re-BUS

You have downloaded a document from
RE-BUŚ
repository of the University of Silesia in Katowice

Title: Protection of Polish critical infrastructure (CI) against air threats

Author: Michał Piekarski, Karolina Wojtasik

Citation style: Piekarski Michał, Wojtasik Karolina. (2022). Protection of Polish critical infrastructure (CI) against air threats. "Security and Defence Quarterly" Vol. 39, No 3 (2022), s. 1-12, doi 10.35467/sdq/147676

Uznanie autorstwa - Licencja ta pozwala na kopiowanie, zmienianie, rozprowadzanie, przedstawianie i wykonywanie utworu jedynie pod warunkiem oznaczenia autorstwa.

UNIWERSYTET ŚLĄSKI W KATOWICACH
Biblioteka Uniwersytetu Śląskiego
Ministerstwo Nauki i Szkolnictwa Wyższego

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

Protection of Polish critical infrastructure (CI) against air threats

Michał Piekarski[1], Karolina Wojtasik[2]

michal.piekarski@uwr.edu.pl

[1] https://orcid.org/0000-0003-1514-7657

[1]Institute of International Studies, University of Wrocław, ul. Koszarowa 3, 51-149 Wrocław, Poland

[2] https://orcid.org/0000-0002-1215-5005

[2]Institute of Sociology, University of Silesia, ul. Bankowa 11, 40-007 Katowice, Poland

Abstract

The goal of this paper is to analyse challenges related to protecting Polish critical infrastructure (CI) against air threats, such as UAVs, as a case study in a wider discussion on protection of critical infrastructure worldwide. The Polish legal definition of critical infrastructure and laws regarding the protection of such facilities are explained in the article in order to provide context. A review of scientific literature and open-source analysis of known air attacks on CI and the capabilities of air platforms are also included, with special attention being paid to unmanned systems. The threats themselves have been divided into two groups of scenarios: peacetime threats and crisis situations that have hybrid wartime scenarios. Depending on the scenario, the different capabilities of actors must be taken into account. Peacetime air threats include the use of commercially available drones. Those devices have limited capabilities, in terms of weaponisation, due to the limited weight of their cargo and the flight range. More advanced devices, including custom–built drones and military systems, can be supplied and used by state actors. Therefore, there are different requirements regarding protection systems. In peacetime, anti-drone systems are certainly recommended due to their capabilities and safety of use for bystanders. In more dangerous scenarios, typical military systems, including Very Short-Range Air Defence, Short-Range Air Defence and Medium Range Air Defence systems have to be employed or dedicated kinetic counter-drone systems deployed.

Keywords:

terrorism, critical infrastructure, hybrid warfare, air threats, unmanned aerial vehicles

Article info
Received: 26 October 2021
Revised: 25 February 2022
Accepted: 24 March 2022
Available online: 9 May 2022

Citation: Piekarski, M. and Wojtasik, K. (2022) 'Protection of Polish critical infrastructure (CI) against air threats', Security and Defence Quarterly, 37(1), pp. 00–00. doi: 10.35467/sdq/147676.

© 2022 M. Piekarski, K. Wojtasik published by War Studies University, Poland.
This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

Introduction

Efficient critical infrastructure is a key condition for the efficient functioning of society and basic social and political institutions. State security depends on the efficient functioning of the facilities and systems that make up the critical infrastructure. Because of this, such facilities and systems can be the target of attacks, including those carried out with the use of various types of aircraft - both manned and unmanned - in times of peace and crisis. The main research question related to this is could Poland's critical infrastructure be attacked from the air and, if yes, then what can it do to protect itself? To answer this it is necessary to analyse both the critical infrastructure (CI) and the principles for protecting it in Polish law and examine the possible threats. The first part of the article looks at the definition of critical infrastructure (CI), the principles and the most frequently used methods and forms of protection. The second part contains an analysis of possible tactics and attack scenarios and indicates the necessary capabilities for protecting Polish critical infrastructure (CI).

The research was especially based on analysis of known situations when critical infrastructure or military facilities were threatened by drones and other aerial vehicles. Due to the rapidly changing security environment and rapid technological progress, many of the sources used were defence–oriented magazines and online portals that were able to deliver a significant amount of factual information.

Critical Infrastructure and its protection

The most important document explaining why critical infrastructure is *critical* is the Crisis Management Act of 26 April 2007 (Ustawa o zarządzaniu kryzysowym, 2007). According to this act, critical infrastructure consists of systems and their constituent functional facilities, including structures, equipment, installations, services which are critical to the security of a state and its people, and which ensure the effective functioning of public administration, institutions, and businesses. Critical infrastructure belongs to subjects of mandatory protection according to the Protection of People and Property Act (Ustawa o ochronie osób i mienia). Critical infrastructure includes 11 systems related to: energy supply, energy-producing raw materials and fuels, communications, IT networks, finance, food and water supply, health protection, transport, medical emergency response, continuity of public administration, production, holding, storage and use of chemical and radioactive substances including pipelines for dangerous substances. Not every facility that is important on a daily basis is a part of critical infrastructure. The decision to include a given facility in the CI is based on detailed criteria specified in a classified attachment to the National Program for Critical Infrastructure Protection (Narodowy Program Ochrony Infrastruktury Krytycznej, 2020), which is updated every two years (the most recent in 2020). This document contains the rules for identifying certain systems as critical: the factors assessed are the parameters of a facility or system and, more importantly, the consequences of operations being ended or a facility or system being destroyed.

The National Critical Infrastructure Protection Program (Narodowy Program Ochrony Infrastruktury Krytycznej, 2020) designates six areas of key importance for CI security. Firstly, physical security, i.e., organisational, and technical activities that are to minimise the risk of interference with the functioning of CI as a result of people illegally entering or trying to enter the premises of an enterprise or disrupt the operation of the system. Secondly, technical safety, i.e., all activities that minimise the risk of disrupting the ongoing technological processes. Thirdly, personal security, i.e., activities related to minimising the risk that some employees or individuals authorised to enter the CI premises will disrupt the functioning of the company or the system. Fourth, ICT security, i.e., activities

related to minimising the risk of the functioning of CI being interfered with as a result of the impact on the control apparatus and the ICT systems and networks. Fifth, legal security, i.e., those measures and procedures that protect a company or system against the legal effects of the actions of external entities. Sixth, business continuity and recovery plans, understood as a set of organisational and technical activities leading to the maintenance and restoration of functions performed by CI.

Critical infrastructure is a prerequisite for the efficient functioning of society, the systems that create it are essential in people's daily lives, and any disruption has an impact on the population. CI is a communicating vessel system, a failure in one system most often affects the other with far-reaching consequences. Natural disasters, failures, and finally, the human factor, whether intentional or not, can harm critical infrastructure in a significant way, causing material losses on the one hand, and hitting the sphere of the so-called soft effects.

Critical infrastructure is susceptible to destruction, damage, and disruption, which may be caused by forces of nature or human actions, entailing a threat to the life and property of citizens and having negative consequences for the development of the economy. Therefore, it is one of the top priorities of the authorities of the Republic of Poland to protect critical infrastructure. According to the Crisis Management Act of 26 April 2007 (Ustawa o zarządzaniu kryzysowym), CI protection are actions designed to ensure functionality, continuity of operation and integrity of critical infrastructure in order to prevent threats, risks or vulnerabilities, limit and neutralise their effects and quickly restore the infrastructure in the event of a failure, attack, or other event interfering with its proper functioning. In the field of critical infrastructure protection, the Government Centre for Security plays the most important role, coordinating the activities of other entities, supporting, providing information, and building a partnership between entities involved in CI protection. Other entities involved in CI protection are CI Operators, Ministers responsible for CI systems, the Council of Ministers, law enforcement and emergency services, as well as regional and local authorities (at voivodeship, county and city or municipality level).

The obligation to ensure the safety of CI facilities belongs to the CI operator, i.e. the owner and independent and dependent owner of facilities, installations, devices, and services of the critical infrastructure. Considering the fact that measuring CI security is an extraordinarily complex task and the lack of reliable models for such an assessment, the following measures are adopted to measure the achievement of the objectives of the National Program for Critical Infrastructure Protection (Narodowy Program Ochrony Infrastruktury Krytycznej, 2020):

1. The approved CI protection plan. The CI protection plan is the basic document confirming the operator's compliance with the obligation to protect CI referred to in Art. 6 sec. 5 of the Act on Crisis Management. The plan shows how much work was put into the preparation and implementation of CI protection. A properly conducted planning process increases an organisation's ability to identify and reduce vulnerabilities, counteract threats, and react to them and minimise their impact (Załącznik 1 do NPOIK Standardy Służące Zapewnieniu Sprawnego Funkcjonowania Infrastruktury Krytycznej. Dobre Praktyki i Rekomendacje).

2. Audit of CI protection status.

3. Structural and budgetary changes.

4. Exercises in which rescue and security services take part.

The CI protection plan includes elements such as: general company data, the data of the CI facility, the characteristics of threats, dependencies, resources, variants of action in the event of a threat, continuity, recovery, and principles of cooperation with other entities. Detailed requirements regarding the CI protection plan are included in the Regulation of the Council of Ministers of April 30, 2010 (Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony Infrastruktury Krytycznej)on the plans for Critical Infrastructure Protection. The Government Centre for Security ultimately approves such a plan.

The issues of Critical Infrastructure (CI) and protection of those facilities and systems are directly interlinked with issue of possible air threats and air defence.

In order to further analyse those issues, possible threats to Critical Infrastructure should be described, keeping in mind that those threats may have different forms in peacetime, during crisis situations (especially "hybrid warfare"). Only this, combined with the description of Critical Infrastructure (CI) in Poland, allows for further description of desired air defence capabilities.

Peacetime air threats

During peacetime, understood here as a period of normal international relations, when international tensions are low (and when nation states do not sponsor or support terrorist actions or threaten to use military force against other countries), threats to critical infrastructure are related to various forms of political or industrial espionage, criminal, or terrorist activity or may be due to accidents such as an irresponsible drone pilot or the malfunction of the drone itself. This part of the article focuses on those threats that are caused by intentionally harmful activities.

Espionage (intelligence gathering) may be conducted by various state or non–state actors and by natural, covert, and non-kinetic activity. This may include gathering imagery (still or video) of facilities or their key elements, or even people (IMINT), or various forms of electronic intelligence (ELINT) aimed at electronic systems (including communications systems) or other forms of information, depending on intelligence requirements and the capabilities of sensors. When air assets are considered, they may be used as sensor platforms – the simplest example is of course small, commercially available, camera-equipped drone overflying facility. Since such activities are usually conducted in a covert manner, cover and concealment are the most important factors. Therefore, aircraft used in this role should be difficult to detect or used under cover of legitimate activities (i.e. for recreational use like sightseeing flights). Use of low-cost, commercially available devices, equipped with modern cameras, allows images of the CI facility to be collected while reducing cost (said drones cost from 2000 to 8000 PLN) and also provide credible cover – even if detected and apprehended, anybody operating such a drone could claim it was being innocently used and they were not aware of the fact that is the facility was sensitive.

A special case is gathering intelligence by provocation. For example, an unmanned aerial vehicle may be deliberately flown over a sensitive facility, forcing security forces to respond. In this scenario, intelligence is gathered not on the facility itself, but on the response of security forces (including law enforcement or military)– including response time, equipment used and its capabilities. Some unexplained sightings of aerial phenomena in the USA, including when a swarm of drones harassed security personnel at the Palo Verde Nuclear Generation Station (Rogoway and Trevithick, 2020), may be the result of such activities (Rogoway, 2021).

Assuming that peacetime terrorist activities are not directly inspired, sponsored, or otherwise supported by state actors, they do have limited resources available. However, the increasing availability of small unmanned aerial vehicles drones means they can play two roles in terrorist activities, other than intelligence gathering.

One possibility is to use a drone for recording an attack such as the explosion of a vehicle-borne improvised explosive device for propaganda purposes. The other is using an aerial vehicle as a weapon.

An air attack may help avoid ground security measures, like fences, gates and checkpoints and it is possible to simply fly over them and strike a desired target. A drone can carry an explosive device or release weapon to fly or hover over a target. They have been used in such a manner by a number of actors including the Islamic State of Iraq and Levant (ISIS) (Sims, 2018, Watson 2017).

The main issue with the use of low-cost drones is their limited carrying capability. For example, there are aftermarket devices for cargo carrying and release available. One commercial vendor of such device for DJI Phantom Pro 4 drone states that "safety reasons the maximum payload should be less than 800 grams under ideal conditions and recommended not to exceed 500 grams" (Drone Sky Hook, 2022).

Even if a user connects some other modifications (e.g. removing the camera system), there is still the question of performance (flight speed, flight altitude, manoeuvrability and flight time limited by battery capacity) of the said drone (Łukasiewicz, 2021). Also, assuming that the drone is used for a one-way mission and there is no need to assume any return flight, the maximum load of a low-cost drone (like DJI Phantom 4 or DJI Mavic 2) is small, especially compared with other terrorist IEDs placed in backpacks or especially trucks.

Of course, it may still be possible to carry a small explosive device such as one based on a typical military–grade 200g TNT load and may still be dangerous if placed in a precise manner in a place that is vulnerable to explosion. Even a small detonation may have significant effects. For an illustration of this, the scenario of a low-cost drone attack on an airport is considered. If said low-cost drone hits a traffic control tower or traffic control radar, even only creating light damage, the facility will cease to function at least for the time required for the inspection and repair of damaged devices. In such a case, the airport should be closed. Other consequences may also be significant, especially media attention and public reaction (loss of confidence in the safety of air transport, for example).

More damage can be caused by heavier drones. For example, the DJI Matrice 600 is able to carry up to 6 kg of payload – for a much bigger price, almost 25000 PLN (6k USD) (DJI, 2022). 6 kilograms or even slightly more still mean that the device is less powerful than other weapons available to a terrorist, not to mention military-grade ones. A terrorist with financial resources could, however, purchase several smaller and cheaper drones. This seems a more economical option, especially if it means several facilities can be targeted or harassed by repeated attacks.

Other types of aircrafts can certainly be used. General aviation planes, helicopters and gyrocopters do have much larger capabilities. For example, the popular Cessna 172 or vintage PZL-104 Wilga can carry up to three passengers, plus pilot, and the light helicopter Robinson R44 offers a similar capacity, and other options too that may include heavier planes and helicopters or ultralight planes.

Since they are piloted by a person, an important question arises. How could they be employed, especially that they are not combat aircrafts (and in fact some of them do exist in armed variants, but they are not available on the civilian market)? Of course, they could be adapted to carry some homemade weapons or used to deliver armed personnel to the premises of an attacked facility, but most effective could be converting them for a suicide attack. Because of its mass, energy, and presence of flammable substances (fuel), the aircraft can be used as a weapon and an explosive device, much larger than a drone, could be added, from 50 to 200 kilograms or even higher can add devastating power.

In this scenario, the main issue is the cost of the aircraft itself and costs related to the training necessary to operate them. The costs are much higher than in the case of drones and financial resources for training and purchasing light aircraft start from 100,000 PLN and may reach 600-700,000. Of course, there are other possible options – plane could be leased or even stolen. It is also possible that a determined person could reduce the cost by building one at home. However, people who committed terrorist acts in Europe or USA more recently had much more limited resources and chose cheaper ways to attack (Piekarski and Wojtasik, 2020; Wojtasik, 2019). Therefore, the risk of terrorist attacks with a drone is lower than other types of attacks.

Air threats in crisis situations

In this article, crisis is considered a period of heightened internal and international tensions, when ordinary forces and resources are inadequate for the situation. In Poland's legal system, crisis situation is defined as a situation that negatively affects people's level of safety, high-value property or the natural environment, and includes large-scale restrictions on the operation of public administration due to inadequate forces and resources" (Ustawa o zarządzaniu kryzysowym, 2007). Crisis situation does not mean that an emergency has already occurred. It can also be a situation when the risk of said emergency is higher than usual, and pre-emptive and preventive actions are required, and this also is described in legal acts. For example, in Polish anti-terrorist law, there are four alert states that may be implemented depending on the perceived risk of attack and they each allow for the use of various measures, including those related to protection of critical infrastructure facilities and systems (Ustawa o działaniach antyterrorystycznych, 2016). It should be noted that a crisis situation does not always match its legal definition as the internal situation is normally reflected in it not the international one.

Therefore, a broader approach to international relations is necessary. International crises may be limited to strategic communication and diplomatic activities (recall or expulsion of diplomatic personnel, designating a state as a possible threat), economic actions (especially sanctions), a show of military force (e.g. unannounced, sudden "snap" exercises) and use of covert actions. Those elements have been described recently as "hybrid warfare". Use of political tools of influence, information operations (propaganda, disinformation), and economic pressure may be also supported by armed covert actions. The conflicts in Ukraine and Syria are good illustrations of such mixed use of measures and tools (Bērziņš, 2020).

In one hybrid scenario, Russia is considered a hostile actor, and its intention is to compel Poland to carry out its demands. This may be because of Polish-Russian relations alone or have another background like a crisis in the Baltic states, Ukraine, or Belarus.

Apart from political and propaganda measures, economic sanctions, such as ending the delivery of oil and natural gas, could have significant consequences for the Polish economy.

Poland does have alternative routes – liquid natural gas may be imported from other suppliers using maritime lines of communication; therefore allowing Poland to be at least partially independent from Russian natural gas. Of course, if the terminal becomes inoperable, Poland may become fully dependent again on Russia. Covert use of force like "false flag" operations of intelligence agencies, special operation forces or some terrorist organisations (financed, equipped, and trained), instead of overt use of conventional forces allows for greater flexibility, especially because overt attack is an act of war and also means that Russia will be internationally recognised as an aggressor. If said terminal is attacked by members of some Polish terrorist organisation who were in fact soldiers of a foreign state conducting a covert operation, it will be classified as an act of war only if clear evidence is presented. Other critical infrastructure facilities and systems are also lucrative targets. This includes energy-related infrastructure such as power plants, oil refineries, petroleum storage sites and transportation systems – including railroad stations and marshalling yards (Piekarski, 2019).

It is perfectly safe to assume that critical infrastructure facilities and systems will receive additional protection in crisis situations. The normal security guards contracted or employed by an operator or owner will be supported by police forces, Territorial Defence Forces troops or even regular army forces. Additional protective measures may be implemented. Direct land attack – by sneaking or forcibly breaching a perimeter – is riskier. Risk is not only physical. Any ground fight increases the risk of an attacker being captured and such a person could provide the evidence.

Those factors mean that aerial platforms may be a less risky mode of attack. The fact that those activities are carried out by state forces (like special operation forces), or actors heavily sponsored by the state, means platforms do not need to be cheap, over-the-counter drones. It is possible to use military grade platforms with a heavier payload and capabilities, or even prepare custom-made devices.

Such an option offers a larger payload, greater range, and more sophisticated guidance systems. For example, the Iranian-sponsored Houthi movement in Yemen employs Qasef-1 type ammunition, a variant of the Iranian Ababil system, capable of delivering a 30–45 kg explosive warhead and with a range up to 150 kilometres (Mushin, 2019). Larger ones were also used, but the larger the drone, the more problematic they are. In order to be useful in such a scenario, plausible deniability is required so they cannot be launched from a territory controlled by a sponsored actor. Conflicts in the Middle East and Northern Africa region, where drones have been used extensively by various actors, offer some insight into the capabilities of modern drone attacks, including the much covered attack on Saudi oil facilities (Cieślak, 2021; Niedbała, 2020).

Possible locations include Poland, another state, or the sea (especially outside territorial waters). Drones could be concealed on board a commercial ship (like a large yacht, research vessel or cargo carrier) or smuggled to Poland or another country in parts and assembled before launch. The fact that state support is available might allow for multiple options. For example, intelligence services could establish a number of legitimate front companies, importing perfectly legal goods such as car or machine parts. Elements of drones could be easily concealed in imported goods, especially warheads and some elements (like wings, fuselage, engine, and the majority of electronics system) could even be imported legally. Front companies can also provide other services, like storage/assembly space, vehicles, and cover for personnel responsible for handling the drones. It is also possible to find suitable places for launching drones – the range may mean a suitable secluded property can be identified away from potential targets. Even if a launch or other activities are noticed, there is a chance that they will not be connected with a threat to facilities dozens of kilometres away.

Operating air assets from maritime vessels is an even better option. As long as they stay away from a narrow area (12 nautical miles) of territorial waters, they are free to operate and can enter territorial waters exercising the right to innocent passage or just pretend to visit a port. Large volumes of maritime traffic in the Baltic Sea allows for better concealment of the presence of a "drone mothership". There would be no need to smuggle any parts or equipment – they could be easily transferred onboard the vessel. An additional advantage is the possibility of the ship being used as a platform for intelligence gathering or to operate underwater or surface drones. Drones are not the only useful weapons. Mortars, unguided rockets, or guided missiles can be used, bearing in mind the plausible deniability factor, accuracy, range, and other issues.

Air Defence of Critical Infrastructure in Peacetime and Crisis situations

The protection of Critical Infrastructure (CI) facilities and systems from air threats is shaped by possible threats from one direction and legal and organisational issues from another. The security of facilities and systems is primarily the responsibility of their owners and operators. Since such facilities are also so-called mandatory protected facilities according to the Protection of Persons and Property Act of 1997 (Ustawa o ochronie osób i mienia, 1997), the security is provided by security guards (formally called: employees of specialist armed protection formations). They are authorised to operate any intruder-detection systems, including CCTV and similar tools that could be also used if adequately configured to detect drones. The powers of security guards regarding the use of force are described in the Protection of Persons and Property Protection Act, supplemented by other regulations. The most important is the Aviation Act that gives powers to security guards and the military and law enforcement services personnel to destroy, immobilise or take control over an unmanned aerial vehicle if its flight path or activity puts human life or health in danger, it is a danger to such guarded facilities, disrupts a mass event or creates danger to the participants of such event or there is a reason to consider the UAV as part of a terrorist attack.

Those regulations give security personnel clear authority to intercept any drones that may fly over Critical Infrastructure (CI) facilities and systems. Any technical tools or devices are legal to use and the use of firearms is allowed. The spectrum of possible technical solutions is broad: one study counted 537 systems manufactured by 277 companies (Michel, 2019). Those systems are available in various applications. Some are portable (handheld or backpack mounted), some are mobile, others are stationary. They use various sensors. The most basic ones rely on operator's senses (sight and hearing), while others use more advanced devices like radar, radio frequency monitoring devices, electro-optical sensors (cameras) and others. There are different ways to stop drones: some systems can "soft–kill" a drone by jamming its GPS and similar navigational systems, others can jam the radio link between operator and drone, others use an electromagnetic pulse to render the drone inoperable. Some systems use kinetic ways ("hard–kill") to destroy UAVs – usually simply shooting them down. There are known examples of drones being used against adversary drones. In 2021, the agency DARPA conducted a test of a system with UAVs that used electromagnetic waves – in this case microwaves – to disable a threat by damaging onboard computers (Tingley, 2021). Another system designed in Poland is an example of a kinetic system that is composed of day and night vision cameras, laser rangefinder and a 12/7mm, multibarrel machine gun supported by a radar detection system (Świat Dronów, 2022). Another Polish system uses a large volley of rockets. This system was designed to counter the threat from military-grade UAVs, especially loitering munitions (Kucharski, 2017).

Each kind of counter-drone system has its pros and cons. A "soft – kill" system may, by jamming GPS or communications, force a drone to follow safety protocols and make a precautionary landing or abort a mission and return to base. Such protocols are typical for commercially available drones, which has another advantage because those devices may only use certain frequencies for communication for legal reasons, therefore making it easier to detect drones and jam transmissions.

If a certain drone was designed to operate in autonomous mode or communications systems were designed to make jamming less effective, then jamming communication may not be effective, and if the guidance system is designed to operate without GPS or switch to another guidance mode if jamming was detected. Such capabilities are typical for UAVs designed for military purposes. Therefore, it is safe to assume that "soft kill" systems are more useful in defence than less complicated, commercially available drones, and the more complicated a drone is and if designed for military use, the more probable it is that "hard kill" is necessary. In peacetime, the most threats include the use of commercially available drones; therefore it is recommended that "soft kill" systems should be used to protect CI facilities and systems in peacetime.

In times of crisis, the range of possible threats is much wider and more advanced capabilities may be required. There are a number of possible solutions. For example, situational awareness may by increased by patrolling the airspace around critical infrastructure, in a manner similar to that already employed in Poland during high-profile events like sport games and political summits.

From the perspective of the Polish security system, hybrid warfare also means hybrid response. Since covert use of force can be considered as terrorism, full spectrum of counterterrorist resources may be employed, including domestic intelligence services, various legal measures and countering terrorism financing (Gasztold and Gasztold, 2020). This wide set of capabilities allows for generalized response to hybrid threats, but various forms of attack require tailored measures in order to prevent and response to them.

As it was mentioned earlier, detection of more capable drones and their neutralization may also require use of typical military air – defence systems, that belong to "hard – kill" group. For minimal protection, Very Short-Range Air Defence (VSHORAD) systems equipped with radar and electro-optical sensors and weapons capable of interception of drones and similar threats should be employed. The usefulness of systems based on ZU-23-2 23mm guns in this role is questionable in Poland, but possible options are missiles such as Grom or Piorun that are only used in the Pilica missile system and the Poprad system. Certainly, the more layered air defence is, the more capable, so additional, higher layers should exist in the form of Short-Range Air Defence (SHORAD) and Medium Range Air Defence (MRAD). In contemporary Polish conditions, such capabilities are limited to obsolete Warsaw Pact -Era systems like SA-8 (Osa), SA-6 (Kub) and SA-3 (Newa). The new systems – MRAD MIM-104 Patrion acquired in the Wisła programme should be available in a limited number in the future (two batteries, from eight planned). The supplier of SHORAD systems in the Narew programme, which plans to purchase quite a number (more than 20 batteries) has yet to be announced. One important capability may be provided by the Navy in the Miecznik programme and should result in the purchase of three frigates, but the contract for the delivery of those ships is also not yet signed.

And even if the plans are ambitious, and the potential of Polish air defence forces is large – there is a missile brigade in the Air Force, three air defence regiments in Land Forces divisions (and a recently created fourth), every mechanised and armoured brigade

has an organic air defence battalion, and the navy has two air defence battalions and other organic air-defence elements. However, the word "organic" is the key word. Most of those assets are tasked with supporting their units and their facilities.

The list of facilities and other assets that require air defence is long. It includes a military air base, key land-based assets and naval bases. If land forces are deployed, the forces "in the field" will have to be protected from air threats.

Assuming that plans regarding MRAD and SHORAD systems are at least partially fulfilled in the next ten years, that may mean that the most important facilities and areas may receive layered air defence. For example, the north-western corner of Poland, where the strategically important ports of Szczecin and Świnoujście are located, along with other facilities (Police chemical industrial area, Goleniow airport, Dolna Odra power plant, railroads, highways and even a waterway to Germany) may receive strong air defence in form of future Wisła and Narew systems, due to its importance. One additional advantage is the possibility of using Navy assets (land and sea-based). That raises a question about protection of facilities that are located in much more remote areas, like the power plants Połaniec and Kozienice.

One solution could be building air defence capabilities in Territorial Defence Forces. A number of relatively cheap VSHORAD systems – Poprad or similar ones (e.g. using simpler and cheaper vehicles) may be useful extension of their capabilities. Territorial Defence Forces are not deployable forces, they are responsible for territorial areas of responsibility of each TDF brigade and one of their tasks is supporting civil authorities in crisis situations. In a natural way, this includes protection of critical infrastructure facilities and systems, so an air defence component can provide useful capabilities for this mission. It will also mean that capabilities of a potential air defence component of TDF are composed of not only typical air defence systems, but dedicated counter-drone ones.

There are also other resources. Law enforcement forces (Police) and light infantry units of Territorial Defence Forces do not have the capabilities (unless use of rifle fire is considered) to shoot down hostile drone. But they could be used to screen areas surrounding protected facilities in order to detect air threats or early attempts to launch drones, as well as detect and stop other forms of attacks. Their own air assets, UAVs of Territorial Defence Forces and Police drones, can also help. Finally, the Police Border Guard and military forces have helicopters, and they could be employed not only to detect incoming threats, but could also engage them in favourable conditions.

Conclusion

The protection of the critical infrastructure (CI), due to the relevance of CI systems and facilities for state, economy, and society is itself a critical issue. While there are number of threats to CI and many possible methods for attacking such facilities and systems employed, air threats must not be neglected. This method of attack may be employed in a crisis as part of "hybrid warfare" activities supported and sponsored by a hostile state actor. In such a situation, the order of magnitude of political, economic, and social consequences justifies the allocation of resources to protect critical infrastructure from technically advanced threats. The nature of threat defines the technical capabilities of the necessary counter-drone systems.

Funding

This research received no external funding.

Author Contributions

Conceptualisation, M.P. and K.W.; methodology, M.P. and K.W.; formal analysis, K.W.; investigation, M.P. and K.W.; resources, M.P. and K.W.; writing—original draft preparation, M.P.; writing—review and editing, M.P. and K.W. All authors read and agreed to the published version of the manuscript.

Data Availability Statement

Not applicable.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Bērziņš, J. (2020) 'The theory and practice of new generation warfare: The case of Ukraine and Syria', *The Journal of Slavic Military Studies*, 33(3), pp. 355–380. doi: 10.1080/13518046.2020.1824109.

Cieślak, E. (2021) 'Unnamed aircraft systems: Challenges to air defence', *Safety & Defence*, 7(1), pp. 72–82. Available at: https://sd-magazine.eu/index.php/sd/article/view/110/83 (Accessed: 13 April 2022).

DJI (2022) *Matrice 600*. Available at: https://www.dji.com/cz/matrice600/info (Accessed: 15 April 2022).

Drone Sky Hook (2022) Available at: https://www.droneskyhook.com/product-page/Single-Release-and-Drop-for-DJI-Phantom-4 (Accessed: 14 April 2022).

Gasztold, A. and Gasztold, P. (2020) 'The Polish counterterrorism system and hybrid warfare threats terrorism and political violence', *Terrorism and Political Violence*, pp. 1–18 doi: 10.1080/09546553.2020.1777110.

Kucharski, B. (2017) *Stokrotka – system obrony przed bezzałogowcami i nie tylko* Available at: https://zbiam.pl/artykuly/stokrotka-system-obrony-przed-bezzalogowcami-i-nie-tylko/ (Accessed: 13 April 2022).

Łukasiewicz, J. (2021) *Morskie farmy wiatrowe jako potencjalne cele ataku z użyciem bezzałogowych statków powietrznych Biuletyn analityczny nr 32 Rządowe Centrum Bezpieczeństwa*. Available at: https://www.gov.pl/web/rcb/biuletyn-analityczny-nr-32 (Accessed: 14 April 2022).

Michel, A.H. (2019) *Counter drone systems*. Available at: https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf (Accessed: 15 April 2022).

Mushin, D. (2019) *Houthi use of drones delivers potent message in Yemen War*. Available at: https://www.iiss.org/blogs/analysis/2019/08/houthi-uav-strategy-in-yemen (Accessed: 14 April 2022).

Narodowy Program Ochrony Infrastruktury Krytycznej (2020) Available at: https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej (Accessed: 13 April 2022).

Niedbała, M. (2020) 'Od Półwyspu Arabskiego do Narwi. Atak na rafinerie a polska obrona przeciwlotnicza', *Nowa Technika Wojskowa*, 1/2020, pp. 54–63.

Piekarski, M. (2019) 'Polish Armed Forces and hybrid war: current and required capabilities', *The Copernicus Journal of Political Studies*, 1/2019, pp. 42–64. doi: 10.12775/CJPS.2019.003.

Piekarski, M. and Wojtasik, K. (2020) *Polski system antyterrorystyczny a realia zamachów drugiej połowy XXI wieku.* Toruń: Wydawnictwo Adam Marszałek.

Rogoway, T. (2021) 'Adversary drones are spying on the U.S. and the pentagon acts like they're UFOs', *The War Zone*. Available at: https://www.thedrive.com/the-war-zone/40054/adversary-drones-are-spying-on-the-u-s-and-the-pentagon-acts-like-theyre-ufos (Accessed: 15 April 2022).

Rogoway, T. and Trevithick, J. (2020) 'The night a mysterious drone swarm descended on Palo Verde nuclear power plant', *The War Zone*. Available at: https://www.thedrive.com/the-war-zone/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant (Accessed: 15 April 2022).

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony Infrastruktury Krytycznej, Dz. U. Nr 83, Poz. 542.

Sims, A. (2018) 'The rising drone threat from terrorists', *Georgetown Journal of International Affairs*, 19, pp. 97–107. doi: 10.1353/gia.2018.0012.

Świat Dronów (2022) *Polski system zwalczania dronów – Zakłady Mechaniczne „Tarnów" i WAT*. Available at: https://www.swiatdronow.pl/polski-system-zwalczania-dronow-zaklady-mechaniczne-tarnow-i-wat (Accessed: 13 April 2022).

Tingley, B. (2021) *Drone used high power microwaves to knock down other drones in DARPA demo*. Available at: https://www.thedrive.com/the-war-zone/41025/drone-used-high-power-microwaves-to-knock-down-other-drones-in-darpa-demo (Accessed: 13 April 2022).

Ustawa o ochronie osób i mienia z dn. 22 sierpnia 1997 r., Dz.U. 1997 r., nr 114, poz. 740.

Ustawa o działaniach antyterrorystycznych z dn. 10 czerwca 2016 r., Dz.U. 2016 r. poz. 904.

Ustawa o zarządzaniu kryzysowym z dn. 26 kwietnia 2007 r., Dz.U. 2007 r., nr 89, poz. 590.

Watson, B. (2017) *The drones of ISIS*. Available at: https://www.defenseone.com/technology/2017/01/drones-isis/134542/ (Accessed: 13 April 2022).

Wojtasik, K. (2019) *Anatomia zamachu. O strategii i taktyce terrorystów*. Warszawa: Grupa Medium.

Załącznik 1 do NPOIK Standardy Służące Zapewnieniu Sprawnego Funkcjonowania Infrastruktury Krytycznej. Dobre Praktyki i Rekomendacje.