Safety & Defense 9(1) (2023)
DOI: https://doi.org 10.37105/sd.198

Defense and deterrence as the foundation of the a2/ad system in smart city air defense

Marian KOPCZEWSKI
marian.kopczewski@awl.edu.pl
https://orcid.org/0000-0002-0402-0477
Military University of Land Forces, Poland

Zbigniew GROBELNY
zbigniew.grobelny@awl.edu.pl (Corresponding author)
https://orcid.org/000-0002-6743-7632
Military University of Land Forces, Poland

Norbert ŚWIĘTOCHOWSKI
norbert.swietochowski@awl.edu.pl
https://orcid.org/0000-0001-6582-9694
Military University of Land Forces, Poland,

Received: 14 June 2023 | Revised: 17 August 2022
Accepted: 21 August 2022 | Available online: 18 September 2022

Abstract

Extreme concentration of tangible and non-tangible resources in the environment of the Smart City calls for their securing and protection. In the case of threat emergence, the military would have to enter areas where local authorities cannot guarantee the security of Smart City assets. Thus, the question arises whether or not Smart Cities could potentially assist the military forces in performing their tasks better on the battlefield. Some military agencies are currently exploring the possibility of using the military in Smart Cities. For instance, the United States Army Research Laboratory (ARL) is studying whether smart city communications and infrastructure could be of use on the future battlefield.

This paper aims to indicate the potential for expansion and integration of the anti-aircraft defense systems to serve the needs of urban defense, thereby allowing the achievement of air superiority and implementing the assumptions of A2/AD systems. In reference to the research objective formulated in such a way, discovering the answers to the following questions was deemed crucial: What is the state of the current Anti-Aircraft Defense (AAD) system of urban centers, in particular Smart Cities? What are the possibilities of expanding and improving this system? How can the SMART CITY system be integrated and serve as an element of strengthening the AAD system?

In order to answer the indicated questions, this article was written with the use of qualitative method consisting of text and literature exploratory research and analysis, and comparative analyzes of Smart Cities and Air Defense in contemporary military operations. To achieve the assumed aim, the authors have also conducted the evaluation of Air Defense combat capabilities, as well as the changes that have occurred in the environment of Smart Cities. The authors used thematic analysis methods to interpret patterns and meanings in the data

Keywords: cities, Smart City, threats, combat, A2/AD systems, air defense.

Safety & Defense 9(1) (2023)
DOI: https://doi.org 10.37105/sd.198

1. Introduction

Security environments are becoming increasingly more complex and multidimensional, while the dynamics of the processes occurring in that space have simultaneously accelerated considerably in recent years. It appears that in order to plan and execute operations effectively, commanders and staff officers must step outside the domain of strictly military knowledge. They need to understand geopolitical, macroeconomic and social phenomena and adapt to dynamic technology changes. It is a fairly sizeable catalogue of challenges. Therefore, it is necessary to observe emerging changes and the military need to discern a broader horizon beyond the map, plans or orders. The problem is that it is relatively easy to notice rapid changes, while the identification of slow, long-term processes is difficult to grasp. Hence, it becomes necessary to conduct an intelligent observation of the surrounding world and interpret even the most subtle or barely noticeable signals coming from the surroundings. This, in turn, is not feasible without a sense of curiosity about the world and an aggressive search for knowledge and information, which is accessible through, among others, artificial intelligence (AI), and the so-called Smart City related to it. Cities around the world are transforming to respond to the challenges associated with the habitation of enormous populations in limited space. Currently, around the world, there are 29 cities with a population exceeding 10 million people. According to Gartner Inc., this number will have increased to 43 by 2030. It is very likely that a vast majority of future armed conflicts will take place in large cities (Pradhan, 2020).

From a military point of view, cities are of great importance (Zieliński, et al., 2018). They provide support for military units. Due to the administrative and industrial centers located there, they may constitute areas of particular importance for the enemy. Combat in urban areas can take place on three levels: on the street level, below the street level and above the ground. The urban area is one of the most difficult for all armed forces to operate. The largest agglomerations are becoming an increasingly complex and disorientating combination of multiple entities with shifting alliances, in which the military may be forced to operate in a serious conflict, such as the one in Ukraine, as well as conduct peacekeeping and humanitarian operations. The lessons learned from the recent armed conflicts and the continuous development of air assault assets necessitate the possession of effective systems for counteracting the danger coming from airborne assault/missile attack systems, aircraft, unmanned platforms, etc.

Such assault capability is limited to the maximum by the anti-aircraft component used as part of the A2/AD concept – anti-access and area denial, the structure of which, depending on the threats, may vary and include various types of anti-aircraft systems, whose development and deployment aims to achieve advantage or at least balance military capabilities in a given area.

The conflict in Ukraine shows that on the battlefield, quality – understood as organization and efficiency of functioning – is more important than quantity, assuming, obviously, that the quantitative disproportion is within reason. For what is mounted on a platform or what it carries holds more importance than the platform itself.

This paper aims to indicate the potential for expansion and integration of the anti-aircraft defense systems to serve the needs of urban defense, thereby allowing the achievement of air superiority and implementing the assumptions of A2/AD systems. With reference to the research objective formulated in such a way, discovering the answers to the following questions was deemed crucial: What is the state of the current Anti-Aircraft Defense (AAD) system of urban centers, and Smart Cities in particular? What are the possibilities of expanding and improving this system? How can the SMART CITY system be integrated and serve as an element of strengthening the AAD system, the most important element of which is the network-centric command system of the US Army, also implemented in the Polish Armed Forces (PAF), IAMD Battle Command System (IBCS)?

In order to answer the indicated questions, this article was written using the qualitative method consisting of text and literature exploratory research and analysis, and comparative analyses of Smart Cities and Air Defense in contemporary military operations. To achieve the assumed aim, the authors have also conducted an evaluation of Air Defense combat capabilities and the changes that have occurred in the environment of Smart Cities. The authors used thematic analysis methods to interpret patterns and meanings in the data.

2. Smart City in context of military operations

Intelligent transport, GPS, public, commercial and private vehicle monitoring, traffic light management, city monitoring, environment monitoring, smart buildings, online shopping, remote medical consultations, education, e-media, social networks, autonomous vehicles and ICT – almost every area of life and economy has its mirror image in the electronic sphere (Cocchia, 2014). By 2025, more than 80% of cities are expected to have achieve smart status, and all known reports indicate that people increasingly often relocate to cities (Gawkowski, 2019). In modern urban centers, traffic congestion, air pollution, water and energy consumption, and even parking lot lighting are monitored. At the same time, surveillance cameras and drones monitor the streets, and mobile transmitters and GPS systems record the location of both people and objects. All these interconnected systems create a new city model, the so-called Smart City. Thus, the Smart City is an urban center leveraging information and communication technologies to increase the interactivity and efficiency of urban infrastructure and all its components, as well as to raise the awareness of its residents (Stawasz & Sikora-Fernandez, 2015; Dameri, 2013).

Safety & Defense 9(1) (2023)
DOI: https://doi.org 10.37105/sd.198

The prerequisite for the development of smart technology is efficient telecommunication devices linking individual appliances. The global Internet, which has been developing for several decades now, combines billions of devices, creating the so-called Internet of Things (IoT), i.e., a system of electronic devices which can automatically communicate and exchange data over the network without human intervention (Michalski &Bernat 2019).

One of the most important technologies of Smart Cities is the LoRaWAN Internet network. It is an extensive, narrowband long-distance network capable of transmitting data in two directions from 0.3 kbps to 50 kbps. It is an ideal solution for transmitting smaller quantities of data, e.g., from various sensors located across the city, which do not require continuous transmission. Creating an entire urban LoRaWAN network is much cheaper than constructing traditional networks due to much lower costs of devices and the use of unlicensed radio frequencies that do not require expensive permits. LoRaWAN is also characterized by a very long range: in practice, up to several kilometers in built-up areas, and even up to several kilometers in open areas. Currently, e.g., in Wrocław, there are four base stations for the LoRaWAN urban network, but there are plans to launch more.

A smart parking system is another component of the Smart City. The aim of the project which has been implemented for more than two years, is to identify an optimal solution that will allow for identifying available parking spaces, offer convenient parking options and make this data available to drivers. Among others, solutions based on visual detection using HD cameras and magneto-optical sensors based on LoRaWAN communication are undergoing testing.

The Smart Trip is another program within the Smart City. The project is based on the analysis of transport resources, including roads, parking lots, car rentals, bicycles and trams. The use of these resources is expected to be optimized. In the advanced version, based on travelers' preferences, this tool is designed to assist in choosing not only the right means of transport and convenient route, but also reduce travel costs and facilitate payments.

The Intelligent Transport System is another component of the Smart City program. The system records data from road control and measurement devices (e.g., cameras, stop boards) and public transport, then performs its processing and makes it available to traffic participants. Information points provide passengers with real-time information about the arrival of buses and trams. Based on the data from the system, it is possible to adjust traffic lights in order to optimize traffic flow. By analyzing these and other materials, we can ask the following question: Why should the military possess knowledge and learn to use the Smart City? A better understanding of smart cities will result in improved situational awareness, improved operational assessments and the identification of opportunities to lead and execute impact operations (Braszko, 2023).

Undoubtedly, the military would be able to use the capabilities of the Long Range Wide Area Network (LoRaWAN). It is a popular network protocol used in smart cities, which connects large implementations of Internet of Things (IoT) devices over long distances.

In any type of urban military operation, possessing information is a rudimentary requirement. The military must have a Common Operational Picture (COP) in order to respond quickly to changes in tactical situations. Data from multiple Smart City sensors could be used to generate tactical maps as well as continuously and dynamically track blue and red power.

The widespread use of online communication equipment is no longer limited to phones and computers. Other everyday objects and devices are starting to be increasingly connected to each other via the IoT and will leverage widespread and ongoing data collection in order to provide information about both machine processes and the processes of human decision-making (Bogan & Feeney, 2019). Civilian IoT devices used in smart cities, including laptops, tablets, mobile phones, smart lights, sensors and media, generate huge amounts of data useful for monitoring and predictive analysis. This phenomenon facilitates sharing data and using this data to improve processes and functions. On the battlefield, soldiers, weapons, drones and vehicles, including ships and cars, can also use these databases on the same terms. This is how the Internet of Battlefield Things (IoBT) can be created. The principle of IT is to use the information generated by sensors and networks for military purposes (Osborne, 2023).

Automated Number Plate Recognition (ANPR) provides vehicle recognition capabilities and allows the location, tracking and tracing of specific vehicles in an urban area. This allows the military to target opponents faster and more accurately as well as reduce collateral damage (Bogan & Feeney, 2019). Therefore, in the Smart City environment, the military can access city monitoring and any other sensors, thereby gaining enhanced Common Operating Pictures (COPs) and generating digital maps and entering data into the Blue and Red Force Tracker system through the use of urban Long Range Wide Area Network (LoRaWAN) to maintain communications and efficient command. In addition, the military still has many other capabilities, such as:

- the use of an intelligent traffic system for the efficient passage of troop masses through a city or to organize the evacuation of the population;
- the use of the data generated by the Internet of Things for military purposes and the generation of information from the Internet of Military Things;
- influencing devices through the Internet of Things;
- better identification of opportunities emerging in the process of targeting and shaping the course of a military operation.

Safety & Defense 9(1) (2023)
DOI: https://doi.org 10.37105/sd.198

However, it should be remembered that Smart City devices, and in particular, sensors, may prove dangerous for our armed forces if these systems are not properly marked and controlled.

3. Air defense in the Smart City

1. **Air threats to cities**

In recent years, significant progress has been made in the development of the air assault assets (AAA). The capabilities of aircraft, helicopters, unmanned aerial vehicles (UAVs) and precision-guided weapons are continuously undergoing development. The concept of the impact of air assault assets should be understood as air surveillance, attack delivery (firepower and by electronic means), overflights of aircraft securing airborne landings, and other operations carried out using airborne platforms, e.g., feint and demonstration activities, smokescreen laying, scatterable mine laying, dropping propaganda leaflets, etc. On the other hand, the enemy's AAA include ballistic missiles, flying aerostatic and aerodynamic craft (both carriers and weaponry alone), designed to achieve military objectives related to surveillance, attack delivery, deception and transport of assault groups (Giffinger, 2015).

Modern air threats, as the experience of the conflict in Ukraine shows, are not related only to the use of conventional means, such as airplanes and attack rotorcraft. Of course, they still play a significant role on the battlefield, but thanks to the development of modern technologies since the 1980s, a trend towards the use of unmanned combat assets is noticeable, especially with regard to urban infrastructure. The fight against AAA is a task largely incumbent on the air defense forces. According to the documents concerning air defense, both national and allied (FM 3-01, 2020), the most dangerous air assault assets are those depicted in Figure 1.

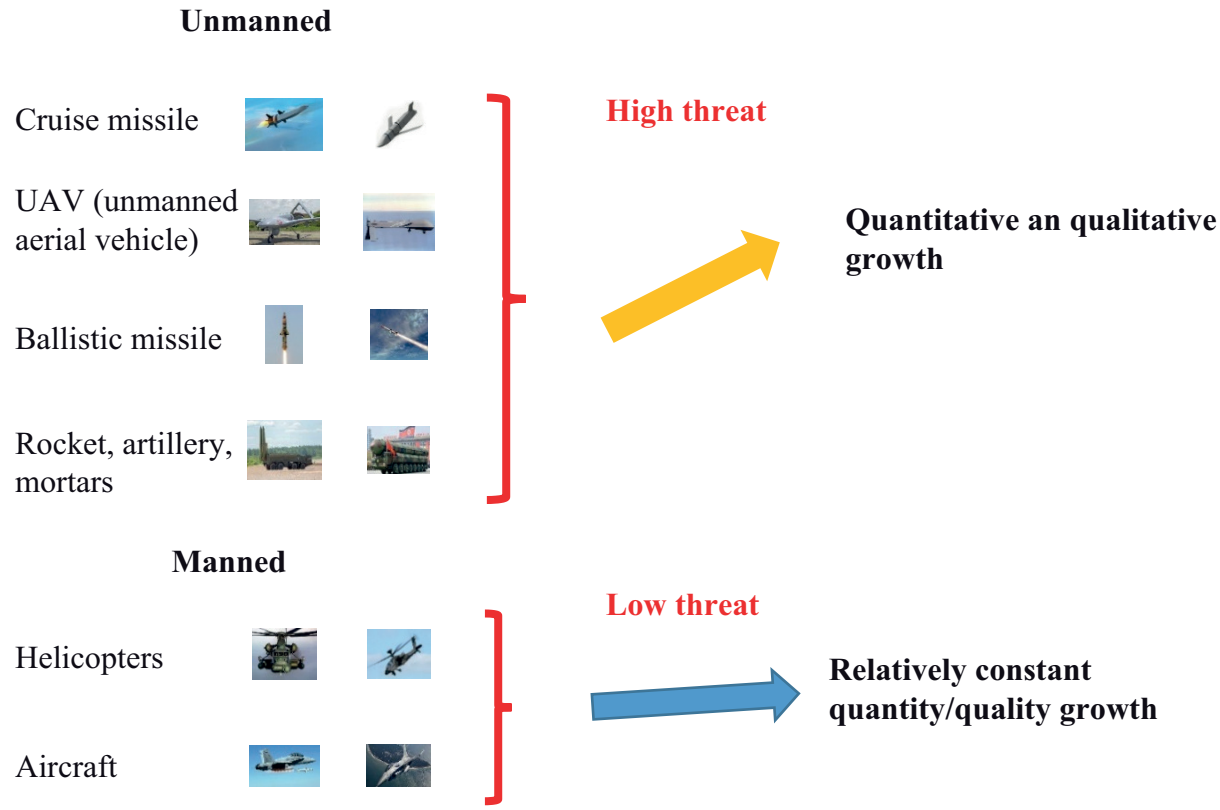

Figure 1. Contemporary air threats. Author's own work
Adopted from: "Materials of the Air and Missile Defense Board", Warsaw 2022

These include:

- manned aircraft (MA) – aircraft and helicopters of the air, land and sea forces. In this group of assets, a rapid development of air-to-surface armament is taking place, the carriers of which are increasingly often aircraft or helicopters, while the command system functions beyond the effective range of AAD assets;

Safety & Defense 9(1) (2023)
DOI: https://doi.org 10.37105/sd.198

- unmanned aerial vehicles (UAVs), and especially drones – their multifunctional and mass deployment in military operations will cause them to gradually take over the tasks performed so far by manned aircraft;
- cruise missiles (CMs) and tactical ballistic missiles (TBMs), which are still one of the main types of air threats but are no longer the exclusive domain of some economically and militarily powerful states;
- rocket and artillery mortars (RAM) are a relatively new type of threat, not because of technological solutions but due to the fact that they are classified as an air threat. Due to their large-scale deployment (on the example of cities in Iraq and Afghanistan, and now in Ukraine), growing attention is paid to the issue of intercepting mortar shells. This is the main threat to the units and subunits of the component of land forces and, in particular, critical infrastructure facilities, including those located in cities, including the Smart City.

2. Diagnosis

New technologies and, at the same time, new surveillance devices force the construction of automated surveillance systems that consider changes in the field of conducting and developing surveillance. The analysis of the development of surveillance assets and the conclusions from the stabilization missions in Iraq and Afghanistan, taking into account urban combat, shows that the assumptions and capabilities of the surveillance system, threats to national security and anticipated models of operations and tactics of urban combat have a decisive impact on the creation of a prospective surveillance system. The main objective of the diagnosis, and thus the basic requirements and concepts of the surveillance system stem from these premises. The determinants listed influence changes in the theory and practice of surveillance. These changes concern, among others (Wasiak, 2023):

- developing new theories of surveillance, especially in relation to crisis operations, activities in a network-centric environment of a non-military nature;
- introducing new or upgrading old but still prospective equipment;
- identifying new areas for conducting surveillance;
- developing new ways and techniques for the implementation of surveillance tasks;
- developing new procedures in the surveillance units of the command center at tactical and operational levels;
- developing modular organizational structures indispensable for implementing specific tasks due to the purpose and capabilities of surveillance subsystems in urban centers of Smart City type;
- perfecting the system of training surveillance specialists of all possible specializations being at the disposal of the commander and administrative bodies;
- automatizing procedures and surveillance systems, using the logistics and IT infrastructure of Smart Cities.

New opportunities for using surveillance equipment necessitate new tactics for its deployment. Currently, the biggest problem of the components of the allocated forces in urban centers is their protection against the impact of the enemy's firepower assets. The past and current peacekeeping and stabilization operations have demonstrated certain equipment-related and procedural deficiencies in the deployment of the surveillance system in cities. These gaps became very conspicuous during Operation Iraqi Freedom and the ongoing war in Ukraine. The absence of surveillance subunits in the national component makes it necessary to seek assistance from allies, who cannot always provide the patrols dispatched and surveillance posts with information about the threat. Nevertheless, the principal source of information in Smart Cities may be its assets, amongst which a special role may be played by the media and ICT channels (information about the enemy as well as the warning system), which may be supplemented by surveillance and observation posts located on high-rise buildings, especially administrative ones, manned by uniformed municipal services and equipped with basic visual recognition equipment and means of communication, ensuring surveillance capability with a range of up to 10 km. The modern surveillance system of air defense (AD) troops provides the capability of conducting surveillance within a range of up to 150 km, creating its multilayer image up to a ceiling of 30 km in the following surveillance modes: radiolocation, thermal-visual, night-vision, thermal-visual and visual systems – in total about 200 systems of various types can be listed.

3. Defense of cities

Conclusions from recent armed conflicts and analyses conducted in the area of security allow us to state that it is the defense of important facilities of urban infrastructure and military groups, which will be one of the most important factors ensuring success in conducting military operations. The contemporary threats which are present in the air domain necessitate the possession of effective anti-access and area-denial (A2/AD) systems because the effective defense of troops against air strikes is the most important condition for the success of a defensive operation (Szymanowski, 2023).

Currently, and in the future, the basic tasks of the air force and AAD units will include the prevention of incursions into the airspace by foreign aircraft, protection of critical infrastructure and airspace in the event of an air terrorism threat, and participation in allied operations. In the event of an attack on the territory of our country, the basic tasks of the air force and

Safety & Defense 9(1) (2023)
DOI: https://doi.org 10.37105/sd.198

anti-aircraft defense units should be focused on cooperation with allied forces in order to win air dominance. The main types of actions will be strategic air operations, operations against the enemy's ground and naval forces and so-called supporting air operations. Wrestling air dominance will be difficult, since the advantage of potential enemies, especially the Russian Federation, in combat aircraft is clear.

Therefore, in addition to the acquisition of new-generation aircraft, we should also boost our F-16 multirole aircraft stock. The air force's technical development should focus on increasing the combat range and precision of strikes. The capability of cyberspace operations is also of significant importance. It is vital to not only have ICT systems ensuring the collection, analysis, selection and distribution of information, but also the ability to impact enemy IT systems, without which modern command systems cannot function.

In the field of air and missile defense of cities, solutions consistent with the idea of network-centricity are of growing importance. Here, we refer to combat modules, the core of which is a command and control system, into which one can plug arbitrarily selected and characterized by appropriate parameters, sensors and effectors. The construction of the final structure of such a module will depend on the scale and type of threat. Such a subunit should be able to provide protection for important facilities, troop concentrations, command posts, logistics facilities, administrative and economic centers against a wide range of air threats, including protection against tactical ballistic missiles. Developing centralized command for missile modules will be a considerable challenge in practice. This is the basis for ensuring the effective repelling of air or missile strikes against objects located at a large distance from each other, i.e., cities. In the course of repelling air strikes, integrating the efforts made by all elements of AD in the fight against the air enemy becomes the fundamental principle of operation for the entire system. Therefore, combat modules created using modern sets of medium and short-range anti-aircraft missiles should meet all the necessary urban warfare standards and protect its infrastructure components. On the other hand, the combat modules of short-range missiles (Grom, Piorun) and ZU-23-2 AA artillery units can be placed on the rooftops, constituting elements of the Territorial Defense Force (TDF), or operational troops, as shown in Figure 2.

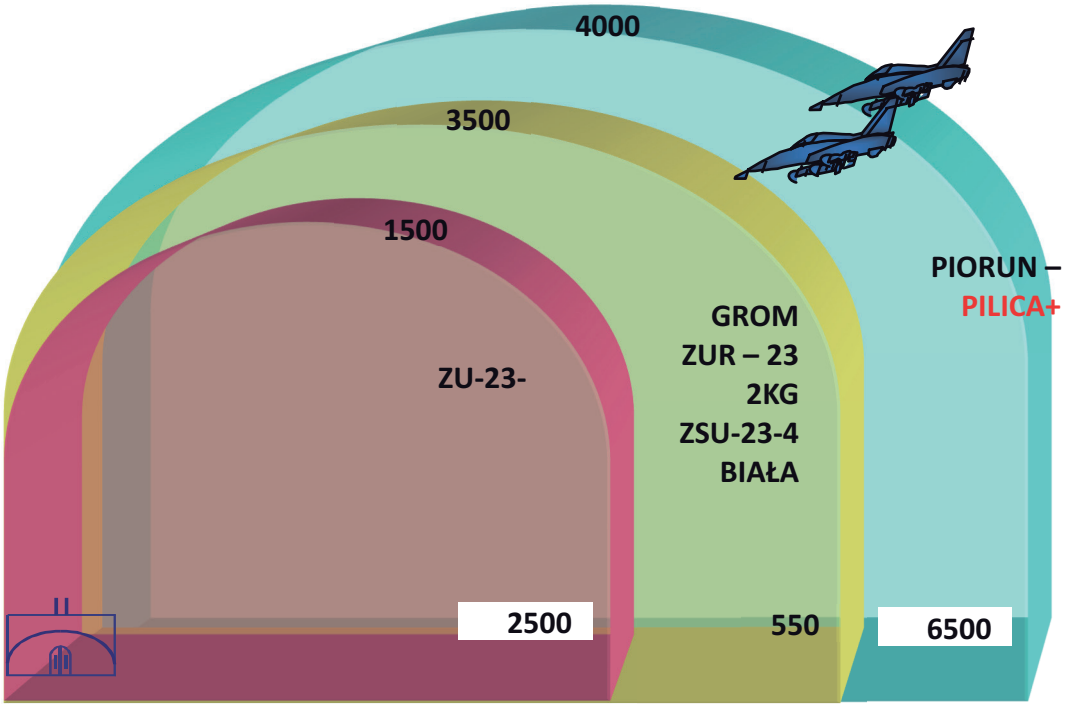

Figure 2. The fire system of the artillery and missile module
Adopted From: "Materials of the Air and Missile Defense Board", Warsaw 2022

Safety & Defense 9(1) (2023)
DOI: https://doi.org 10.37105/sd.198

The modern air defense system of urban centers should cover three layers: close range – up to 10 km, short range – up to 25 km, medium range – up to 100 km. Therefore, the modernization of AD troops, the "Shield of Poland" (Pol. Tarcza Polski), consists of three levels of defense, with ranges of 10, 25, 100 kilometers, including:

- the medium-range missile system "WISŁA" – replacing NEWA and WEGA;
- the short-range missile system "NAREW" – replacing OSY and KUBY;
- the short-range missile system "POPRAD", with the PIORUN missile; PILICA, with the PIORUN missile and ZUR-23-2 cannon;
- anti-aircraft warfare and decision-making systems, compatible with NATO systems – ŁOWCZA – REGA;
- additionally: unmanned systems, W2MPIR multirole surveillance and strike systems with "Warmate-2" loitering munition, devices emitting incapacitating energy in A2/AD zones, WRE systems and others. In the general perspective, as part of the development of air defense capabilities, it will be necessary to achieve a balanced (qualitatively and quantitatively) potential of active combat assets, surveillance and command measures in order to ensure high effectiveness in fighting air threats and to maintain the viability of the national air defense system.

Today, a conflict of limited scale, including one below the threshold of war, is more likely to threaten our country than an armed conflict. If this were to happen, the air defense system would have to face limited missile attacks (without an official aggression and aggressor), or a series of air and missile attacks intended to compel a certain behavior. In this case, the most important challenges for the air force and AD units will include early detection of incoming missiles and aircraft, immediate engagement of the largest possible part of the air force (to both minimize losses and counteract the threat) and executing a retaliatory operation. This would be an operation intended to eliminate at least part of the assets used in the attack, which is impossible without an appropriate Command and Control plus Intelligence, Surveillance, Target Acquisition, and Reconnaissance (C2ISTAR) system.

The course of modern armed conflicts indicates that the fundamental condition for victory was usually to gain air supremacy and maintain a certain degree of domination in the airspace. It was associated with the necessity to fight enemy aircraft in the air and on the ground. In order to counter this threat, a modern and powerful air defense should be at our disposal. In recent years, the air defense subunits have been equipped with a small number of new combat assets, including command automation assets. In addition, works intended to ensure the compatibility of the Polish air defense troops with NATO air defense forces have commenced. Unfortunately, the process of implementing and modernizing air defense subunits is costly and time-consuming. Nevertheless, work is still underway to ensure that the air defense and ground forces could be an effective combat asset countering a potential enemy's air assault resources. Depending on the deployment of forces and the organization of the anti-aircraft fire system in the protection of cities, the three following ways of anti-aircraft defense can be distinguished. These include:

- zone defense used by long- and medium-range (sometimes short-range) anti-aircraft missile units (sub-units). It consists in the creation of a fire zone in front of or around the defense area, which will prevent the enemy's AAA from reaching it;
- object (direct) cover (defense) implemented in the conditions of deficient AAD assets, which necessitates focusing the efforts on defending only priority facilities of the urban infrastructure;
- zone-object defense, which is a combination of the two above-mentioned methods, consisting in separating part of the forces for zone defense while implementing the protection of priority facilities in the object (direct) method (Szymanowski, 2023).

Therefore, the most important undertaking in the field of the technical modernization of the anti-aircraft defense troops is to achieve the ability to combat new categories of air threats at a distance of up to about 100 km, including tactical ballistic missiles. There are plans to achieve these capabilities through the acquisition of new short- and medium-range Narew and Wisła anti-aircraft defense missile sets. In such a case, only Wisła missile sets will possess the capability to counter tactical ballistic missiles. It is planned to acquire eight of these missiles sets and 19 Narew sets. In addition to these priority programs, the operational program includes a number of projects related to the development of very short-range anti-aircraft systems. The most important are: Poprad and Pilica anti-aircraft sets, Soła/Bystra radiolocation station and the modernization of PPZR (anti-aircraft rocket-propelled set) Grom to the Piorun version.

As a result of the implementation of the operational program, the scope of combat operations conducted by AAD troops will be significantly increased, including: enlarging the size of firing zones; acquiring the ability to counter ballistic missiles; the capability to simultaneously combat multiple air targets (multi-channel systems). However, in urban conditions, the current system, especially the command system, is not able to defend all critical infrastructure facilities and resources of armed forces (especially those moving across cities) against the full spectrum of air threats. The outdated architecture of our command systems has prevented interceptions of tactical missiles and rockets on multiple occasions. Other shortcomings of the current system solutions include limited flexibility in the deployment of available resources, which results in the need to commit forces greater than required, excessive workload of logistics units, as well as the lack of an efficient and secure communication system beyond the line of sight (BLoS), ensuring adequate communication between command systems, sensors and effectors.

Safety & Defense 9(1) (2023)
DOI: https://doi.org 10.37105/sd.198

Therefore, in response to the increasing threats from the air, the Army Integrated Air and Missile Defense (AIAMD) program built in the Republic of Poland is expected to enable the combination of various existing and being under development Air and Missile Defense systems (AMD) into one integrated, multi-layered system. Its most important element is the network-centric IBCS command system (IAMD Battle Command System). The idea of the IBCS system, which operates in the US Army and is currently to become part of the PAF, assumes the connection of separate hardware components using an Integrated Fire Control Network (IFCN), such as:

- command and control posts of the Engagement Operations Center (EOC) of the IBCS system at various levels;
- sensors: Patriot AN/MPQ-65 radiolocation stations and modified AN/MPQ-64 Sentinel radiolocation stations;
- effectors – PAC-2 and PAC-3 missile launchers of the Patriot system (M902 and M903).

In the near future, the system will also provide the capability of integrating short-range and close-range missile defense systems and the network of universal radars and missile launchers.

4. Conclusions

Contemporary and historical conflicts have shown the benefits urban areas may offer to asymmetric forces. Future urban operations will place a great deal of emphasis on information operations, regardless of whether the operation concerns a conventional conflict, counter-insurgency efforts, humanitarian aid or provision of aid in the case natural disasters.

Smart city systems and the data they generate could be used to support a variety of military operations, including rapid intelligence, surveillance and reconnaissance (ISR) assessments of physical, social and digital infrastructure; targeting opponents with greater precision; improving the methods of humanitarian aid distribution.

In order to achieve effective use of the smart city environment, the military must possess the information and the ability to use existing civilian systems. The military should seek to preventively recruit or hire professionals knowledgeable in these systems to gain practical knowledge of how to make the best use of the digital infrastructure.

When analyzing the future operational environment, the military must pay more attention to changes in the urban environment, in particulary the development of Smart City initiatives. The armed forces should seriously consider incorporating Smart City terminology into their official doctrine, including the defense of critical infrastructure facilities against air strikes. Smart City technologies present in urban centers should be codified, and the armed forces should be trained in using Smart City technologies in many domains, including anti-aircraft defense, as this may prove necessary to fight and win future operations in urban environments facing a technologically advanced airpower opponent.

The analysis of Smart City air defense systems presented in the above descriptions allows for synthetic conclusions indicating that the basis for the defense of cities against air strikes must be the elements of the A2/AD system, in which Smart City elements can be used in a multifaceted way as extended knowledge and intelligence. Therefore, a smart city should foster the diversity of control systems, characterized by creativity and innovation, which lead to effective decisions, also in the field of anti-aircraft defense.

Nowadays, these are also smart anti-aircraft systems – new weaponry elements such as: pulsed electromagnetic guns, laser systems, microwave incapacitating weapons and others – these are the future-oriented forces of anti-aircraft defense, including – perhaps in particular – the defense of Smart Cities.

The keystone in building an advantage over an air enemy as part of A2/AD is also the broad knowledge of the battlefield and its surroundings, which are constituted by critical infrastructure. The advantage in air and cyberspace will be given to those who will control faster and more efficiently the processes of collecting and processing information about the operations of their own troops and the enemy troops, as well as about the environment, terrain and meteorological conditions. Consequently, cyberspace, which a smart city also is, will ensure faster collection, processing and delivery of information, and airspace will become an integrated air and ground defense system. Creating and using modular missile and artillery sets will also become common, enabling operations according to the "plug and fight" principle (See the Figure 3). This type of missile and artillery sets will be the core of the anti-aircraft defense troops of the future; therefore, as part of the anti-aircraft defense capability, it will be necessary to achieve a balanced potential: active combat, reconnaissance and command assets (IBCS (IAMD – Battle Command System)), which will allow for high effectiveness in combating air threats, deterrence and maintaining the viability of the country's system of resistance to threats, and particularly so in Smart Cities.

Safety & Defense 9(1) (2023)
DOI: https://doi.org 10.37105/sd.198

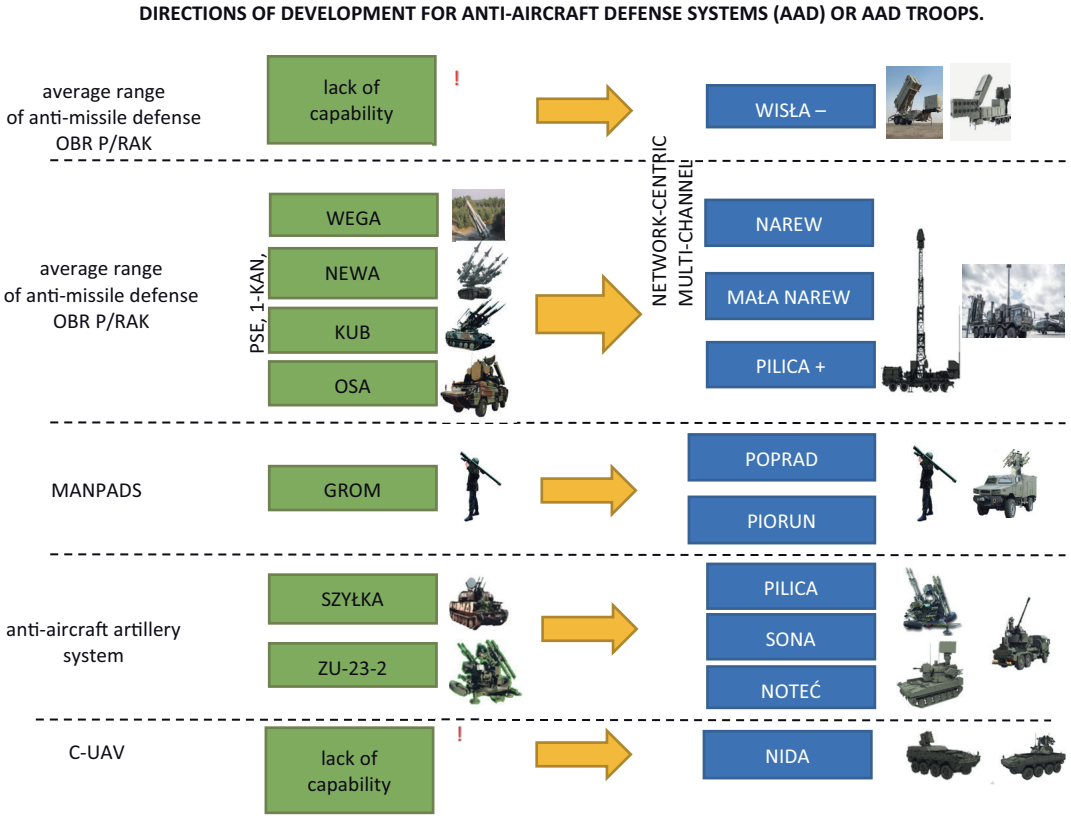

Figure 3. Directions of development for AAD troops
Author's own work.

Taking into account the analyses presented in this article, we can put forward the thesis that the anti-aircraft defense troops should develop in the direction of:

- the ability to combat manned and unmanned assets, rockets and missiles of the modern battlefield;
- mobility of anti-aircraft defense systems;
- dual firepower capability: anti-aircraft and anti-missile;
- compatibility and integration with NATO systems;
- autonomous operation.

Declaration of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. Braszko, A. (2023.07.20). *Military Implications of Smart Cities*. Mad Scientist Laboratory. https://madsciblog.tradoc.army.mil/242-military-implications-of-smart-cities/
2. Bogan, J., & Feeney, A. (2019).. Defence and Security Analysis, Fareham.
3. Cocchia, A. (2014).. Springer. DOI:https://doi.org/10.1007/978-3-319-06160-3_2
4. Dameri, R.P. (2013). Searching for smart city definition: A comprehensive proposal.,, 2545–2551. DOI: https://doi.org/10.24297/ijct.v11i5.1142
5. FM 3-01. (2020). *U.S. Army Air and Missile Defense Operations*. Headquarters, Department of the Army, Washington, D.C.
6. Gawkowski, K., (2019.08.10). *Smart robi różnicę*. A&S Polska. https://aspolska.pl/smart-robi-roznice/
7. Giffinger, R. (2015)., Vienne University of Technology.

Safety & Defense 9(1) (2023)
DOI: https://doi.org 10.37105/sd.198

8. Michalski, D. & Bernat, P. (2019)., 2019 International Conference on Military Technologies (ICMT), Brno, Czech Republic, 2019, pp. 1–5, doi: https://10.1109/MILTECHS.2019.8870070
9. Osborne, Ch. (2023.07.19). *US Army tests IoT for the battlefield in smart cities*. ZDNET. www.zdnet.com/article/us-army-tests-iot-for-the-battlefield-in-smart-cities/
10. Pradhan, M., (2020)., Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE, Wachtberg.
11. Stawasz, D., & Sikora-Fernandez, D. (2015).. Placet, Warszawa.
12. Szymanowski, K., (2023). Komponent przeciwlotniczy w systemie antydostępowym, 92–97.
13. Wasiak, T., (2023). Teoretyczne aspekty rozpoznania., 84–92.
14. Zieliński, Z., Wrona, K., Suri, N., Fuchs, Ch., Pradhan, M. & others, (2018). Conference paper. International Conference on Military Communications and Information Systems (ICMCIS).