Wojciech Wosek, Ewelina Parysek, Paweł Wawrzyniak
University of Business and Administration in Gdynia

INNOVATIVE SECURITY STRATEGIES FOR THE PORT OF GDYNIA INFRASTRUCTURE

Abstract: The Port of Gdynia is an operator of critical infrastructure. It is also a dual-purpose port, where the specificity of a merchant and naval port interpermeate. This fact is a challenge in the area of port security, the level of which depends, among others, on the implementation of the Comprehensive Drone System (pol. Kompletny System Dronowy, KSD). The authors of the article present the conclusion that the key to the success of the adopted port security strategy is the integration of all KSD component systems: DTM, LSM and Antydron in one solution and the launch of the local ICT infrastructure under CEDD. It is important here to integrate the solution with the U-space foundation, the central PANSA UTM system. The implementation of KSD also perfectly fits into the framework of the smart port concept and has great development potential, which spans over several decades to come. Therefore, the article presents a number of recommendations regarding the implementation of KSD and further implementation of the smart port concept.

Keywords: Smart Port, Port of Gdynia, KSD, PANSA, UTM, DTM, LSM, Antydron, BSP, drone, U-space, CEDD, cybersecurity, automation.

INTRODUCTION

On March 5, 2020, in the port of Gdynia a grain granary with a storage area of 7000 m^2 (235×30×15), which was located in an area leased by the Baltic Grain Terminal, almost completely burned down. The fire broke out before 9 o'clock and 30 fire crews were dispatched to extinguish it. The port guard and the largest ship of the Maritime Search and Rescue Service – MS Kapitan Poinc, also joined the firefighting operation. The warehouse was filled in one tenth with the goods: soybean and grain. There were no people in the facility at the time of the fire, so, luckily, no one was injured. However, there was a risk of the fire spreading over

adjacent gas storage facilities, two tent halls and the halls of a shipbuilding company constructing yachts. Fortunately, thanks to a smooth operation, firefighters managed to stop the fire. About two weeks after the fire was extinguished, workers noticed smoke coming out of the burned warehouse again. The port dispatcher and the fire brigade were immediately informed. Perhaps the threat could have been detected earlier or neutralised with fewer forces and resources had the security of Gdynia port been supervised by *drones*[1]. Some sensitive loads, such as vegetable oils, cereals, feed, nut shells, or wood chips, which are stored in the port of Gdynia, require constant inspection. In the event of local temperature increase, thermal camera drones could immediately notify the relevant services, operating in 24/7 mode under safe weather conditions.

In September 2019, seven cruise missiles and a swarm of 18 long-range drones with suspended explosives forced their way through Saudi Arabia's advanced air defense systems, destroying the world's largest refinery in Abqaiq and Khurais and the processing installations there. This event has had a huge global impact. Yemeni rebels from the Houthi movement have taken responsibility for this precise attack, which halved Saudi Arabia's oil and gas production and increased prices of these raw materials on the global market[2]. The report presented at the UN Security Council meeting identified many similarities between the drones used in the attack and Iran's IRN-05 unmanned aircraft[3].

These two events described above are just some examples of extremely different incidents – the contrast between them highlights the potential of drone technologies, both in the area of support for critical infrastructure security systems and new potential threats that involve a previously unidentified risk of large-scale use of Unmanned Aerial Vehicles (in short: UAV).

In order to face today's challenges in the area of critical infrastructure security, in April 2019, during the conference "Security of critical infrastructure and mass events in the era of technological breakthrough of the 21st century" („*Bezpieczeństwo infrastruktury krytycznej oraz imprez masowych w dobie przełomu technologicznego XXI w.*"), the Port of Gdynia Authority S.A. (*Zarząd Morskiego Portu Gdynia S.A.*, ZMPG) announced plans to implement an innovative, comprehensive drone system (*kompletny system dronowy* – KSD), and at the end of 2019 signed a letter of intent with Pelixar S.A. from the Pomeranian Science and Technology Park (*Pomorski Park Naukowo-Technologiczny* – PPNT) for the im-

---

1 *Pożar w Porcie Gdynia. Niemal doszczętnie spłonął spichlerz zbożowy, https://gdansk.tvp.pl/46987346/pozar-w-porcie-gdynia-niemal-doszczetnie-splonal-spichlerz-zbozowy*, [access: 28.06.2020].

2 In an interview with Der Spiegel, Mohamed Ali al – Houthi claims that the Houthis are in possession of drones: Samad – 1, Samad – 2, Samad – 3 and Qasef – 1 (according to their data with a range of 1500 km.). Vide: „Forum" 21/2019, p. 27; N. Sharkey, *Broń autonomiczna*, „Świat Nauki", 2020, nr 4 (344), p. 38.

3 H. Pamuk, *U. S. probe of Saudi oil attack shows it came from north – report*, https://www.reuters.com/article/us-saudi-aramco-attacks-iran-exclusive/exlusive-u-s-probe-of-saudi-oil-attack-shows-it-came-from-north-report-idUSKBN1YN299, [access: 28.06.2020].

plementation of the Aviation Monitoring System (pol. *Lotniczy System Monitoringu* – LMS)[4]. Those are the elements of the Gdynia port infrastructure security strategy that this study is devoted to.

SHORT CHARACTERISTICS OF UNMANNED AERIAL VEHICLES

UAVs are piloted remotely (are not autonomous) by operators or have autonomy (limited or total). For this reason, the abbreviation UAV is sometimes developed as "Unmanned Aerial Systems" (UAS). Fully autonomous drones are also considered as a component of Autonomous Weapons Systems (AWS) and – as many researchers point out – are likely to participate in hostilities today[5]. The armed versions of the UAVs, intended for combat operations, are referred as the Unmanned Combat Air Vehicles (UCAV)[6]. The degree of autonomy or control of the UAV by the human (operator) can be determined according to the following scale, relating to the location of the operator in the so-called control loop:[7]

- Human in the loop – the operator remotely controlling UAV (or other device, e.g. a robot) fully retains control over its actions.
- Human on the loop – UAV has a high degree of autonomy, moves independently and searches for goals. In the case of UCAV, it attempts to attack the target, but the operator must authorise this decision.
- Human out of the loop – fully autonomous UAV (or any other device, e.g. robot, UCAV, etc.).

UAVs are very diverse not only in terms of degree of autonomy, but also in size, weight or construction (vide: Fig. 1). We distinguish here[8]:

1. Single rotor, Multi-rotor drones – i.e. rotorcrafts with rotors in essentially vertical axes (e.g. Black Hornet Nano, 10×2.5 cm);
2. Fixed Wing drones – aerodynes[9] with fixed load-bearing surfaces (e.g. Chinese Feihong-98 in size Antonov AN-2 aircraft[10]).

---

4 *Port Gdynia w nowej erze bezpieczeństwa – list intencyjny pomiędzy Zarządem Morskiego Portu Gdynia S.A., a firmą Pelixar S.A.*, https://oficynamorska.pl/2019/port-gdynia-w-nowej-erze-bezpieczenstwa-list-intencyjny-pomiedzy-zarzadem-morskiego-portu-gdynia-s-a-a-firma-pelixar-s-a/, [access: 28.06.2020].

5 N. Sharkey, *Broń*.

6 P. Polko, R. Polko, *It was safe already*, Gliwice2018, p. 56.

7 *Ibidem*, p. 60.

8 Vide: P. Burdziakowski, *Groźne platformy*, „Przegląd Sił Zbrojnych", 2017, nr 4, pp. 120-127.

9 *Aerodyne* (gr. *a r* – air, gr. *dýna(mis)* – force) – an aircraft heavier than air, floating in the atmosphere as a result of air exposure to its supporting surfaces. Based on: *Aerodyna*, https://encyklopedia.pwn.pl/haslo/aerodyna;3866014.html, [access: 28.06.2020].

10 It is worth noting that the airframe Antonov AN-2, which became the basis for the construction of the Feihong-98, was flown already in 1947. The Chinese version of Antonov AN-2 is known as Yun-5.

Contrary to stereotypical opinions, most drones do not carry combat payloads and are used only for the collection of intelligence. Therefore the solutions designed for the military are so willingly used by other formations and institutions dealing with e.g. monitoring of national borders, search for missing persons, emergency rescue, observation of weather changes, spread of natural disasters or, precisely, monitoring the condition and ensuring the safety of critical infrastructure. Consequently UAVs are widely used not only in the military but also in the civilian sector, including applications such as recreation, business and industry[11].

Fig. 1. On the left, the Black Hornet Nano combat drone (photo: Corporal Daniel Wiepen/MOD); on the right, transport drone Feihong-98. You can see the difference in size, weight, construction and purpose of UAVs[12].

It is worth recalling the PrimeAir initiative implemented by Amazon, which (for the first time in 2013) presented the concept of delivery drones – allowing to deliver the shipment to the customer's place of residence of their own e--commerce platform. The development of this concept continues to this day and still requires overcoming a number of technological and legal challenges related to inter alia air traffic safety[13]. In 2017, the Civil Aviation Authority of Israel (CAAI) has given Israeli startup Airobotics a permission for commercial and completely autonomous flights in Israel[14].

---

11 P. Polko, R. Polko, *Bezpiecznie…*, p. 56.

12 Own study based on: (1) A. Pawłowski, US Army zamówiła miniśmigłowce Black Hornet Nano, https://www.konflikty.pl/aktualnosci/wiadomosci/us-army-minismiglowce-black-hornet-nano/, [access: 28.06.2020]; (2) SF Express, the express delivery giant in China, showcases its unmanned aerial vehicle. The UAV is called FH98, which is based on a retired Yun-5, https://twitter.com/ChinaAvReview/status/1052013620920377344/photo/3, [access: 28.06.2020].

13 M. Zawadzak, *Nowe drony Amazon PrimeAir robią wrażenie!*, http://www.swiatdronow.pl/nowe-drony-amazon-primeair-robia-wrazenie, [access: 28.06.2020].

14 L. Kolodny, *Airobotics scores authorization to fly autonomous drones in Israel*, https://techcrunch.com/2017/03/27/airobotics-scores-authorization-to-fly-autonomous-drones-in-israel/, [access: 28.06.2020].

The potential of the UAVs and the entire market associated with this technology can be demonstrated by the following figures:[15]

- 73.5 billion USD – the value of the global civilian drone market for 2017–2026;
- 20.7 billion USD – the value of the European civilian drone market in 2017–2026;
- 3.26 billion PLN – the value of the Polish civilian drone market in 2017–2026;
- 100,000 – the number of drones in Polish airspace.

All these features present a challenge of integrating drone technologies into the economy nowadays. This requires action in the area of regulation, technical infrastructure, as well as the development of products and services that will benefit from the availability of airspace. It is estimated that the value of integrating drones into the economy, i.e. the indirect benefits that the economy as a whole can bring, is significantly higher than the value of the drone market itself, calculated as the value of the equipment produced[16]. The key issue here is the development of the U-space environment, which will open up a whole new market for technology and services. The initial value of this market estimated over the period of 10 years includes 310 billion PLN according to a pessimistic scenario, 576 billion PLN according to a moderate scenario, and based on the assumptions of an optimistic scenario up to 913 billion PLN in economic benefits[17].

U-SPACE CONCEPT

U-space is a widely accepted term in the European Union covering all aspects of UAVs integration into the economy. Poland has been actively involved in the creation of this concept and is now one of the leading Member States in its development. This term is not used outside the European Union[18]. The main pillars of the U-space are shown in Fig. 2.

The gradual development of the U-space environment, with the technological development of UAVs, including system elements to improve UAVs' flight management and legislation, will involve the use of drones in areas where they have not yet been used at all or to a small extent. Commercial use of UAVs will become increasingly common in industry, agriculture, infrastructure investment and construction[19], as well as in the wider sense of emergency rescue and security. Drones

---

15 *Biała Księga Rynku Bezzałogowych Statków Powietrznych. U-Space – Rynek – Wizja Rozwoju*, red. M. Witeska i J. Nowak, Warszawa 2019, p. 4.
16 *Ibidem*, p. 5.
17 *Ibidem*.
18 *Ibidem*, p. 10.
19 *Ibidem*, p. 29.

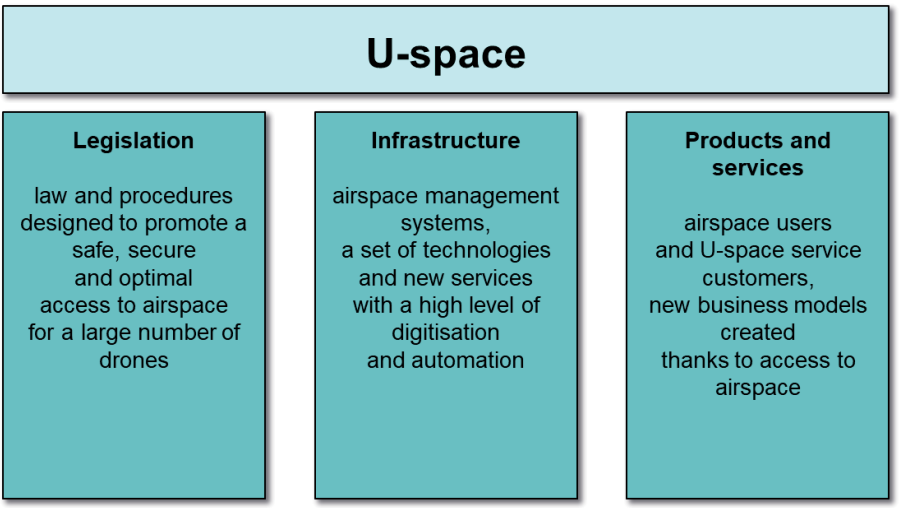

Fig. 2. Three pillars of U-space[20].

will also increasingly appear in cities, which entails the need to define new rules and involve local authorities in the process of managing access to airspace. Large--scale drone operations will require investment in ground infrastructure and the detailed organisation of UAV flights in urban areas, which may even lead to changes in the urban layout[21]. This poses a major challenge, which is also faced by the ZMPG, deciding to implement an innovative security strategy, which contains the UAV component, for the Port of Gdynia infrastructure. In general, U-space can be defined as: *infrastructure for the UAVs, which is to enable collision-free, integrated drone operations in airspace in the future, in particular commercial, economic and state operations*[22]. U-space is an ecosystem that is gradually being developed, in line with the development of technologies that enable increasingly automated processes and autonomous drone operations[23].

ON THE WAY TO THE COMPLEMENTARY DRONE SYSTEM OF THE PORT OF GDYNIA

Poland's unique position in the global drone market is mainly due to user--friendly legislation, the rapid development of unmanned technologies and the largest number of UAVO-qualified operators after the USA and Japan[24]. Between

[20] Own study based on: *Biała Księga Rynku Bezzałogowych Statków Powietrznych. U-Space – Rynek – Wizja Rozwoju*, pod. red. M. Witeska i J. Nowak, Warszawa 2019.
[21] brak przypisu
[22] Vide: *U-Space*, http://cedd.pl/start/jak-dziala-cedd/, [access: 28.06.2020].
[23] *Ibidem.*
[24] (1) UAVO – *Unmanned Aerial Vehicle Operator*; (2) *Port Gdynia w Nowej erze.*

2013 and 2018, the Civil Aviation Authority (pol. *Urząd Lotnictwa Cywilnego*, ULC) issued almost 10,000 UAVO certificates of qualification. During the same period, only 72 incidents involving drones were reported[25].

The greatest asset of Poland, however, is the Central European Drone Demonstrator (CEDD), a program whose task is to create recommendations and procedures for future legislative processes and implement the U-space concept in the country. CEDD has dedicated DroneLabs, task force cells that focus on specific sectors such as U-Space, transport, environment, energy and security. According to the agreement of September 30, 2019, Port of Gdynia became the owner of Security DroneLab, one of the most promising and interesting sectors of CEDD[26].

The Port of Gdynia is of significant geostrategic importance for the country, it is the operator of the Polish critical infrastructure. It is a dual-purpose seaport in which the specificity of a commercial and war port permeates, and both civilian and military infrastructure are present here. The port operates under NATO's HNS programme[27], hosting the North Atlantic Alliance's military force. There are also business entities interested in a high level of security in connection with their business activities and trade secrets[28]. This is a particular challenge in the area of port security, the level of which will depend on – inter alia – the implementation of the Comprehensive Drone System (KSD) of the Port of Gdynia, in the assumptions consisting of the following systems[29]:

- DTM (*Drone Traffic Management*) – a system for managing UAVs' flights over the Port of Gdynia;
- „AntyDron" – a control system dedicated to the detection in the airspace, identification and neutralisation of unauthorised drones;
- LSM (pol. *Lotniczy System Monitoringu* – Aviation Monitoring System) – a system using unmanned aerial vehicles to identify and verify security and crisis events.

Fig. 3 shows a high-level vision of KSD IT architecture for Port of Gdynia.

---

25 *Biała Księga…*, p. 41.

26 *Port Gdynia w nowej erze….*

27 Poland, as a member of the North Atlantic Treaty Organisation (NATO), has been obliged to respect allied commitments. One of them is to support allied forces coming to our country, as host nation, under Host Nation Support (HNS) system. The proper implementation of Poland's support is crucial for the defence of our country, along with its credibility as a partner of allied troops. Vide: S. Łazarek, *Polska jako państwo-gospodarz w ramach systemu HNS*, https://rcb.gov.pl/polska-jako-panstwo-gospodarz-w-ramach-systemu-hns/, [access: 28.06.2020].

28 Vide: (1) T. Jurczak, *Port w Gdyni planuje wykorzystać drony do wsparcia monitoringu, bezpieczeństwa ludzi i analizy zanieczyszczeń*, https://www.sztucznainteligencja.org.pl/nad-portem-gdynia-beda-czuwac-drony/, [access: 28.06.2020]; (2) *Port Gdynia w nowej erze….*

29 *Port Gdynia w nowej erze….*

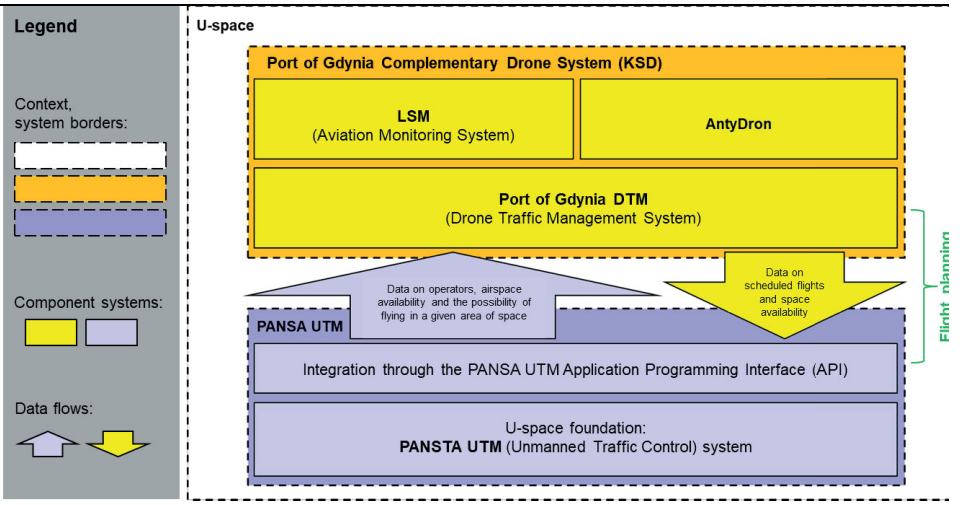

Fig. 3. High-level vision of KSD IT architecture for Port of Gdynia

OWN STUDY

Key to KSD's operation is integration with the U-space foundation, the PANSA (Polish Air Navigation Services Agency – pol. *Polish Air Navigation Agency*, PAŻP) UTM system (Unmanned Traffic Control), which is a central system for coordinating and managing drone traffic, operated by PAŻP. Thanks to integration through the appropriate protocols and usage of the API (Application Programming Interface), PANSA UTM can exchange data with vendor-based on-premises DTM systems that operate across the country – e.g. Port of Gdynia DTM. On the other hand, the Port of Gdynia DTM system acts as a local UTM system and is intended to support the management of UAVs flights over the port area[30]. The data exchanged between PANSA UTM and Port of Gdynia DTM systems are necessary in the UAVs flight planning process – the exchanged data scope is as follows:

- From Port of Gdynia DTM system to PANSA UTM system – data on planned flights and availability of airspace of the Port of Gdynia.
- From PANSA UTM system to Port of Gdynia DTM system – data on operators, space availability and the possibility of flight in the airspace of the port.

In addition to the Port of Gdynia DTM, under KSD also LSM and AntyDron systems are being operated. The first, LSM, supports the implementation of – inter alia – such tasks as:

- environmental monitoring of water and air,

[30] At the time of writing, the Port of Gdynia DTM system tests were in progress.

- control of technical infrastructure,
- monitoring of security threats,
- verification of emergency calls,
- monitoring of bulk material depots,
- operational support during protests (e.g. environmentalists),
- support for Search&Rescue (SAR) operations within the port's administrative precinct,
- operational support in the event of environmental contamination,
- the supply of emergency or medical supplies between the port and the ship.

The second system, AntyDron, is responsible for:

- detection and identification of unmanned aerial vehicles,
- interfering and neutralising the work of the UAVs,
- forcing UAVs to land,
- preventing foreign drones from entering port's airspace,
- tracking of flying objects that have breached the port airspace.

All KSD component systems, i.e. local DTM system (ensuring integration with the central PANSA UTM system), LSM and AntyDron should eventually be integrated for maximum usability of the solution. A system deployment project of this complexity requires a step-by-step approach and multiple tests, so it is expected that KSD will gradually achieve its full functionality. Here appears, inter alia, a number of challenges in the area of cybersecurity, and the system itself has a high potential for development, which can be placed in the perspective of a dozen years or even decades. It is worth emphasizing that KSD fits perfectly into the smart port concept, which involves the use of not only air drones, but also water (marine) drones[31], e.g. in the area of port security.

INNOVATIONS IMPLEMENTED BY PORTS. SMART PORT CONCEPT

According to *Port Cybersecurity*[32] report by European Union Network and Information Security Agency (ENISA), it is recommended that ports develop their own cybersecurity and infrastructure, as well as data protection. The general trend towards digitalization obliges ports to meet new technological directions, while the smart port[33] concept aims to innovate and increase port security. The necessary premise of this approach, given the high competitiveness of ports, is to

[31] Water drones (aquatic drones); marine drones (sea drones).

[32] *PORT CYBERSECURITY. Good practices for cybersecurity in the maritime sector*, https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector, [access: 28.06.2020].

[33] Koncepcja smart port według Yann Alix. Vide: *What is a smart port?*, http://parisinnovationreview.com/articles-en/what-is-a-smart-port, [access: 28.06.2020].

implement technologies from the areas of artificial intelligence, big data analysis[34], blockchain[35], cloud computing[36] or the Internet of Things[37].

The smart port concept involves integration of seaport security systems, as well as automation of port equipment and processes. In the context of this type of integration, the potential of KSD of the Port of Gdynia, which can be part of a long-term development strategy in line with the smart port concept, is revealed. It should be noted that one of the key challenges facing modern seaports is the increase in competitiveness and efficiency of transshipment operations. However, these objectives cannot be achieved at the expense of security. The introduction of autonomous transshipment facilities will minimise the risk of accidents. It will also significantly increase the efficiency of handling processes by making the most of the equipment's uptime. In order to improve port operations, it is advisable to use aerial and water (marine) drones[38]. Drones are used in places where other technical solutions cannot be used, e.g. in the case of structures that are difficult to reach for humans or specialised machinery and, in particular, in work that endangers human health and life.

In turn, the automation of devices supporting the water zone through the use of e.g. marine drones will significantly affect the safety of ship traffic in port channels and allow better planning and implementation of transshipment tasks. The smart port concept identifies a wide field of use for aerial and water (marine) drones. For air drones, inter alia, the following tasks are assumed:

- port infrastructure inspection,
- inspections of quays, buildings, cranes, holds, pipeline routes, solar panels,
- monitoring terminals for security,

---

34 Ports run Big Data projects to increase correlations of data collected and processed, as well as to improve port security and security processes. For example, the port of Valencia has launched an innovative Big Data project with the intention of improving the efficiency of terminal logistics and advanced navigation. Vide: *PORT CYBERSECURITY…*, p. 57.

35 The blockchain system, in relation to the needs of seaports, is designed to secure distribution and workflow of documentation.

36 Some European ports have launched cloud projects to exchange data on an ongoing basis in a centralised way, such as the Port Single Window system, which is the central port data management system. The assumption of this approach is the flow of information between the Port Authorities, the operators and the Customs Office.

37 With the IoT platform it is possible to monitor port infrastructure, reloading works and to collect data. The implementation of the sensor system and RFID technology is crucial here, e.g. the Port of Rotterdam launched its own IoT platform by installing sensors on buoys and quays to optimise ship docking time and location. Vide: *PORT CYBERSECURITY…*, p. 57.

38 The ports of Amsterdam and Rotterdam have made their air and sea areas available to drones to improve port operations. Vide: (1) *Drones in the Amsterdam port area*, https://www.portofamsterdam.com/en/port-amsterdam/drones-amsterdam-port-area, [access: 28.06.2020]; (2) Vide: *Water drone is Rotterdam's latest port innovation*, https://www.portofrotterdam.com/en/news-and-press-releases/water-drone-is-rotterdams-latest-port-innovation, [access: 28.06.2020].

- supporting port supervisory authorities,
- taking action in specific situations, e.g. in the case of a detection of flameless fire and subsequent notification to the relevant services. It is advisable that the drones used for this type of activity have smoke detectors, optical and ionising sensors,
- control of maintenance on board ships, terminals,
- deliveries to ships and oil rigs,
- medical transport (e.g. blood and human organs),
- passenger transport (e.g. in rescue operations),
- transport of heavy loads,
- transport of materials to ships (supporting the offshore industry).

On the other hand, the potential use of water (marine) drones[39] is:

- use of unmanned boats equipped with a camera that can send images of the quay and thus carry out surveillance and inspection from the water surface (the aim is to complement the work of manned patrol boats),
- controlling the water environment to identify and neutralise unauthorised marine drones[40],
- constant inspection and reporting of the underwater quay lines' technical condition,
- monitoring of concrete structures, e.g. oil terminals,
- control of the water condition in terms of contamination (sampling),
- detection of leakages of liquids and hazardous substances using, inter alia, a thermal imaging camera,
- removal of waste from water, clearing docks,
- checking the quality status of the sides, rudders and propellers in ships moored in port,
- the role of harbour pilots (supporting ships' entrance to and exit from ports),
- determination of volume, dimensions of bulk goods,
- underwater search (drowned bodies or materials, etc.).

It should be emphasised that cybersecurity must be maximised, before such complex and extensive systems for managing infrastructure and port facilities, assuming a high degree of system integration and the amount of data processed, will be implemented.

---

39 Cf. *Pojazdy bezzałogowe. Autonomiczny dron morski*, http://atol.umg.edu.pl/ev/dron/dron.html, [access: 28.06.2020].

40 Organised crime groups use air drones and small submarines to smuggle drugs. It is believed that it is a matter of time before autonomous ships integrate with marine drones to increase the efficiency of logistics and drug transport. Cf. (1) *Skuteczniejsze wykrywanie małych statków powietrznych i dronów ułatwi ochronę europejskich granic morskich*, https://cordis.europa.eu/article/id/418277-better-detection-of-small-aircraft-and-drones-helps-protect-europe-s-maritime-borders/pl, [access: 28.06.2020]; (2) *Robot Boats and Drug Subs. ENG prof and students developing autonomous boats to find drug traffickers*, https://www.bu.edu/articles/2017/autonomous-boats-and-drug-subs/, [access: 28.06.2020])

The main challenges of the smart port concept are:

- raising awareness and trainings on cybersecurity in the port ecosystem,
- building cybersecurity strategies,
- introduction of adequate security measures to protect against cyber-attacks,
- increasing the time and budget for cybersecurity,
- qualified management of automated equipment,
- complexity of information technology (IT) and operational technology (OT) integration.

Despite such serious challenges, the long-term implementation of the Smart Port concept can ensure significant benefits for the port. It is worth mentioning that a number of tasks defined under the smart port concept for air drones will soon be carried out in the Port of Gdynia, thanks to the implementation of KSD. Moreover, in the future, water (marine) drones can interact with aerial drones under the control of KSD (vide: Fig. 4).

Fig. 4. One of the water (marine) drones used in the Port of Rotterdam, the Netherlands[3]

The idea of using water (marine) drones also indicates the direction of further potential development of the KSD and expansion of its functionalities, or a possible area of integration with another dedicated port system responsible solely for the supervision of water (marine) drones operating in the port water zone, as part of a long-term strategy for the implementation of the smart port concept. However, it should be borne in mind that the assumption of such an approach creates further dangers associated with cyberattacks. The fundamental question is: will the financial outlay on cybersecurity not be greater than the benefits of implementing the smart port concept?

41 Own study based on: *Water drone is Rotterdam's latest port innovation*, https://www.portofrotterdam.com/en/news-and-press-releases/water-drone-is-rotterdams-latest-port-innovation, [access: 28.06.2020].

CHALLENGES AND RECOMMENDATIONS FOR KSD OF THE PORT OF GDYNIA

In the course of analysis of the KSD of the Port of Gdynia potential, the following challenges were identified, which are important for the success of the project:

- the combination of civil and military infrastructure in the Port of Gdynia – the problem here concerns e.g. radio interference,
- providing a technical backshop for drones, including places for charging, storing, modernizing, servicing and operating – in addition to the implementation of KSD, future plans for day-to-day operation should be developed,
- UAV's resistance to extreme weather – will KSD operate in strong breeze or fresh gale conditions (limit of 6B, 7B or 8B)?[42]
- 24/7 continuous operation – does KSD provide organizational and technical 24/7 continuous operation capabilities? What is the estimated annual availability time of the system including failures, service, planned inspections and variability of weather conditions?
- functional requirements definition, e.g. monitored parameters, logged events, authentication and authorization/permission control, interfaces to other systems and APIs, etc. – there must be an accurate specification of the requirements for the system,
- non-functional requirements definition, e.g.: availability, resiliency, security, scope and degree of integration, scalability, data retention, etc. – it is suggested to draw up an accurate specification of the requirements for the system,
- cybersecurity and cyber-resilience – the system should absolutely be resistant to the attempts of cybernetic impact.

In view of the above, it is recommended to:

- recognise KSD as a strategic project in the area of security of the Port of Gdynia,
- carry out a deep and regularly repeated risk analysis,
- conduct the analysis of issues related to the protection of sensitive data and the privacy of persons within the scope of the system,
- ensure that the agreement clearly defines the responsibilities of the Supplier and the Recipient of KSD (ZMPG),
- precise the specification of functional and non-functional requirements and scope of integration of KSD (e.g. PANSA UTM, other existing Recipient's systems, etc.),

[42] Description of the wind force in Beaufort scale is using degrees. Strong breeze is 6B; high wind, moderate gale and near gale is 7B; gale and fresh gale is 8B.

- establish a team of experts on the side of the ZPMG,
- monitor the work progress carried out by the Supplier within the monitoring committees and the project steering committee on a regular basis,
- verify the compliance of the solutions provided by the Supplier with the contract at each stage of implementation,
- build the knowledge and competences in the operation of the integrated KSD already at the design stage,
- carry out penetration, integration and load tests before the acceptance of delivered KSD (preferably by a third party),
- perform User Acceptance Testing (UAT) before the acceptance of delivered KSD (via ZMPG),
- take the view that the integration of all systems into a single solution and the deployment of local IT infrastructure within the CEDD are essential for the success of the port security strategy.

SUMMARY

The purpose of this article was an attempt to present selected innovative security strategies for the infrastructure of the Port of Gdynia, taking into account the use of unmanned aerial vehicles (UAV's) as part of the implementation of the smart port concept. The article pays particular attention to the challenges related to the plans for the implementation by the Port of Gdynia Authority SA the Comprehensive Drone System (KSD) and the integration of UAV's with the maritime economy. It was recommended that integration with the U-space foundation, the PANSA UTM system, is crucial for the operation of this system. In particular, it is indicated that all components of the KSD system, i.e. DTM, LSM and Antydron, are integrated to achieve the full usability of the solution.

The aim of the article was to determine the extent to which Port of Gdynia could use aerial and water (marine) drones, as well as identify the challenges relevant to the success of this project. Global digitisation obliges Port of Gdynia to initiate new solutions in the area of cybersecurity and infrastructure. The biggest challenge is to gain the benefits from the implemented innovative concepts that justify the financial outlays. The challenges and recommendations set out in the article may be the beginning of further research into port infrastructure security.

BIBLIOGRAPHY

LITERATURE

Biała Księga Rynku Bezzałogowych Statków Powietrznych. U-Space – Rynek – Wizja Rozwoju, red. M. Witeska i J. Nowak, Warszawa 2019.

Polko P., Polko R., *Bezpiecznie już było*, Gliwice 2018.

MAGAZINES AND ARTICLES

„Forum" 21/2019.

Sharkey N., *Broń autonomiczna*, „Świat Nauki", 2020, nr 4 (344).

Burdziakowski P., *Groźne platformy*, „Przegląd Sił Zbrojnych", 2017, nr 4.

INTERNET SOURCES

Drones in the Amsterdam port area, https://www.portofamsterdam.com/en/port-amsterdam/drones-amsterdam-port-area

Jurczak T., *Port w Gdyni planuje wykorzystać drony do wsparcia monitoringu, bezpieczeństwa ludzi i analizy zanieczyszczeń*, https://www.sztucznainteligencja.org.pl/nad-portem-gdynia-beda-czuwac-drony/.

Kolodny L., *Airobotics scores authorization to fly autonomous drones in Israel*, https://techcrunch.com/2017/03/27/airobotics-scores-authorization-to-fly-autonomous-drones-in-israel/

Łazarek S., *Polska jako państwo-gospodarz w ramach systemu HNS*, https://rcb.gov.pl/polska-jako-panstwo-gospodarz-w-ramach-systemu-hns/

Pamuk H., *U. S. probe of Saudi oil attack shows it came from north – report*,. https://www.reuters.com/article/us-saudi-aramco-attacks-iran-exclusive/exlusive-u-s-probe-of-saudi-oil-attack-shows-it-came-from-north-report-idUSKBN1YN299

Pawłowski A., *US Army zamówiła miniśmigłowce Black Hornet Nano*, https://www.konflikty.pl/aktualnosci/wiadomosci/us-army-minismiglowce-black-hornet-nano/

Pojazdy bezzałogowe. Autonomiczny dron morski, http://atol.umg.edu.pl/ev/dron/dron.html

PORT CYBERSECURITY. Good practices for cybersecurity in the maritime sector, https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

Port Gdynia w nowej erze bezpieczeństwa – list intencyjny pomiędzy Zarządem Morskiego Portu Gdynia S.A., a firmą Pelixar S.A., https://oficynamorska.pl/2019/port-gdynia-w-nowej-erze-bezpieczenstwa-list-intencyjny-pomiedzy-zarzadem-morskiego-portu-gdynia-s-a-a-firma-pelixar-s-a/

Pożar w Porcie Gdynia. Niemal doszczętnie spłonął spichlerz zbożowy, https://gdansk.tvp.pl/46987346/pozar-w-porcie-gdynia-niemal-doszczetnie-splonal-spichlerz-zbozowy

Robot Boats and Drug Subs. ENG prof and students developing autonomous boats to find drug traffickers, https://www.bu.edu/articles/2017/autonomous-boats-and-drug-subs/

SF Express, the express delivery giant in China, showcases its unmanned aerial vehicle. The UAV is called FH98, which is based on a retired Yun-5, https://twitter.com/ChinaAvReview/status/1052013620920377344/photo/3

Skuteczniejsze wykrywanie małych statków powietrznych i dronów ułatwi ochronę europejskich granic morskich, https://cordis.europa.eu/article/id/418277-better-detection-of-small-aircraft-and-drones-helps-protect-europe-s-maritime-borders/pl

U-Space, http://cedd.pl/start/jak-dziala-cedd/

Water drone is Rotterdam's latest port innovation, https://www.portofrotterdam.com/en/news-and-press-releases/water-drone-is-rotterdams-latest-port-innovation

What is a smart port?, http://parisinnovationreview.com/articles-en/what-is-a-smart-port

Zawadzak M., *Nowe drony Amazon PrimeAir robią wrażenie!*, http://www.swiatdronow.pl/nowe-drony-amazon-primeair-robia-wrazenie