä (2022).

Enhanced subjective experience of resilience is identified, as partaking in CITINT activities, may produce feelings of being capable of taking initiative for an individual—a theme worth exploring further among CITINT actors. Information appraisal and consolidation are inherent in activities that are set in complex and information-rich environments. Moreover, Interviewee #1 emphasized the importance of networking and communications due to their inherent value but also due to their significance in information production: Through broad networks, skilled communication, and applying HUMINT techniques, CITINT operators may even access data and information unavailable for official actors.

5.2 Interfaces between citizen and government intelligence

In comparison to the outline proposed by Laulajainen et al. (2023), a more useful and workable way to define CITINT would be to limit it to non-governmental intelligence activities. This definition is also accepted by Interviewee #1, a founding member of the private intelligence group and OSINT expert. CITINT actors could thus include commercial companies, NGOs, professional associations, individual activists, and even criminal organizations.

This can be linked to a problematic dimension identified through the literature review: government intelligence and CITINT are not entirely separate but may be interpreted to have overlapping aspects and characteristics (Figure 4). In addition, an explicit dissection between governmental intelligence and CITINT can be challenging, as individual citizens may produce inputs into governmental intelligence processes, or governmental actors may use NGOs as contractors in the production of intelligence products.

As shown in Figure 4, the government can facilitate CITINT by providing a collection platform. In addition, the State can buy from CITINT actors the different phases or sub-implementations of the intelligence for different needs (Saini Fasanotti, 2022). State counterintelligence may also benefit from CITINT, for example, when citizens can report suspicious activities such as drone sightings (Lapinkangas and Julkunen, 2022).

Citizen-reported data have gained great importance in today's conflicts, as citizens can provide valuable data to support military, government intelligence, and humanitarian operations (Pešek, 2023, p. 19). In a sense, every photo or video shared on social media can be intelligence data, but it is particularly valuable for images and videos of equipment and operational activities in conflict zones or domains that are targeted in hybrid operations.

Civic intelligence can also have a commercial overlap with government information. Indeed, it is possible that an established OSINT intelligence producer would have government contracts to produce or distribute an intelligence product. This was also alluded to by Petteri Kajanmaa, then Director of the National Defence University, who publicly reported that the National Defence University (Maanpuolustuskorkeakoulu, 2019) was collaborating with the OSINT group Black Bird Group (Kajanmaa, 2022).

Interviewee #1 says that the CITINT group has been holding briefings for politicians and political parties in Finland. It is also easier for decision-makers and authorities to refer openly to intelligence information that the group has gathered from open sources. It is neither secret nor classified, and the group can be cited as the source. Interviewee #1 reminds us that you cannot leak classified information from within an official organization, but you can give the same information collected from outside.

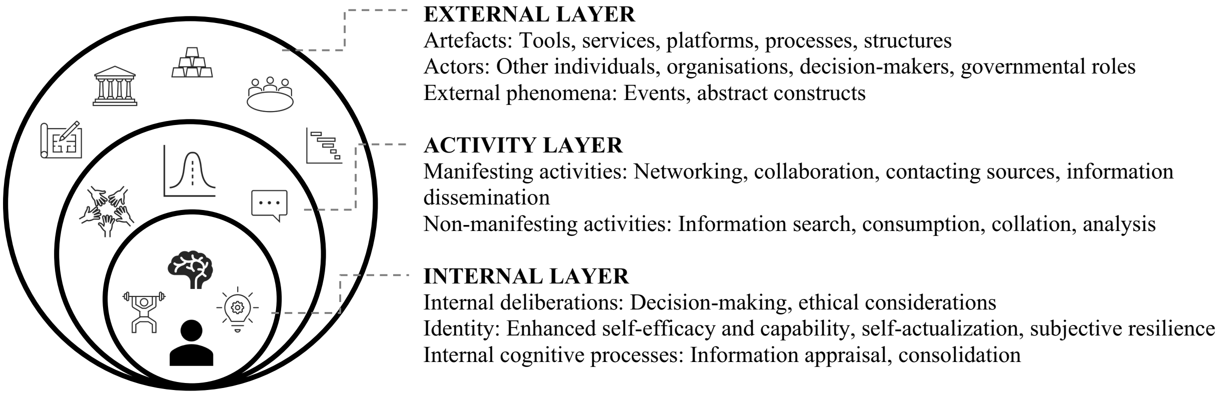

EXTERNAL LAYER
Artefacts: Tools, services, platforms, processes, structures
Actors: Other individuals, organisations, decision-makers, governmental roles
External phenomena: Events, abstract constructs
ACTIVITY LAYER
Manifesting activities: Networking, collaboration, contacting sources, information dissemination
Non-manifesting activities: Information search, consumption, collation, analysis
INTERNAL LAYER
Internal deliberations: Decision-making, ethical considerations
Identity: Enhanced self-efficacy and capability, self-actualization, subjective resilience
Internal cognitive processes: Information appraisal, consolidation

FIGURE 3
Implications of CITINT in the CCSCM framework.

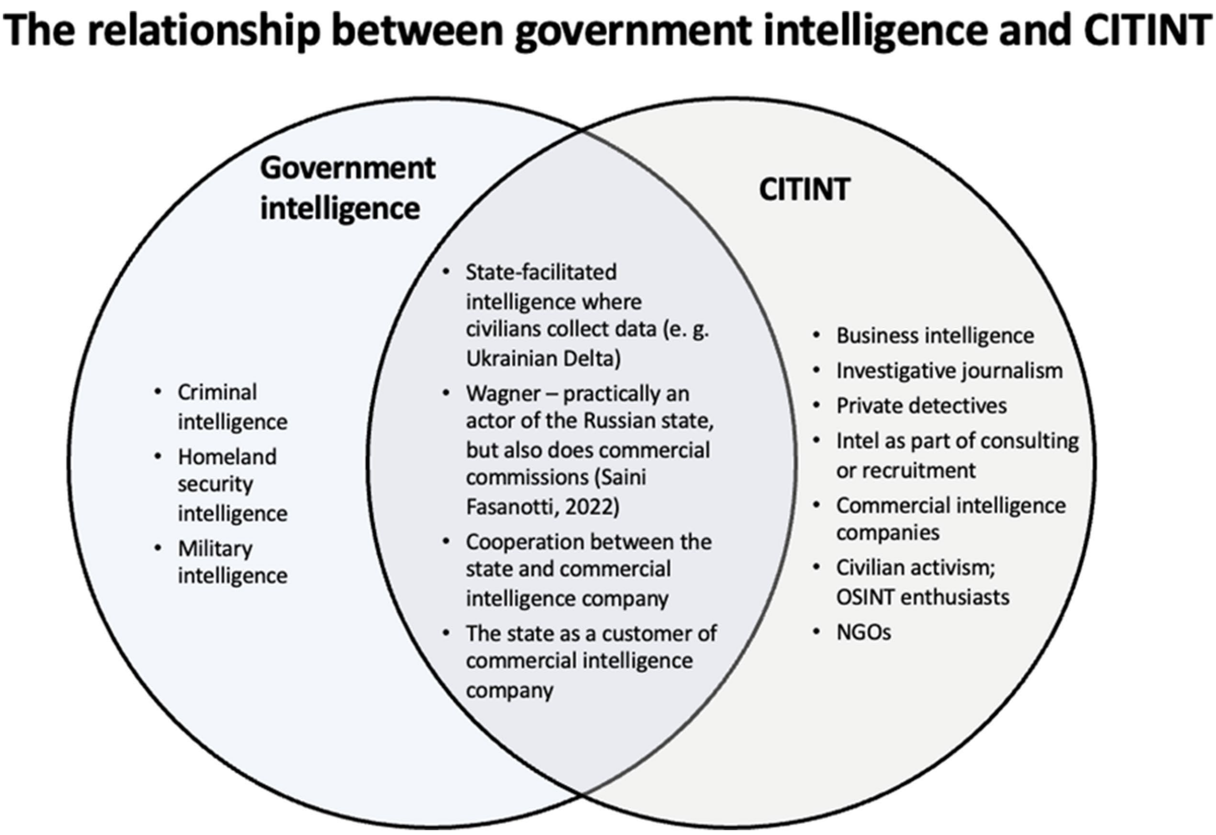

The relationship between government intelligence and CITINT
Government intelligence
CITINT
• Criminal intelligence
• Homeland security intelligence
• Military intelligence
• State-facilitated intelligence where civilians collect data (e. g. Ukrainian Delta)
• Wagner – practically an actor of the Russian state, but also does commercial commissions (Saini Fasanotti, 2022)
• Cooperation between the state and commercial intelligence company
• The state as a customer of commercial intelligence company
• Business intelligence
• Investigative journalism
• Private detectives
• Intel as part of consulting or recruitment
• Commercial intelligence companies
• Civilian activism; OSINT enthusiasts
• NGOs

FIGURE 4
Relationship between government intelligence and CITINT.

One way to try and understand the nature, role, and potential of CITINT is through contextualizing it with related concepts. According to the findings of this review, CITINT often seems to be associated with open-source intelligence (OSINT), situational awareness, and collective knowledge production. Social media tools, platforms, and tools developed by CITINT groups, and governmental tools to facilitate CITINT activities have taken on particular importance for CITINT. These three dimensions are linked to data collection, processing, analytics, and dissemination. Additionally, it is possible to recognize affinity between concepts of CITINT and SOCMINT as outlined by Henrico and Putter (2024) as it emphasizes the possibility of individual citizens trolling various social media platforms for intelligence gathering and dissemination.

In this article, a significant top-level breakdown of CITINT is specifically related to CITINT activities carried out by the individuals on their own initiative, the more organized third sector and NGO CITINT activities, and government-facilitated CITINT activities. Figure 5 shows the interfaces and facilitation platforms between governmental and citizen intelligence activities.

5.3 Further discussion

While many strengths and opportunities have been identified in CITINT, this article also identified challenges and weaknesses. Bringing the information produced by CITINT into, for example, governmental or military situational awareness and decision-making systems is a complex system-level endeavor, moving between several non-coherent and unstructured data sets. It is technically and architecturally challenging to create stable and coherent integrations between systems, even if third-party interfaces can be relied upon in some cases.

Moreover, if the distribution or processing of products at the CITINT operator's end depends on third-party services, problems such as availability and, of course, confidentiality of information may be encountered. The heterogeneity of processes and structures identified between different CITINT organizations and tools also complicates integration. In addition, the user of the information must establish mechanisms for assessing the reliability of the information to be used and pay particular attention to the validation and verification of the information, as there may be vulnerabilities to influence in CITINT. In the Finnish context, the mechanisms related to data confidentiality, clearances, and classification pose their own challenges, so it is necessary to consider how to ensure the correct and timely security classification of and access to the data.

The rapid evolution of CITINT processes and organizations places particular demands on the individual states' legislative work and the definitions contained in international agreements. For example, would a CITINT operator be considered a protected person under Article 4 of the Geneva Convention in its section on civilians? Or do they qualify for the exceptions set out in Article 5, where "[…] a party to the conflict has reasonable grounds to suspect that a particular protected person under this treaty is engaged in an act that endangers the security of the state, or if it is established that he or she is in the act of doing so […]" (Ulkoasiainministeriö, 2015). This reflection is particularly topical, as according to certain

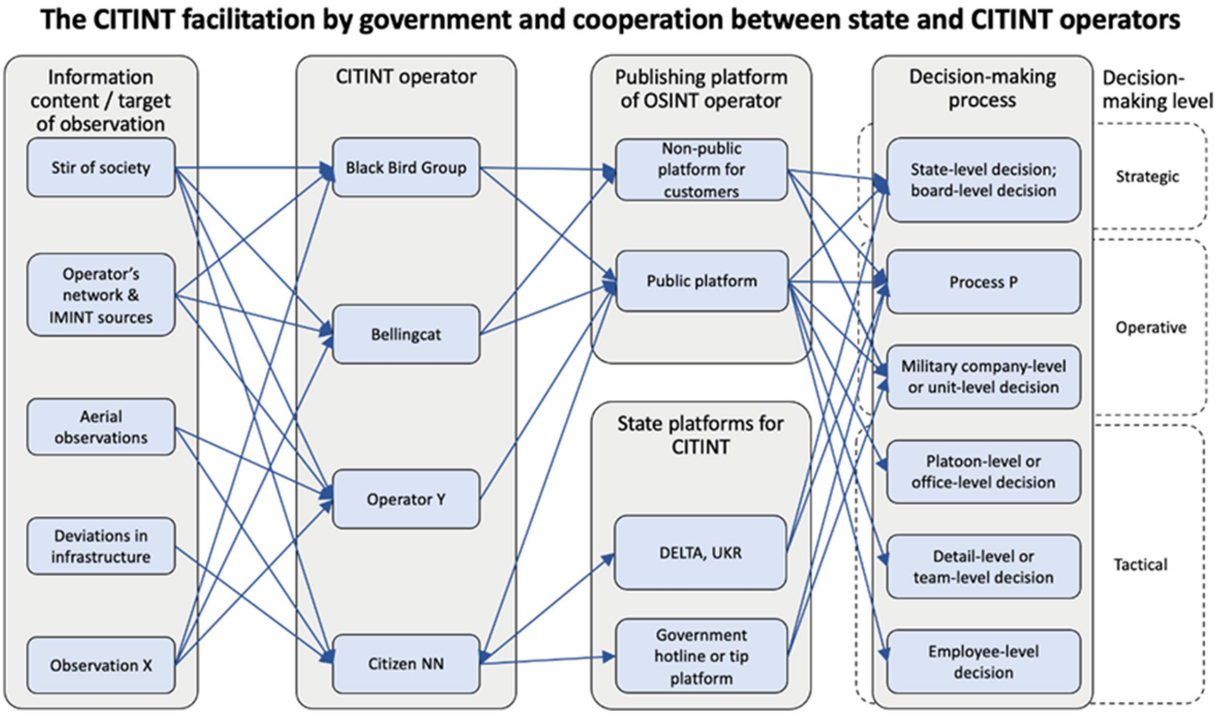

The CITINT facilitation by government and cooperation between state and CITINT operators
Information content / target of observation
Stir of society
Operator's network & IMINT sources
Aerial observations
Deviations in infrastructure
Observation X
CITINT operator
Black Bird Group
Bellingcat
Operator Y
Citizen NN
Publishing platform of OSINT operator
Non-public platform for customers
Public platform
State platforms for CITINT
DELTA, UKR
Government hotline or tip platform
Decision-making process
State-level decision; board-level decision
Process P
Military company-level or unit-level decision
Platoon-level or office-level decision
Detail-level or team-level decision
Employee-level decision
Decision-making level
Strategic
Operative
Tactical

FIGURE 5
Relationship between government intelligence and CITINT. The figure illustrates how actors, platforms, observations, data content, levels of activity, and decision-making processes are interlinked through examples.

interpretations, for example, the Finnish company Iceye can be considered a party to Russia's war of aggression against Ukraine, as it offers the possibility of a significant capability for Ukraine. Russia could thus legitimately target the company's satellites for interference (see, e.g., Nasu, 2022a,b; Court, 2023; Militarnyi, 2023b).

This article has also identified several opportunities and strengths of CITINT. At its best, CITINT can enable very rapid dissemination of information through processes and, on the other hand, dissemination within networks. CITINT may play a key role in promoting openness and accessibility for information used in governmental decision-making. Noteworthy is also the fact that the temporal and geospatial coverage is scalable with the coverage of the networks of CITINT actors. In a good case, data and information on a given phenomenon can be available over a wide area in a dense and rapid manner. Taking CITINT into account in the way organizations operate can also allow for interactivity and even the exploitation of tailored, specific requests for information. Intelligent facilitation of CITINT can also be of national benefit, for example, through increased cohesion and a potential impact on subjectively perceived resilience. Interaction in the facilitation of CITINT takes on its own weight in supporting capabilities.

Tools such as Delta in Ukraine, with its fast update cycle and wide user base, can enable benefits at strategic, operational, and tactical levels. Delta supports the horizontal dissemination of information and the creation of an intact and structured situational picture to support decision-making.

It is likely that both the number of CITINT actors separate from the state and the number of CITINT facilitation by the state will increase as the global political situation becomes more uncertain. This is exacerbated by increasing disinformation and other factors affecting the reliability, integrity, and availability of information. We may also see more and more CITINT in non-governmental professional activities such as recruitment, consultancy, journalism, science, and the security sector.

5.4 Conclusion through revisiting the questions steering this article

5.4.1 How should CITINT be conceptualized and defined?

Many aspects were identified and elaborated. However, explicit dissection of CITINT is challenging due to the high degree of contextuality and dynamic nature of related concepts and processes. This article emphasizes the various non-governmental actors whose relevance in intelligence activities and processes is increasing and certainly do fall within CITINT. Thus, the explicit definition and conceptualization require a broader review and study, including, for instance, conducting interviews among CITINT actors broadly, and conducting thematic, semiotic, and discourse analyses. However, CITINT set in CCSCM framework highlights the various dimensions of CITINT and its affine characteristics with societal participation.

5.4.2 How is CITINT positioned in the overall field of intelligence?

This article outlines differences between the different activities, disciplines, and organizations in intelligence. Basis for addressing CITINT as a separate discipline or sub-area of intelligence are identified and elaborated through the characteristics of processes, actors, and legislative implications. This identification is important, as it provides premises for creating mental models, structures, and mechanisms for how various stakeholders may be able to exploit the capabilities offered by CITINT. In addition, two very different publicly announced tools were briefly introduced to further illustrate the possibilities in CITINT at the practical level. The shift in ownership of intelligence as an issue relates to the positioning of CITINT in the intelligence fields and is elaborated further in the next paragraph.

5.4.3 What are the implications of CITINT in the perspective of societal participation, power relations, and (intelligence-) issue ownership?

Although initial in nature, the especially significant assertion in this article regards the shift in power relations and ownership of intelligence *per se* from governmental and central actors to more fragmented landscape implicated by the increased relevance of intelligence conducted and produced by individuals and NGOs. Furthermore, the identification and designation of two different approaches to CITINT (state-facilitated or top-down, and citizen-conducted or bottom-up) form a key contribution of this article and support future elaborations on the subject. Increasing visibility and number of followers of CITINT organizations in various media, growing recognition of their capabilities, skills, and resources, and utilization of CITINT actors as subcontractors by governmental and commercial organizations reflect the ongoing shift in issue ownership of intelligence from centralized model toward a more divided landscape. This shift should be further studied to support the ethical, legislative, methodological, and educational developments, and to enhance cohesive development.

Indeed, various questions regarding the future landscape in the ownership and power in intelligence activities should be addressed. How do we ensure that intelligence, especially CITINT, is conducted in a fair and lawful manner in the different sectors and in compliance with laws? And how will this development be considered in future legislation? How will the shift in ownership and power in intelligence from governmental actors to individual citizens and NGOs reform and affect the role of intelligence activities in decision-making and administration? How should the decision-making processes be developed so that CITINT may be exploited as an informative component? How should CITINT be facilitated so that it may contribute to constructive factors, such as promotion of experienced resilience and societal self-efficacy? How can we facilitate CITINT to promote cognitive security on all layers of CCSCM? How power relations change as CITINT actors occupy more space and what are the implications? What is the nature of threat vectors due to the ownership change and how can we mitigate them? These questions should be addressed with a broader and deeper literature review with higher structure, as this article is limited in its items included in review, empirical foundation, and analysis structure. Moreover, these questions should be explored through individual and group interviews with various stakeholders, including intelligence professionals, governmental officials and decision-makers, NGOs, and active individuals, to gain better understanding on the various nuances and perspectives of CITINT and its potential.

To conclude, the activities that may be regarded as CITINT are likely to increase from both ends: governmentally and centrally facilitated, and from bottom-up conducted by individuals and NGOs. Moreover, CITINT can be considered as a form of societal participation as outlined by, e.g., Pietilä et al. (2021) and Pietilä (2022) thus promote subjective experience of capability and resilience and perhaps contribute to cognitive security. Especially through these remarks, the implications of CITINT in issue ownership and power relations in intelligence fields may be significant.

Data availability statement

The datasets presented in this article are not readily available because data is interview data and thus not available for distribution. Requests to access the datasets should be directed to iikka.pietilae@gmail.com.

Ethics statement

Ethical approval was not required for the studies involving humans because no attributes outlined by Finnish National Board on Research Integrity (TENK) were identified to require external ethical approval. Participants gave informed consent in writing. Participants were adults. Only data acquired from participants was interview data. The studies were conducted in accordance with the local legislation and institutional requirements. The participants provided their written informed consent to participate in this study. Written informed consent was obtained from the individual(s) for the publication of any potentially identifiable images or data included in this article.

Author contributions

IP: Conceptualization, Data curation, Investigation, Methodology, Project administration, Resources, Supervision, Visualization, Writing – original draft, Writing – review & editing. KK: Conceptualization, Data curation, Investigation, Methodology, Visualization, Writing – original draft, Writing – review & editing. UP: Conceptualization, Investigation, Writing – original draft, Writing – review & editing. MT: Conceptualization, Investigation, Writing – original draft.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Acknowledgments

DeepL Translator (https://www.deepl.com/) has been used for parts of the translation from Finnish to English in this article. Part of this article was produced as coursework in Security and Strategic Intelligence Studies at Jyväskylä University, and the corollary report collection is available at: https://jyx.jyu.fi/handle/123456789/40515. The authors express their gratitude to Jyrki Isokangas for the constructive feedback and thank the reviewers for their support.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Althoff, M. (2015). "Human intelligence" in *The 5 disciplines of intelligence collection*. eds. M. Lowenthal and R. Clark (Los Angeles: CQ Press / Sage) 45–79.

Arthur, P., and Cowell-Meyers, K. (2023). Irish Republican Army. Encyclopaedia Britannica. Available at: https://www.britannica.com/topic/Irish-Republican-Army

Borger, J. (2022). 'Our weapons are computers': Ukrainian coders aim to gain battlefield edge. The Guardian. Available at: https://www.theguardian.com/world/2022/dec/18/our-weapons-are-computers-ukrainian-coders-aim-to-gain-battlefield-edge

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

Collin, P. (2020). Turun 17 vuoden takaisesta arvokuljetusryöstön yrityksestä vaaditaan yli seitsemän vuotta vankeutta – vahvin todiste hanskoista löytynyt DNA. Available at: https://yle.fi/a/3-11200771

Court, E. (2023). Military intelligence: crowdfunded satellite had 'very important role' in Sevastopol attack. The Kyiv Independent. Available at: https://kyivindependent.com/military-intelligence-crowdfunded-satellite-had-very-important-role-in-attack-on-sevastopol/

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Hum. Factors* 37, 32–64. doi: 10.1518/001872095779049543

Esitutkintalaki 805/2011. (2024). Available at: https://www.finlex.fi/fi/laki/ajantasa/2011/20110805

EU. (2021). European convention on human rights. European Court of Human Rights. Available at: https://www.echr.coe.int/documents/d/echr/Convention_ENG

Finder. (n.d.). Iceye Oy. Yrityshakemisto. Available at: https://www.finder.fi/Kaavoitus+ja+maankäytönsuunnittelu/Iceye+Oy/Espoo/yhteystiedot/2927748

Fornusek, M. (2023). Minister: Ukrainian Delta system ready to integrate Western equipment, including F-16 jets. The Kyiv Independent. Available at: https://kyivindependent.com/minister-ukrainian-delta-system-ready-to-integrate-western-equipment-including-f-16/

Ghioni, R., Taddeo, M., and Floridi, L. (2023). Open source intelligence and AI: a systematic review of the GELSI literature. *AI & SOCIETY*. London: Springer.

GIJN (n.d.). Global conferences. Available at: https://gijn.org/global-conferences/

Glaser, B. G., and Strauss, A. L. (1967). *The discovery of grounded theory*. New York: Aldine.

Henrico, S., and Putter, D. (2024). Intelligence collection disciplines—a systematic review. *J. Appl. Secur. Res.* 1-25, 1–25. doi: 10.1080/19361610.2023.2296765

Higgins, E. (2021). *Me olemme Bellingcat — Tiedustelupalvelu verkossa*. Jyväskylä: Docendo.

Hirsjärvi, S., and Hurme, H. (2000). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Helsinki: Gaudeamus.

Iceye (n.d.). Iceye story. Available at: https://www.iceye.com/company.

Inhunt (n.d.). Suorahaku – headhunting. Available at: https://inhunt.fi/suorahaku-headhunting/

Isokangas, J. (2023). *Intelligence studies lecture series*. Jyväskylä: Jyväskylä University.

Järjestyslaki 612/2003 (2022). Available at: https://www.finlex.fi/fi/laki/ajantasa/2003/20030612

Kajanmaa, P. (2022). A tweet by Finnish National Defence University Unit Director regarding collaboration with the Black Bird Group. Available at: https://twitter.com/PutteKaj/status/1502754325994647555?s=20.

Kerttunen, M. (2007). Strategia. Julkaisusarja 3, Strategian asiatietoa, no 4, 2007. Maanpuolustuskorkeakoulu, Strategian laitos. Available at: http://www.urn.fi/URN:NBN:fi-fe201201241125

Lapinkangas, E., and Julkunen, P. (2022). Dronehavaintoja tulee nyt ennätystahtia – toimi näin, jos näet jotain epäilyttävää. Ilta-Sanomat. Available at: https://www.is.fi/kotimaa/art-2000009152128.html

Laulajainen, A., Taivalmaa, A., Vilén, T., and Virtanen, M. (2023). Valtiollisen tiedustelumonopolin murtuminen. Teoksessa J. Isokangas (toim.), Tiedustelun maailma: Muuttuva tiedustelu. Tiedusteluanalyysi I -kurssin raportteja (s. 9–24). Informaatioteknologian tiedekunnan julkaisuja, 98. Jyväskylän yliopisto. Available at: https://jyx.jyu.fi/bitstream/handle/123456789/86797/1/Tiedustelun%20maailma%20-%20Muuttuva%20tiedustelu.pdf#page=9

Lowenthal, M., and Clark, R. (2015). *The 5 disciplines of intelligence collection*. Los Angeles: CQ Press / Sage.

Lozovenko, T. (2023). *Ukraine's Delta system passes NATO tests and can integrate F-16s*. Kiev: Ukrainska Pravda.

Maanpuolustuskorkeakoulu (2019). Kadettikoulutuksen mahdollistajat. Kolumni. Available at: https://maanpuolustuskorkeakoulu.fi/-/kadettikoulutuksen-mahdollistajat

Mäki-Kuhna, J. (2023). *Intelligence lecture series*. Jyväskylä: University of Jyväskylä.

Malkki, L. (2014). Toisen terroristi, toisen vapaustaistelija – Terrorismin määrittelyn ongelmat. *Vihatkoot kunhan pelkaavat. Nakokulmia terrorismiin ilmiona*. eds. A. Paronen and O. Teirilä (Helsinki: Maanpuolustuskorkeakoulu) (pp. 15–42).

McDowell, D. (2008). *Strategic intelligence: a handbook for practitioners, managers, and users*, vol. *5*. Maryland: Scarecrow Press / Rowman & Littlefield.

Meriläinen, N. (2014). *Understanding the framing of issues in multi-actor arenas: power relations in the human rights debate*. Jyväskylä: University of Jyväskylä.

Militarnyi (2022). Ukraine unveiled its own Delta situational awareness system. Available at: https://mil.in.ua/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system/

Militarnyi (2023a). The defense forces of Ukraine to introduce the Delta system. Available at: https://mil.in.ua/en/news/the-defense-forces-of-ukraine-to-introduce-the-delta-system/

Militarnyi (2023b). Ukrainian intelligence showcases images from ICEYE satellite, funded by local donations. Available at: https://mil.in.ua/en/news/ukrainian-intelligence-showcases-images-from-iceye-satellite-funded-by-local-donations/

Mitrovich, G. (2016). Theorizing citizen learning of open source intelligence as tradecraft training. Available at: https://www.proquest.com/openview/bcb13358b8e1775f077d51abab09395b

Moher, D., Liberati, A., Tetzla?, J., Altman, D. G., and PRISMA Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Informaatioteknologian tiedekunnan julkaisuja, 98. Jyväskylän yliopisto. *PLoS Med*. 6:e1000097. Available at: https://pubmed.ncbi.nlm.nih.gov/19621072/

Nasu, H. (2022a). *Targeting a satellite: contrasting considerations between the jus ad bellum and the jus in Bello. International law studies*, vol. 99 2022, s. 143–177. Newport: U.S. Naval War College / Stockton Center for International Law.

Nasu, H. (2022b). "The eye in space": Iceye's SAR satellites and the law of war. Lieber Institute, West Point: Articles of war. Available at: https://lieber.westpoint.edu/eye-space-iceyes-sar-satellites-law-of-war/

Nelliyullathil, M. (2020). Teaching open source intelligence (OSINT) journalism: strategies and priorities. *Commun. J. Res.* (Calicut: The University of Calicut) 9, 61–73.

Oktay, J. S. (2012). Grounded theory. *Pocket guides to social work research methods*. Oxford: Oxford University Press.

p1ngul1n0 (2023). Blackbird. An OSINT tool to search fast for accounts by across 581 sites. Available at: https://github.com/p1ngul1n0/blackbird/blob/main/README.md

Paasonen, J. (2023). Yksityisetsivätoiminnan huomioiminen lainsäädännön kehittämisessä. Blog post. Available at: https://jyripaasonen.fi/yksityisetsivatoiminnan-huomioiminen-lainsaadannon-kehittamisessa/

Perustuslaki 731/1999. (2018). Available at: https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Pešek, K. (2023). *Komparativni připadove studie: využiti občanskeho zpravodajstvi (CITINT) během probihajiciho konfliktu na Ukrajině v porovnani s vybranymi soudobymi konflikty. Master's thesis*. Brno: Masaryk University, Faculty of Social Studies.

Pietilä, I. (2022). *Studies of digital solutions supporting societal participation of youths*. Doctoral dissertation. Tampere: Tampere University.

Pietilä, I., Meriläinen, N., Varsaluoma, J., and Väänänen, K. (2021). *Citizen-centric socio-cognitive model for societal participation. Short paper. EGOV2021 – IFIP EGOV-CeDEM-EPART 2021 conference and in proceedings of ongoing research, practitioners, posters, workshops, and projects at EGOV-CeDEM-ePart 2021 co-located with the IFIP WG 8.5 international conference EGOV-CeDEM-ePart 2021*. Aachen: CEUR workshop proceedings / RWTH Aachen University.

Poliisi (2023). KRP tutkii epäiltyä turvallisuussalaisuuden paljastamista - kolmea vaaditaan vangittavaksi. Available at: https://poliisi.fi/-/krp-tutkii-epailtya-turvallisuussalaisuuden-paljastamista-kolmea-vaaditaan-vangittavaksi

Puolustusvoimat (n.d.). Puolustusvoimien tiedustelulaitos. Available at: https://puolustusvoimat.fi/tietoa-meista/tiedustelulaitos

Putter, D., and Henrico, S. (2022). Social media intelligence: the national security-privacy nexus. *Sci. Militaria S. Afr. J. Milit. Stud.* 50, 19–44. doi: 10.5787/50-1-1345

Rikoslaki 39/1889 (2024). Available at: https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Saini Fasanotti, F. (2022). Russia's Wagner Group in Africa: influence, commercial concessions, rights violations, and counterinsurgency failure. Available at: https://www.brookings.edu/articles/russias-wagner-group-in-africa-influence-commercial-concessions-rights-violations-and-counterinsurgency-failure/

Scott, B. (2023). "Everyone freaks out when the leaks are made": data leaks, investigative journalism and intelligence practice. Available at: https://www.emerald.com/insight/content/doi/10.1108/JFC-05-2023-0123/full/pdf?title=everyone-freaks-out-when-the-leaks-are-made-data-leaks-investigative-journalism-and-intelligence-practice

Sisäministeriö (2017). Siviilitiedustelun ja suojelupoliisin ohjauksen kehittäminen sisäministeriön hallinnonalalla – työryhmän raportti. Available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80032/Siviilitiedustelun%20ja%20suojelupoliisin%20ohjaus_NETTI.pdf?sequence=1&isAllowed=y

Soeiro, L. (2023). BlackBird — Osint Tool. Medium.com. Available at: https://lucassoeiro.medium.com/blackbird-osint-tool-c1ed8a88c7aa.

Steele, R. D. (2002). *The new craft of intelligence: achieving asymmetric advantage in the face of nontraditional threats*. Pennsylvania: Strategic Studies Institute, US Army War College.

Suojelupoliisi (n.d.). Supon tehtävät selkokielellä. Available at: https://supo.fi/supon-tehtavat-selkokielella

SYL. (n.d.-a). Etusivu. Available at: https://www.yksityisetsiva.fi/

SYL. (n.d.-b). Eettiset säännöt. Available at: https://www.yksityisetsiva.fi/?page_id=207

Teti, A. (2012). Intelligence of the third millennium – the 'citizen intelligence'. Gnosis 4/2012. Agenzia Informazioni e Sicurezza Interna. Available at: https://gnosis.aisi.gov.it/

Tietosuojalaki 1050/2018 (2024). Available at: https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Tilastokeskus (n.d.). Toimialaluokitus 2008. Available at: https://www2.tilastokeskus.fi/fi/luokitukset/toimiala/

Tutkivan journalismin yhdistys (2011). Yhdistyksen säännöt. Available at: https://www.tutkiva.fi/wp-content/uploads/2023/05/YhdistyksenSaannot.pdf

Tutkivan journalismin yhdistys (2023). Tutki!2023 puhujat. Available at: https://tutkikonferenssi.fi/puhujat/

Ulkoasiainministeriö (2015). Sodan oikeussäännöt. Available at: https://um.fi/documents/35732/48132/julkaisu__sodan_oikeussäännöt

Vähätalo, E. (2019). Jyväskylän kybermaistereilla riittää kysyntää. Ruotuväki-lehti. Available at: https://ruotuvaki.fi/-/jyvaskylan-kybermaistereilla-riittaa-kysyntaa

Vapa, M. (2023). Marko Vapa Youtube channel. Youtube video was removed. Available at: https://www.youtube.com/watch?v=JiVfAFcuP9w

Walton, A. (2013). Financial intelligence: uses and teaching methods (innovative approaches from subject matter experts). Available at: https://www.jstor.org/stable/10.2307/26485084