ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Military Situation Awareness: Ukrainian Experience

Viktor Putrenko | EPAM School of Digital Technology, American University Kyiv, Ukraine | ORCID: 0000-0002-0239-9241

Nataliia Pashynska | Taras Shevchenko Kyiv National University, Ukraine | ORCID: 0000-0002-0133-688X

Received: 23.11.2023

Accepted: 20.04.2024

Published: 17.07.2024

Cite this article as:
V. Putrenko,
N. Pashynska "Military situation awareness: Ukrainian experience," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190341

Corresponding author:
Viktor Putrenko, EPAM School of Digital Technology, American University Kyiv, Ukraine.
E-Mail: putrenko10@gmail.com;
00000-0002-0239-9241

Abstract

Situational awareness (SA) has become one of the key concepts in military sector. The Russian-Ukrainian war led to the development of information technology in Ukraine to manage troops and combat situations. The army was supported by numerous volunteer initiatives involving IT professionals. As a result, Ukrainian army has received modern software solutions based on the principles of SA for use in real combat conditions. The purpose of the study is to analyse the development of military and civilian SA information systems during the war between Russia and Ukraine. In the course of the study, the methods of system analysis of the problem of SA were used. The research classifies information solutions, assesses the distribution of products by different classification sectors, and conducts a strengths, weaknesses, opportunities, and threats (SWOT) analysis of the developed products. Using the example of the most common solutions, the main features of existing software products and the technologies on which they operate were identified. Prospects for the development of solutions, their contribution to military management, and problematic issues are identified.

Keywords

situational awareness, network-centric warfare, information technology, Ukraine

1. Introduction

One of the results of the war between Russia and Ukraine was the rapid growth of information technology in Ukrainian army. The main reason of this process is the need to gain an advantage over the enemy on the battlefield and in planning relevant operations. In addition to purely military components, it also includes security aspects of the management of territorial bodies that carry out regional and local governance, informing the population about the existing military and other types of hazards.

In this regard, it becomes relevant to study the formation of the most common approaches to the organisation of information interaction at the military and civilian levels based on the approaches of situational awareness (SA) and the concept of network-centric warfare (NCW). Since 2014, Ukraine has been actively developing technologies related to the information and telecommunications complex, the creation of unmanned systems, and the development of situation centres for the needs of the military sector. The joint use of the latest and updated types of weapons and these technologies allows the military to perform tasks at a new level of efficiency. Analysing this experience is important in terms of developing new approaches to military management and the use of information technology.

The goal of the study is to analyse the development of military and civilian situational awareness information systems (SAIS) during the war between Russia and Ukraine.

The objectives of the study are to analyse current trends in the development of the concept of SA, peculiarities of the use of SA tools during the war between Russia and Ukraine, trends and results of the development of information tools for SA in Ukraine, and to assess further prospects for the development of SA systems in modern wars.

In the course of the study, the methods of system analysis of SA problem based on the classification and typification of software development for military purposes were used. A conceptual modelling of the structure of the SA information system development on the basis of structural and graphical models was carried out. Separately, a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of the prospects for the development of the SA information system in Ukraine was carried out. Based on the results of the analysis, perspective and problematic areas in the development of systems were identified. The characteristics of the existing developments are built and they are divided depending on the scope of military tasks and development prospects on the basis of a comparative analysis.

2. Theoretical Aspect of Situational Awareness

Situational awareness is a model of situational judgement. One of the most famous researchers in this field is Mika Endsley [1], who formed the following definition: ‘SA is the perception of elements and events of the environment in relation to time or space, understanding their meaning and projecting their status in the near future’.

The purpose of SA is to actively detect and analyse information relevant to immediate operational stability and safety and to coordinate such information across the organisation to ensure that all organisational units are operating within a common operating view.

Situational awareness enables the operator to understand the operating environment of critical services and the environment that affects their performance. This understanding provides stakeholders with a reasonably accurate and relevant understanding of the past, current, and foreseeable future state of such services and supports effective decision-making in the context of the overall operating environment.

Situational awareness process establishes a common operating picture by collecting, fusing, and analysing data to support automated or human decision-making when responding to incidents. Such data must necessarily be communicated in a timely manner and in a form that allows a human to understand quickly the key elements needed to make right decisions.

The overall operational picture needs to be accurate and actionable (suitable for decision support and action). However, different participants in the process need different and not necessarily complete knowledge of the operational environment. Depending on how it is presented, a complete picture may contain too much information and overwhelm the decision-maker. Operators should also not be provided with a big amount of data. Rather, operators should only see what is important, as determined by the risk strategy and the overall risk pattern.

We present the model for SA and associated decision-making. Figure 1 depicts SA and dynamic decision-making model that

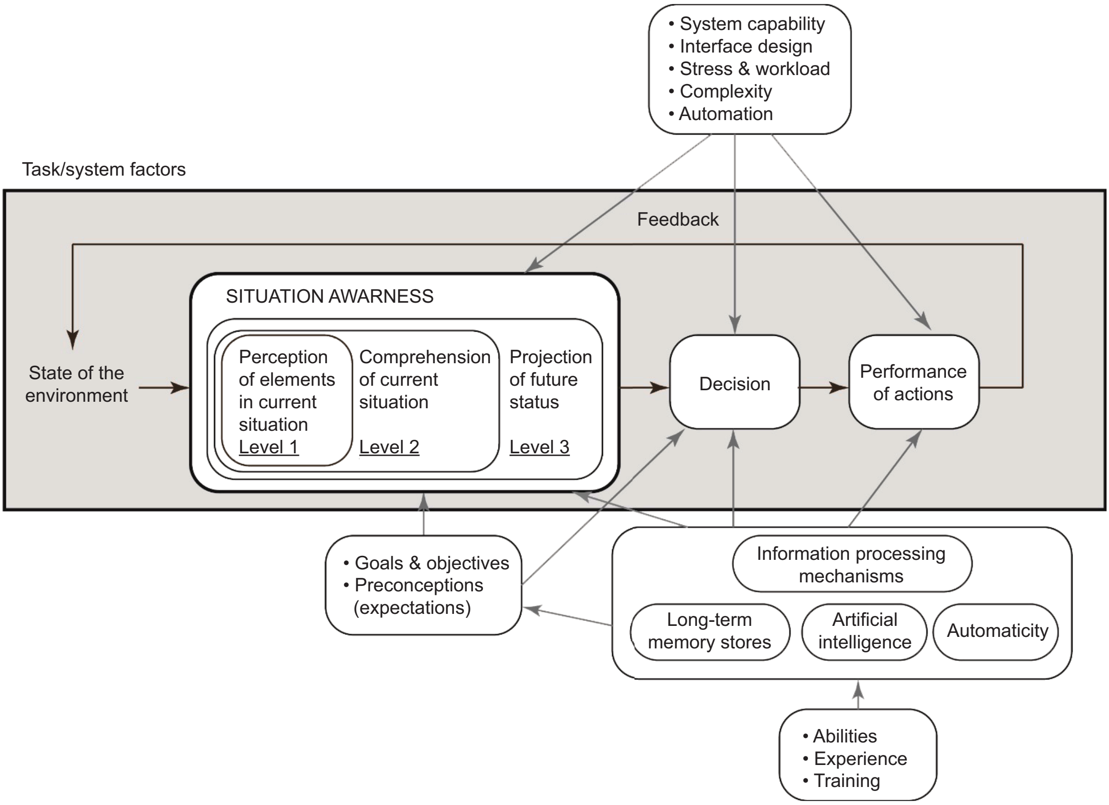

Figure 1. Modified Endsley's model of situation awareness.

has been inspired from Endsley's model of SA [1], which has been widely adopted. The model has an SA core whereas sensing and decision-making elements are built around the SA core. A multitude of sensors sense the environment to acquire the state of the environment. The sensed information is fused together to remove the redundancies in the sensed data, such as multiple similar views captured by different cameras or quantities sensed by different sensors in close locality, and also to overcome the shortcomings of the data acquired from a single source, such as occlusions, change in ambient lighting conditions, and/or chaotic elements in the environment. The fused data is then passed to the SA core, which comprises three levels or stages [2, 3].

Perception – Level 1 SA: The first stage of attaining SA is the perception of the status, attributes, and dynamics of the entities in the surroundings. For instance, an operator needs to discern important entities in the environment, such as other aircraft, terrain, and warning lights along with their pertinent characteristics [4].

Comprehension – Level 2 SA: The second stage of SA is the comprehension of the situation, which is based on the integration of disconnected level 1 SA elements. The level 2 SA is a step further than just being aware of elements in the environment as it deals with developing an understanding of the significance of those elements in relation to an operator's objectives. Concisely, we can state the level 2 of SA as understanding of entities in the surroundings, in particular when integrated together, in connection to the operator's objectives. For instance, an operator must understand the significance of the perceived elements in relation to each other. An amateur operator may be able to attain the same level 1 SA as more experienced ones, but may flounder to assimilate the perceived elements along with relevant goals to comprehend the situation fully (level 2 SA) [5].

Projection – Level 3 SA: The third level of SA relates to the ability to project the future actions of entities in the environment at least in the near term. This projection is achieved based on the cognisance of status and dynamics of elements in the environment and comprehension of the situation. Succinctly, we can state level 3 of SA as prediction or estimation of the status of entities in the surroundings in the future, at least in the near future. For example, from the perceived and comprehended information, the experienced operators predict possible future events (level 3 SA), which provides them knowledge and time to determine the most befitting course of action to achieve their objectives [6, 7].

As shown in Figure 2, the SA core also receives input from the commanders at strategic or operational levels regarding goals or objectives of SA. Our model enhances the SA model from Endsley [8] for perception, comprehension, and projection by adding support for artificial intelligence (AI)-assisted decision-making and resource management. Perception is addressed through the standard information fusion and resource management loop.

Owing to the recent advancements in AI, it has become an integral part of SA core and dynamic decision-making. AI assists operators in comprehending the situation (level 2 SA) and then making projections about the future actions of entities in the environment (level 3 SA). Thus, both robustness of AI models and operators' ability, experience, and training determine the level of comprehension acquired by the operators and the accuracy of future projections. Based on the acquired comprehension and projection, decisions are recommended by AI models to the commanders and then the commanders make appropriate decisions taking into account the

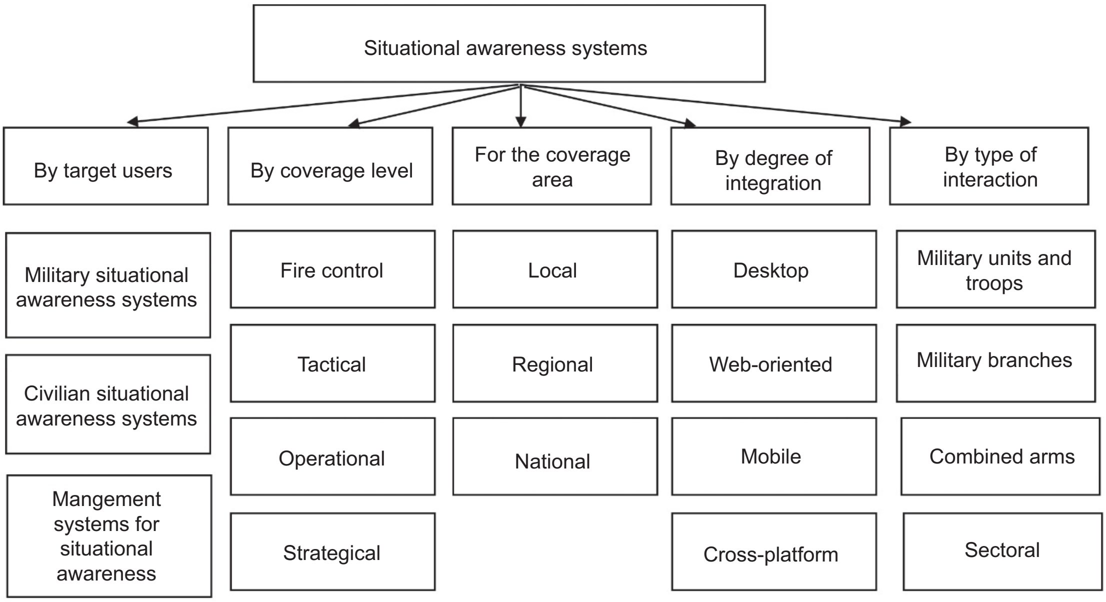

Figure 2. SAIS classification.

input from AI and the assessed situation. Finally, the decisions are implemented at tactical level by operators. The decisions to be implemented have a vast range, including, for example, the positioning of personnel and equipment, firing of weapons, medical evacuation, and logistics support [9, 10].

Situational awareness (and the operational situation as its component) are functions of time and can be represented as follows:

$$CO(t) \leq OO(t), M >,$$

CO(t) – situational awareness for a period of time *t*;

OO(t) – operational situation for a period of time *t*;

M – mental model.

The concept of ‘situational awareness’ in the context of military component analysis is very closely related to the concept of NCW [9].

The definition of NCW can be found in [11]:

> NCW is about human and organisational behaviour. At the heart of the concept of NCW is the adoption of a new

> way of thinking, network-centric and its application in military operations. The NCW concept focuses on the combat power that can be gained as a result of the network integration of military formations engaged in combat operations or the organisation of effective communication between them [12]. It is characterised by the ability of geographically dispersed forces (consisting of individual units) to create a high level of common battle space awareness that can be used through self-synchronisation and other network-centric operations to achieve the command's intent.

The definition of NCW is further elaborated on by the key concepts given in the same paper [13, 14]: 'The use of a geographically dispersed force; a high degree of awareness between the units involved in the warfare; effective communication'. Additional information about the content of the concept is provided by the basic principles of NCW (basic tenets), formulated in [15, 16]:

1. Reliable networking improves information exchange.
2. Information sharing and cooperation improve information quality and SA.
3. General SA allows for self-synchronisation.
4. Increasing the effectiveness of the mission.

3. Analysis of Ukrainian Situational Awareness Information Systems

3.1. Approaches to Classification of Situational Awareness System

The basis for analysing SAIS is a basic classification of the existing solutions in Ukraine and its comparison with international practice.

Situational awareness information systems can be classified by target users, level and geographical scope of coverage, degree of integration with information and communication platforms, and type of interaction based on them (Figure 2).

According to the general concept of military operations management and approaches to SAIS, there are four levels of information interaction at the appropriate level of coverage, which correspond to the respective classes of software and communication systems. These levels include the level of fire control on the battlefield, tactical, operational, and strategic (intelligence) levels (Figure 3). These levels are characterised by different spatial and temporal resolution

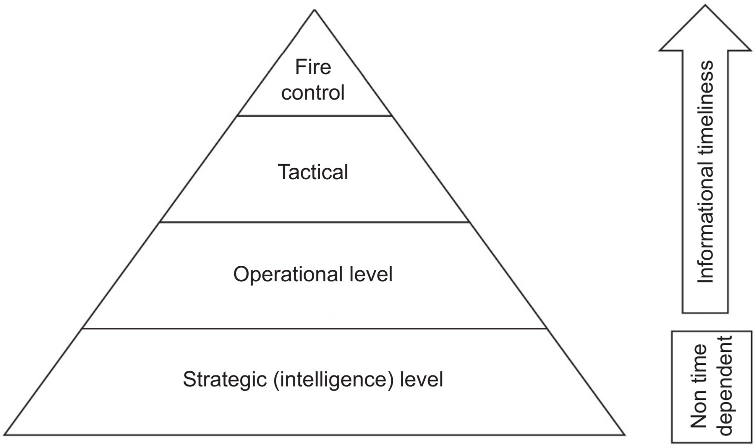

Figure 3. Levels of military control based on SAIS.

of data and the ways and methods of processing them. The speed of response to events is rapidly increasing at the fire control level, and the greatest coverage of information is important at strategic level [17].

Depending on use at different levels of combat management, the existing software solutions in the field of SAIS used in Ukrainian army were classified. Table 1 shows that in each category there are information systems and solutions that complement and compete with each other in some way. Most of these solutions are volunteer developments that are at different stages of obtaining documents for official use in the army. However, all of them are already widely used in combat operations [18].

The review of these software solutions allows us to conduct a SWOT analysis of this product segment and identify relevant priorities in its development, prospects, and problems (Table 2). SWOT analysis (or SWOT matrix) is a strategic planning and strategic management technique used to help a person or organisation identify strengths, weaknesses, opportunities, and threats related to business competition or project planning.

The results of SWOT analysis show that the greatest advantage in the development of information systems at different levels of SA is the availability of significant IT potential in Ukraine and motivated developers. A certain decentralisation of activities in the development of SAIS for the military sector gave a significant boost to the formation of a volunteer movement of software development teams. Most of these teams began to form after 2014 and

Table 1. SAIS solutions in Ukrainian army.

System class	Name	Functionalities	Year of development start
Fire Control	'Bronia'	Calculation for artillery firing, terrain orientation	2015
	MilChat	Messaging, broadcasting geo-positions	2018
Tactical level	Ukrop (MyGun)	Calculation for artillery firing and terrain orientation	2009
	'Terminal'	Tactical situation and orientation	2015
Operational level	GISArta	Calculation for artillery firing, targeting, and operations planning	2014
	Kropiva	Calculation for artillery firing and orientation	2014
Strategic level	ComBat Vision	Intelligence, targeting, and decision support	2015
	Delta	Orientation, data exchange, and departmental management	2016
	'Dzvin-AC'	Command and control of combat operations at the command level	2016
	'Virash-planshet'	Gathering, displaying, and analysing air traffic information	2016
	'Prostir'	Management of troops and weapons at the brigade level	2021

Table 2. SWOT analysis of Ukrainian SAIS.

Strengths	Weaknesses
• Modern technological base of development • Integration with NATO-standard data transfer protocols and services • Testing in real-war conditions • Strengthening cyber defence	• Weak communication base in Ukraine • Need to combine different means and forces in combat conditions • Public–private partnership base for development
Opportunities	**Threats**
• Export of technologies • Involvement of professional specialists and teamwork • Attracting external sources of funding • Testing of modern technologies	• Lack of stable sources of funding • Changing conditions for project development as a result of hostilities • Conflict situations with military (state) structures • Subversive activities, cyber attacks on infrastructure

their activities intensified after the outbreak of full-scale war. The teams involved highly qualified specialists. Therefore, the existing software solutions have found a large number of users and are improved constantly. This creates preconditions for the development of software solutions that are competitive not only in Ukraine but may have export potential. Weaknesses include the fact that software solutions are developed mostly autonomously, which means that they are highly dependent on donations for the needs of volunteer teams, and do not coordinate with or compete with other software products. Therefore, the biggest threat is that software developers may face various organisational difficulties, and without systemic support, the results of their work may be lost.

Weaknesses include the fact that software solutions are mostly developed autonomously, which means that they are highly dependent on donations for the needs of volunteer teams and do not coordinate with other software products. Therefore, the biggest threat is that software developers may face various organisational difficulties, and without systemic support, the results of their work may be lost [19].

3.2. Examples of the Most Used Systems

3.2.1. Delta Situational Awareness System

Delta is a system for collecting, processing, and displaying information about enemy forces, coordinating defence forces, and providing SA in accordance with North Atlantic Treaty Organization (NATO) standards, developed by the Defence Technology Innovation and Development Centre of the Ministry of Defence of Ukraine.

Delta is used by very different units. It is a tool for multi-domain operations. This system is used by army, navy, and air defence. Each branch of the armed forces has its own needs and tasks in using Delta.

The Delta system integrates information about the location of enemy forces and assets and allows real-time tracking of the position of enemy troops and promptly recording detected objects for their further fire damage [20]. The system integrates information about the enemy on a digital map, with data taken from various sources: satellite imagery providers, radars, sensors, Global Positioning System (GPS) trackers, and radio intercepts. Users can see what is happening on land, at sea, in the air, in space, and in cyberspace. The system can run on any device: laptop, tablet, or mobile phone. The Delta system was used during well-known operation, such as the defeat of the cruiser Moskva and the liberation of Zmeinyi Island.

The system is used to plan operations and combat operations. The secure ELEMENT messenger, which is part of Delta, is used to coordinate between units and exchange information securely. Delta's platform and services are built to NATO standards, support the Multilateral Interoperability Programme (MIP) specification and allow for NCW. The system is compatible with similar solutions used by the armies of NATO member states [21]. The system was presented during the NATO Tide Sprint event.

Delta is a cloud-based solution and is already implementing NATO standards and the latest industry trends, such as cloud native environment, zero trust security, and multi-domain operations. In NATO member states, such solutions are only at the stage of experimental implementation.

Detla supplants the Soviet principle of information transfer, when an intelligence officer from the grassroots passed information about the enemy to the military leadership. The leadership would make decisions and send them down the chain of command. Such a long path of information slows down the army, and if the command post is destroyed, the possibility of coordination is lost.

In June 2023, Poland hosted the annual NATO CWIX exercise on interoperability of national combat and information systems with NATO systems and protocols. From 18 to 22 June 2023, specialists from the A2724 military unit, as part of a delegation from the Communications Troops of the Armed Forces of Ukraine (J6), tested the Delta Integration Platform for interoperability with similar NATO systems using the state-of-the-art MIP4-IES protocol at the NATO CWIX international exercise in Poland. Currently, only seven out of 28 NATO countries have implemented this protocol and can have all its benefits. Ukraine is among those states that have confirmed the ability to exchange situational information using the modern military exchange protocol. This also gives Ukraine the ability to automatically exchange information with NATO member states during joint exercises and missions. The main protocol tested in 2023 is Link 16. It enables data to be transmitted to Delta from F-16 fighter jets [22].

It is important that the systems on the market are interoperable, and that their developers consider the importance of interoperability at the stage of product development. Delta is just such a system that can exchange data with software solutions from NATO countries. The system interacts with NATO battlefield management systems and operates in accordance with these information exchange protocols [23].

At its core, it is an integration platform designed to ensure that data from various sensors and systems can be collected correctly, and that the Delta user can exchange this information. For example, Delta integrates chatbots developed by the Ministry of Digital Transformation – eVorog and the Security Service of Ukraine – STOP Russian War.

The system is equipped with modern tools for monitoring suspicious activity. Since 2021, allied cyber units have been continuously checking the system for vulnerabilities, unauthorised intrusion attempts, data leaks, etc.

The system is constantly under enemy attack of varying intensity and scale. Separate teams of Russians have been assigned to ‘put down’ Delta.

Delta developers are constantly learning from the scale of a major war. The priority is to strengthen the system’s security. In August 2022, Russians launched a phishing attack on Delta and gained access to two accounts.

For a long time, Delta hid the system from being indexed by search robots so that there were no links to the login page when searching on Google. Hackers faked the resource and raised it in search queries. One of the users took advantage of it and gave their accounts to a phishing site.

The users had access to a limited amount of information about enemy forces in certain areas. The hackers managed to make a recording, but they did not receive complete information about the system’s architecture.

Users are checked according to the Security Service of Ukraine protocol, and employees undergo a polygraph. The system has protocols for recognising patterns of suspicious behaviour. Cyber specialists monitor security at all levels – from development to use – 24×7.

Now the developers are faced with the task of providing Fast Identity Online Alliance (FIDO) security keys to all users of the Delta SA system. This is a two-factor authentication tool for accessing various systems and applications. The security key is used in addition to the password as the second factor of user verification. The key is supported by major operating systems and browsers. FIDO is an association of leading technology companies, government agencies, service providers, financial institutions, and payment systems that promotes the development, use, and compliance with authentication standards. The FIDO Alliance has more than 250 members, including such leading companies as Microsoft, Google, Apple, Amazon, Facebook, Mastercard, American Express, VISA, and PayPal. FIDO protocols use standard public-key cryptography methods to ensure stronger authentication. When registering with an online service, the user's client device creates a new key pair. It stores the private key and registers the public key with the online service. Authentication is performed by the client device, which confirms that it owns the private key by signing the call [24].

Semantic data integration takes place on the basis of a mapping framework that displays different data sources. For example, it can be automatic marking when information is taken from sensors in a war zone. Some layers are filled with marks manually: they confirm the information received, for example, about the location of enemy troops, verify it, and give a certain number of participants access to the corresponding layer. The symbols on the map correspond to NATO standards.

After Ukraine's victory, there will be a big question of maintaining the Delta data set, which is a huge resource. This could lead to the corporatisation of the product.

The Delta system has the following export potential:

- compatible with NATO systems,
- hosted in a secure cloud,
- supports integration of different data sources and sensors,
- adapted to the needs of specific types of troops.

In parallel, in 2016, the Ministry of Defence of Ukraine ordered another development from a third-party contractor – Dzvin, a de jure competitor to Delta. Ukrainian army needs a common automated operational-level system for command headquarters to ensure that the troops are covered by the command. The Ministry of Defence tested Dzvin, which was supposed to solve this problem, but the project was frozen in 2021. Prototypes were developed and tested, but encountered bureaucratic obstacles related to the cost of development, time, and product ownership.

It also started to engage foreign companies. The Ministry of Digital Transformation engaged the developer Palantir. The US company with a capitalisation of $16.6 billion has contracts with the CIA, and the US and British defence departments. In Ukraine, Palantir will work with the Ministry of Defence and the General Staff to provide

SAIS of various levels. They help to process and combine information from satellites, drones, and other sources, and make faster decisions.

The functions of Delta in Russia are partially performed by the Acacia-M system, but it is more focused on troop management than on frontline awareness. The Russian Ministry of Defence spent RUB (₽)20 billion ($318 million) to purchase 32 sets of the Acacia-M mobile troop management system in 2018. It is supposed to collect information from other systems for different branches of the armed forces and speed up decision-making at operational and tactical levels.

3.2.2. Operation System Kropyva

The Kropyva tactical command and control system is a software for creating intelligent maps in combination with devices and instruments designed to plan and guide missions. It was developed by Logika Design Bureau LLC, a member of the League of Defence Enterprises of Ukraine.

The development, integration, and testing of the system began in 2014 at the beginning of Russia's war against Ukraine as a volunteer project, when a group of developers from the Army SOS volunteer organisation began supplying tablets to armed forces. Between 2014 and 2023, 10,000 units of software were installed, and a technical and software support service was set up [25].

The system provides:

- access to an digital map of the area with your own GPS position,
- data exchange with other system subscribers. Data generally includes positions of allied units, coordinates of detected targets, and short text messages,
- solving individual calculation tasks, such as calculating the march, fire area, or artillery corrections,
- ensuring the interaction and transfer of data from reconnaissance assets: unmanned aerial vehicles (UAVs), radar, and sonar systems in an automatic mode.

Equipment required to use the system:

- tablet computer with GPS,
- drone,
- radio station,
- binoculars,
- laser rangefinder,
- thermal imager.

The Kropyva system is used by 90–95% of artillerymen. Kropyva is also used by the Land Forces of the Armed Forces of Ukraine – armoured vehicles, infantry or reconnaissance units, etc. Because of the development, the time to deploy an artillery battery is reduced by fivefold, the time to hit an unplanned target is reduced by almost threefold, and the time to open counter-battery fire is reduced by tenfold, compared to Soviet calculators.

The Kropyva system is an Android application that enters the coordinates of an enemy target, which is received by the nearest artillery battery, which then strikes.

In the course of development, the application has been updated with additional functionality. It updates geometric information about the front line on a daily basis. Soldiers can see where the enemy is and where they are, exchange positions and intelligence, and communicate with the command post. It also includes a navigator, a map with accurate elevations, the distance from one object to another, and the calculation of the range of a gun to an object.

The data from Kropyva is not stored centrally on servers to be streamed to all devices. Each tablet has information only on the positions and weapons it needs.

3.2.3. Bronia System

Bronia is the system that allows firing without a direct line of sight to the enemy. It is used by armoured troops.

When a tank enters a firing position, it has to determine its orientation. This data is transmitted to the platoon commander, who enters it into a tablet application. The parameters of the shells are also entered there and meteorological data is automatically analysed.

The firing positions are calculated at the command post for several tanks simultaneously. For example, for three tanks, this takes 5–7 min, and manually without application, it takes 20–25 min. The commander transmits two parameters of the azimuth pointer and the lateral level to the crew for firing.

The programmers have provided the ability to switch from satellite maps to the general staff maps while retaining information about the targets. The general staff maps show not only that it is a particular road but also the width of the roadway and its surface.

All volunteer solutions were developed on a bottom-up basis, responding quickly to the needs of the military.

3.3. The Situation Centre in the Structure of SAIS

An important component of SA during a military conflict is decision-making based on situational centres. ‘Aerorozvidka’ unit is developing situational centres that provide SA for all representatives of the security and defence sector at all levels. They are implementing the intelligence, surveillance, target acquisition and reconnaissance (ISTAR) process in Ukrainian army, which has been introduced in NATO countries since the 1990s.

The situation centre is a technological hub that integrates and coordinates intelligence assets and helps to conduct effectively joint operations. Based on this information, headquarters can plan operations much more efficiently, including joint operations involving different units and even agencies. Sharing intelligence assets helps to optimise the resources available to the security and defence forces.

The first situation centre was set up in Kyiv within days of the start of the full-scale invasion. Interacting with the civil–military administration of Kyiv, the situation centre team formed a comprehensive overview of the condition of the city’s infrastructure and the region. Coordination was also established between checkpoints and patrols to avoid conflicts over the use of UAVs and the movement of crews near the location of Ukrainian units [26].

The information gathered was used to plan the actions of defenders, establish effective cooperation between different units, and form an operational picture for the leadership of the Ministry of Defence and the military–civilian administration of Kyiv (Figure 4).

Currently, there are eight situation centres in Ukraine; each collects information on its own area of the frontline. The situation centres

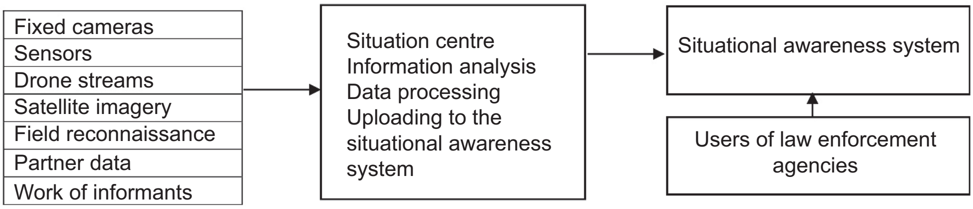

Figure 4. Data analysis model based on the situation centre [27].

are located in Kyiv, Mykolaiv, Kherson, Zaporizhzhia, Kryvyi Rih, Kharkiv, Sumy, Chernihiv, and Donbas. Waging NCW, in which the main advantage over the enemy is achieved in the information component, allows for faster operations, faster management, and greater effectiveness in defeating enemy forces. SA in the context of modern threats is the basis of security, which makes it possible to respond quickly to changes in the situation and have an advantage over the enemy, even with fewer forces and means.

NATO's security system includes the Situation Information Centre (NATO: SITCEN), which provides SA during times of peace, tension, and crisis as well as during strategic exercises. SITCEN receives, processes, and disseminates data from all available internal and external resources. The system also acts as a link to similar facilities in Allied countries and NATO's high command. SITCEN was founded in 1968, but has since been restructured several times to adapt to the demands of the times. Through its various divisions, the centre operates around the clock and provides information to the Alliance's leadership to ensure informed decision-making.

SITCEN Watch provides NATO headquarters with round-the-clock SA of incidents and events around the world. The staff consists of a team of officers and assistants who are on duty in 12-h shifts, 24 h a day, 7 days a week. They monitor and disseminate information and intelligence on the international, political, economic, and military situations, including developments that could affect the Alliance. Watch alerts the relevant military or civilian authorities at headquarters to important developments identified from both covert and open sources.

SITCEN Watch also monitors NATO's ballistic missile early warning systems, supports crisis management organisations and task forces, and assists the NATO security management office in its missions abroad.

The geospatial division provides integrated geographic services to NATO headquarters across land, sea, air, and space. This can range from rapid mapping to providing the most up-to-date overall operational picture. The division also manages geoportals on various networks to build training scenarios during exercises.

The Situational Awareness Integration Team (SAIT), established in March 2020, is dedicated to developing a comprehensive shared understanding of the global and regional security environment and its impact on the Alliance, NATO Allies, and partners. The team contributes to SA by pooling knowledge and expertise and analysing current topics and issues relevant to the Alliance's interests and missions. Among its many tasks, it prepares, coordinates, and hosts the chiefs of staff meeting, which brings together senior officials from NATO headquarters.

The situational awareness integration team also conducts qualitative and quantitative research and brings together stakeholders from across NATO member states. For its research and coordination work, it uses and applies the latest developments in information science.

3.4. Communication Infrastructure

Effective use of the SAIS should not have been possible without the provision of communication infrastructure on the front line. In Ukrainian army, the deployed Starlink system played such a role.

Starlink is a broadband satellite-enabled Internet developed by SpaceX, which makes Ukrainian forces independent from fibre optic cables or mobile networks vulnerable to Russian attack. Currently, there are approximately 20,000 Starlink terminals in Ukraine, most of which are funded by western support [17]. The terminals are crucial for their ability to conduct NCW in Ukraine.

The critical characteristic of Starlink is that its satellite-based design is more resilient towards jamming than regular radio signals. Furthermore, owing to quick installation time, approximately 15 min, Ukrainian forces can maintain a high level of communication without relying on Internet cables. Therefore, access to Starlink hardware is crucial to enhance and sustain Ukrainian NCW capability through the Delta system. In addition, drones use Starlink to keep connected when Ukraine lacks Internet and power because of Russian artillery targeting its critical infrastructure.

As the system highly depends on western support, there is a reason to assume that NATO countries are interested in its operational capability to counter Russian threats.

3.5. Civilian Component of Military Situational Awareness

Since the outbreak of the war, civic initiatives to interactively inform the public about military operations and warn of air threats have developed actively. A number of web and mobile applications are made available to the public to provide SA to the population. Many information elements are implemented in these applications for the first time for civilian purposes. These applications include DeepStateMap.Live, alerts.in.ua, and the mobile applications eTrivoga, AirAlert, and Povitriana trivoga.

3.5.1 Project DeepStateMap.Live [28].

Based on non-profit OpenStreetMaps, DeepStateMap.Live is an interactive online map of the fighting in Ukraine that allows you to follow the changes in the front line and the course of hostilities in the Russian-Ukrainian war. In the spring of 2023, the company launched its own app for Android and IOS.

The map has the following conventional symbols:

- territory de-occupied in the last 2 weeks – blue,
- de-occupied territory – green,
- territory that requires clarification – grey,
- territory captured by Russian troops – red,
- territory of the occupied Crimea and ORDLO – dark red,
- territories of other states occupied by Russia – light pink,
- enemy unit – a unit icon according to NATO standards or a 'pig' icon,
- enemy headquarters – the icon of enemy headquarters according to NATO standards or the icon of a tent,
- enemy airfields – an icon of an airfield according to NATO standards or an airfield icon,
- directions of enemy attacks – a red arrow.

You can view the map in different formats. Available map formats are:

- standard,
- topographic,
- satellite.

It is possible to enable the display of fire points based on data from the National Aeronautics and Space Administration (NASA) firms system and compare them with the front line.

Owing to a special mode, it is possible to measure the range of various artillery systems: HIMARS, M777, CAESAR, etc. along the entire front line. A special mathematical modelling of the force of a nuclear explosion of different masses across the map is developed.

The map has a ruler for determining the distance between points in metres. It is possible to build a broken line, which is calculated in total between all points. If the line is closed, you can calculate the area of the created shape. The radiation monitoring points have been added to the map in partnership with SaveDnipro. The application shows enemy fortifications available in open sources since 16 June 2023 [29].

Owing to cooperation with Griselda, an automated military data processing system, on 13 November 2022, the Patogen functionality was launched, which shows modified data on the concentration of enemy numbers along all front lines for civilians, based on classified data. Cooperation with the Griselda system also affects the accuracy of front line mapping, as it allows teams to share operational data. There is a table showing the percentage of liberated and occupied territories since the beginning of the invasion.

There is a closed map functionality for access only to military, with a map of enemy trenches and the ability to calculate azimuth. Since 1 June 2023, regular users have been able to locate their location. A publicly available weather viewer was added on 9 November 2023.

The map of application is widely quoted and used to visualise the fighting in Ukrainian and international media.

3.5.2. Alerts.in.ua

Alerts.in.ua is an online service that visualises information about air alerts and other threats on the map of Ukraine [30].

The main part of the site is a map of Ukraine, which highlights in real time the regions where air alerts or other threats are declared.

The application supports five types of threats:

- air raid alert,
- threat of shelling,
- threat of street fighting,
- chemical threat,
- radiation threat.

Additionally, information about shelling and other dangerous events, such as explosions, demining is published on the basis of media reports.

The service uses the following information sources by default:

1. The official Air Alert Telegram channel from Ajax Systems, which reports airborne alarms and other threats.
2. Official Telegram channels of regional military administrations, public broadcasting, the state emergency service, and their specialised channels for alerting about alarms at the regional level.
3. Official air alert map.
4. Official Telegram channel of the Air Force of Ukraine.

Most of civilian applications are volunteer developments that, if popular, are actively supported by the state government. These apps aggregate data and transform information into a user-friendly form based on cross-platform developments. In parallel, official state channels operate for informing about the situation. Mobile operators support push notifications from the state emergency service of Ukraine. However, government services are often not customer-oriented. Therefore, citizens prefer to use volunteer apps with better interface design and easier usage.

3.6. Cartographic Support

The main basis for the tasks of military and civilian SA is an up-to-date cartographic basis and the use of geographic information systems. Since 2014, Ukraine has been updating the topographic mapping of the eastern regions based on the USC-2000 coordinate system.

With the outbreak of war in 2022, the Ukrainian army faced a shortage of its own mapping data for the northern part of Ukraine. The use of NATO standards in Ukrainian army has led to a transition to using coordinate systems for military cartography based on the WGS-84 coordinate system. Most volunteer projects use open data sources based on non-commercial OpenStreetMaps.

The lack of Ukraine's own satellite remote sensing data on the territory of Ukraine remains a problem. In particular, an attempt was made to lease a radar satellite from the Finnish company ICEYE to obtain intelligence data. The data operator was the Defence Intelligence of Ukraine. The status of use of this data is currently unknown. Ukraine's dependence on external sources of high-resolution satellite data complicates the development of SAIS. This is offset by the active use of reconnaissance UAVs of various types at the frontline.

4. Conclusions

During the Russian-Ukrainian war, there was an urgent need to develop various information systems to support SA at different levels of military and civilian management. This has led to the appearance of many volunteer initiatives and the development of state military systems for managing troops. Given the high level of development of the IT sector in Ukraine and the unprecedented scale of military conflict, many solutions in the SA sector have become pioneering and visionary for the military of other countries. In particular, the use of modern web and mobile technologies based on cloud infrastructures, accompanied by advanced encryption and cyber security methods, has become the basis of technological solutions for real-time data exchange.

The second trend was the construction of systems based on NATO standards and the need for effective interaction with the systems, tools, and data warehouses of the Alliance. In Ukrainian army, SAIS are developed at different levels of command and control and include the integration of data from UAVs, satellite imagery, cartography, field data, and intelligence results. SAIS are classified according to four levels of military command: fire control, tactical, operational, and strategic levels. According to their purpose, SAIS are classified by target users, level and geographical dimension of coverage, degree of integration with information and communication platforms, and type of interaction based on them.

The results of the SWOT analysis of software development show a high potential for the development of the existing systems in Ukraine. At the same time, most existing projects are at risk because they do not have ongoing government support. Duplication of work by volunteer teams that do not have joint development management remains a problem.

To date, the most promising systems developed have been Kropyva at the operational and tactical level and Delta at the strategic management level.

A separate mention should be made of civilian initiatives to ensure public awareness, which are divided into military situation monitoring systems and rapid air raid response systems.

Perspective areas for the development of SAIS include standardisation and unification with NATO standards, improving cyber defence and reliability of the systems. The use of systems in real-world combat operations significantly improves their quality of development and creates conditions for further exchange of experience and export of technologies in this area.

The further development of SA systems in Ukraine is to integrate the existing systems, organise an ecosystem of military information systems with the ability to exchange data through secure channels, and a high level of cyber security. From a technological point of view, the development of SAIS is focused on the use of AI tools, big data processing algorithms, methods of forecasting and scenario modelling of changes in the situation [31], and joint processing of ground-based, airborne, maritime, and space-based information sources. From an organisational perspective, products in this segment are aimed at unification and standardisation based on NATO approaches. The process of public–private partnerships continues in this technology sector. There is a high probability that software and solution developers are structured to form vertically integrated structures that may include weapon developers, IT companies, innovation centres, and start-up incubators.

References

[1] M.R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1, pp. 32–64, 1995, doi: 10.1518/001872095779049543.

[2] M.R. Endsley, "Situation awareness in aviation systems," in *Handbook of aviation human factors*, D.J. Garland, J.A. Wise, V.D. Hopkin, Eds., Mahwah, NJ: Lawrence Erlbaum, 1999, pp. 257–276.

[3] M. Endsley. (2001). "Designing for Situation Awareness in Complex System." Proceedings of the Second International Workshop on the symbiosis of humans, artifacts and environment. Kyoto, Japan. [Online]. Available: https://www.researchgate.net/profile/Mica-Endsley/publication/238653506_Designing_for_situation_awareness_in_complex_system/links/542b1ada0cf29bbc126a7f35/Designing-for-situation-awareness-in-complex-system.pdf. [Accessed: Jan. 02, 2024].

[4] A. Munir, A. Aved, E. Blasch, "Situational awareness: Techniques, challenges, and prospects," *AI,* vol. *3*, no. 1, pp. 55–77, 2022, doi: 10.3390/ai3010005.

[5] *Handbook of dynamic data driven applications systems,* E. Blasch, S. Ravela, A. Aved. Eds., Berlin: Springer Cham, 2018.

[6] C. Paul, C.P. Clarke, B.L. Triezenberg, D. Manheim, B. Wilson, *Improving C2 and situational awareness for operations in and through the information environment*. Santa Monica, CA: RAND Corporation, 2018. [Online]. Available: https://www.rand.org/pubs/research_reports/RR2489.html. [Accessed: Jan. 02, 2024].

[7] N.A. Stanton, P. Chambers, J. Piggott, "Situational awareness and safety," *Safety Science*, vol. 39, pp. 189–204, 2001, doi: 10.1016/S0925-7535(01)00010-8.

[8] D. Alberts, R.E. Hayes, *Power to the edge: Command, control, in the information age*. Washington, DC: Command and Control Research Program (CCRP), 2005.

[9] D. Reid, G. Goodman, W. Johnson, R. Giffin, "All that glisters: Is network-centric warfare really scientific?," *Defense and Security Analysis*, vol. 21, no. 4, pp. 335–367, 2005, doi: 10.1080/1475179052000345403.

[10] D. Alberts, J. Garstka, F. Stein, *Network centric warfare: Developing and leveraging information superiority*. Washington, DC: Command and Control Research Program (CCRP), 1999.

[11] V. Garg, T. Wickramarathne. (Nov. 4–7, 2018). "Ubiquitous sensing for enhanced road situational awareness: A target-tracking approach." Proceedings of the 21st international conference on intelligent transportation systems (ITSC), Maui, HI, pp. 831–836. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8569918. [Accessed: Jan. 02, 2024].

[12] M.R. Endsley, "The divergence of objective and subjective situation awareness: A meta-analysis," *Journal of Cognitive Engineering and Decision Making*, vol. 14, pp. 34–53, 2020, doi: 10.1177/1555343419874248.

[13] G. Tadda. (Jun. 30–Jul. 3, 2008). "Measuring performance of cyber situation awareness systems." Proceedings of the 2008 11th international conference on information fusion, Cologne, Germany, pp. 1–8.

[14] W.L. Brandão, M.S. Pinho. (Mar. 18–22, 2017). "Using augmented reality to improve dismounted operators' situation awareness." Proceedings of the IEEE annual international symposium on virtual reality (VR), Los Angeles, CA, USA, pp. 297–298.

[15] J. Lundberg, "Situation awareness systems, states and processes: A holistic framework," *Theoretical Issues in Ergonomics Science*, vol. 16, no. 5, pp. 447–473, 2015, doi: 10.1080/1463922X.2015.1008601.

[16] N. Suri., M. Tortonesi, J. Michaelis, P. Budulas, G. Benincasa, S. Russell, C. Stefanelli, R. Winkler. (May 23–24, 2016). "Analyzing the applicability of internet of things to the battlefield environment." Proceedings of the international conference on military communications and information systems (ICMCIS), Brussels, Belgium, doi: 10.1109/ICMCIS.2016.7496574.

[17] R. Oscar. (Feb. 03, 2023). *Network-centric warfare in Ukraine: The delta system*. [Online]. Available: https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system. [Accessed: Jan. 02, 2024].

[18] T. Melnyk. (Feb. 04, 2023). *Delta military software is now officially in the Ukrainian armed forces. It helped in all major operations – from the sinking of the Moskva to the liberation of Zmiine. Why it is faster to fight with it.* [Online]. Available: https://forbes.ua/innovations/twitter-dlya-zsu-viyskoviy-soft-delta-dopomagav-u-vsikh-velikikh-operatsiyakh-vid-potoplennya-moskvi-do-zvilnennya-zmiinogo-chomu-z-nim-zsu-voyuyut-shvidshe-07122022-10318. [Accessed: Jan. 02, 2024].

[19] T. Melnyk. (Nov. 14, 2022). *IT chaos in the service of the armed forces. Hundreds of thousands of military personnel use various software developed by volunteers. Is such decentralisation dangerous?* [Online]. Available: https://forbes.ua/innovations/it-khaos-na-sluzhbi-zsu-sotni-tisyach-viyskovikh-koristuyutsya-riznim-softom-yakiy-rozrobili-volonteri-chi-nebezpechna-taka-detsentralizatsiya-14112022-9700. [Accessed: Jan. 02, 2024].

[20] F. Yura. (Jun. 14, 2023). *How the Delta software works and why the offline approach does not work in the army – An interview with the head of IT at Aerial Intelligence.* [Online]. Available: https://dou.ua/lenta/interviews/delta-and-it-in-the-army. [Accessed: Jan. 02, 2024].

[21] Militarnyi. (Oct. 27, 2022). *Ukraine unveiled its own Delta situational awareness system*. [Online]. Available: https://mil.in.ua/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system. [Accessed: Jan. 02, 2024].

[22] ArmyInform. (Jul. 12. 2023). *Ukraine's Delta situational awareness system passes NATO tests and can integrate F-16 fighters.* [Online]. Available: https://armyinform.com.ua/2023/07/12/ukrayinska-systema-sytuaczijnoyi-obiznanosti-delta-projshla-vyprobuvannya-nato-i-mozhe-integruvaty-vynyshhuvachi-f-16. [Accessed: Jan. 02, 2024].

[23] J.M. Pullen, S. Carey, U. Schade, O.M. Mevassvik, S. Galan, L. Khimeche, S. Godoy, M. Powers, N. Cordonnier, N. de Reus, N. LeGrand. (Feb. 11, 2008). *NATO MSG048 coalition battle management initial demonstration lessons learned and way forward*. [Online]. Available: https://repository.tno.nl/SingleDoc?find=UID%20 59169081-fa5c-4d0e-a46c-64ac3eaaaf13. [Accessed: Jan. 02, 2024].

[24] Ukrinform. (Apr. 04, 2023). *The armed forces of Ukraine told how the military uses the Delta platform.* [Online]. Available: https://www.ukrinform.ua/rubric-ato/3731063-u-zsu-rozpovili-ak-vijskovi-vikoristovuut-platformu-delta.html. [Accessed: Jan. 02, 2024].

[25] T. Melnyk. (Jul. 24, 2023). *Stinging Nettle. How Ukrainian software for artillerymen affects the course of the war*. [Online]. Available: https://forbes.ua/innovations/zhalyucha-kropiva-yak-ukrainske-programne-zabezpechennya-dlya-artileristiv-vplivae-na-khid-viyni-22072022-7054. [Accessed: Jan. 02, 2024].

[26] Ukrainska Pravda. (Sep. 24, 2015). *Innovations for the army. Bronia programme for tankers*. [Online]. Available: https://life.pravda.com.ua/volunteers/2015/09/24/200649. [Accessed: Jan. 02, 2024].

[27] Aerorozvidka NGO. (Jul. 11, 2024). *Unmanned aerial vehicles, situational awareness,* cybersecurity. [Online]. Available: https://aerorozvidka.ngo. [Accessed: Jan. 02, 2024].

[28] DeepStateMap.Live. (Mar. 12, 2023). *Map of military operations*. Available: https://deepstatemap.live. [Accessed: Jan. 02, 2024].

[29] SaveEcoBot. (Jun. 16, 2023). *Radiological maps in Ukraine online*. Available: https://www.saveecobot.com/en/radiation-maps. [Accessed: Jan. 02, 2024].

[30] Alerts.in.ua. (Mar. 18, 2023). *Map of trivog Ukraine*. Available: https://alerts.in.ua. [Accessed: Jan. 02, 2024].

[31] V. Putrenko, N. Pashynska, "Analysis of regional armed conflicts using spatial clustering methods," *Lecture Notes in Information Sciences*, vol. 9, pp. 67–73, 2020.