ISSN: 2450-6869

eISSN: 2719-6763

No. 11, 2021

DEFENCE SCIENCE REVIEW

http://www.journalssystem.com/pno/

DOI: 10.37055/pno/147400

Development directions of cybersecurity in aerospace

Original article

Received: 2021-11-21

Revised: 2022-03-15

Accepted: 2022-03-15

Final review: 2022-03-15

Peer review:

Double blind

Aleksandra Radomska[1,D]
ORCID 0000-0003-4486-8437

[1]Military University of Technology, Poland

A – Research concept and design, B – Collection and/or assembly of data, C – Data analysis and interpretation, D – Writing the article, E – Critical revision of the article, F – Final approval of article

Corresponding author: Aleksandra Radomska; Wojskowa Akademia Techniczna, ul. gen. Sylwestra Kaliskiego 2, 00-908, Warszawa, Poland, e-mail: aleksandra.radomska@wat.edu.pl

Introduction

Aviation radionavigation systems – radionavigation aids and global navigation satellite systems – and the possibilities of their interference – expert interview with Lt. Col. Navigator Rafał Zajkowski Sc.D.

Aleksandra Radomska: What are the most commonly used aviation radionavigation aids in civil aviation, and what in military aviation, and does their selection affect the accuracy |of data provided to aircraft crews?

Rafał Zajkowski: First of all, it is necessary to divide radionavigation aids into two basic groups: military and civil. The most commonly used radionavigation aids in military aviation are Non-Directional Beacon (NDB) and Tactical Air Navigation (TACAN). With reference to the Non-Directional Beacon (NDB), a dual array of ground development of this radionavigation aid is usually used, i.e., a closer NDB and a farther NDB. The military aircraft crewmember then tunes the airborne component equipment to the frequency of NDB beacon; first the farther beacon, then the closer beacon. In addition, NDB beacons generate a non-directional signal and can also transmit Morse code. Despite the fact that they are very basic radionavigation aids, they are still widely used in military aviation. In contrast, the Tactical Air Navigation System TACAN has the ability to provide more precise indications than the Non-Directional Beacon NDB, including the ability to determine azimuth through it. As for the radionavigation aids used in civil aviation, VHF Omni-directional Range (VOR), coupling its operation with Distance Measuring Equipment (DME) in VOR/DME configuration and Instrument Landing System (ILS) are used. The selection of radionavigation aids is determined by the need to provide the most accurate indications to aircraft crews. They are constantly modernized (e.g. by maintaining communication with non-directional beacons NDB, it is possible to send voice signals by the crew in emergency situations). In addition to modernized radionavigation aids, technical devices of newer generations guarantee the highest level of accuracy in providing navigation data (e.g. the ILS system).

Aleksandra Radomska: Do you recognize the possibility of interference with aviation radio aids using technical devices such as jammers, and what effect might this have on the safety of aircraft operations?

Rafał Zajkowski: Yes, this scenario is very real. The radionavigation aids are radio technical devices, receiving and transmitting electromagnetic waves, so jamming them through jammers is a standard practice used during military missions, including Afghanistan. From my own experience, I can say that for the purpose of jamming enemy systems and equipment during a patrol, conducted outside the area of military base, Rosomaks with jammers were used. A significant problem was the range of these jammers, because they also jammed our own equipment, systems and radionavigation aids in case of their close proximity to the base. Consequently, for military operations, jamming enemy technical infrastructure is a precedent commonly used to "blind" the enemy, so to speak. However, in civil aviation, it is also possible to jam the operation of radionavigation aids. However, this is not practiced on such a large scale as in military aviation, but may be perceived as an act of unlawful interference or an act of aviation terrorism. In addition, it is worthwhile at this point to distinguish the meaning between Instrument Flight Rules (IFR) and Visual Flight Rules (VFR) flight operations in case the radionavigation aids would be completely jammed. The more serious consequences for the safety of flight operations in such a situation may occur during the IFR flight, on the approach stage. It is related to the reading of information shown on the on-board indicators, which in such circumstances are erroneous and completely useless. In such situation it is possible for the crew to establish communication with the approach controller in order to divert the aircraft to the alternate airport, where all the radionavigation aids operate continuously and in accordance with their purpose. The prerequisite for taking such action is the determination, based on on-board indicators, that the radionavigation aids are not functioning properly.

Aleksandra Radomska: In your opinion, is there a possibility that in the future radionavigation aids will be deployed at airports in a mobile and feasible way to relocate their design/construction to another place?

Rafał Zajkowski: Yes, the ground component of ground-based radionavigation aids can be relocated in a mobile manner to another location. Let me use the example of the NDB. When performing military missions, it is most often installed on armored vehicles, transported on them and unfolded before use, and seamlessly folded up right after. Not only radionavigation aids have the property of mobile portability, but also include MOSKIT and SALKIT electrolights for illuminating field runways and landing surfaces, "portable" air traffic control tower (TWR) and command posts. Generally speaking, there is a great need for mobility of facilities and equipment of all kinds in the armed forces. With respect to the aspect of using mobile radionavigation aids in civil aviation, there is no need to move their technical infrastructure to another location. Such a need does not have to occur in the future. However, I do not exclude the possibility that in a few years there will be a project of entirely mobile radionavigation aids dedicated to civil aviation.

Aleksandra Radomska: In your opinion, what could be the development directions of aviation radionavigation aids in the technical aspect?

Rafał Zajkowski: Current trends in the development of radionavigation aids are not unambiguous and can be set simultaneously in several directions. It is reasonable to say that future radionavigation aids will be much less deployed on the ground as a ground component. It is worth noting that the specialized equipment provided by Airborne Early Warning And Control (AWACS) aircraft have the capability to provide navigational data to the crews of other aircraft, thus the option exists for them to replace ground-based components of radionavigation aids. Another prediction for the development of radionavigation aids is their cooperation with satellite navigation systems, and sometimes their complete withdrawal in favor of space technologies.

Lt. Col. Navigator Rafał Zajkowski Sc.D. has 15 years of operational experience in air traffic control (ATC) in the positions of Precision Approach Radar (PAR) and Approach Pilot Program (APP) on the RSL-10 system. TWR controller, On-the-Job Training Instructor. Section Chief and Air Traffic Controller on 7th, 10th, 13th shift of Polish Military Contingent Afghanistan. Currently a specialist in aviation guidance in combat conditions following the Joint Terminal Attack Controller (JTAC) course.

Cybersecurity regulation in aviation security – an expert interview with a senior ICT security specialist at the Civil Aviation Authority

Aleksandra Radomska: What do you think about the creation of the Computer Security Incident Response Team (CSIRT) as a part of the Civil Aviation Authority's cooperation with the Ministry of Infrastructure and Construction and the signing of an agreement with the European Union Aviation Safety Agency (EUASA) to test a European pilot program related to aviation cybersecurity?

ICT security specialist at the Civil Aviation Authority: Cyber threats to the civil aviation system is a real and serious problem, which in recent years has become increasingly important. It is conditioned by the progressive process of digitalization and increasing interdependence of systems used in aviation. As a result, even seemingly uncomplicated IT incident can seriously disrupt organization of air services, generating serious financial and image losses, and even become a cause of disastrous events with human casualties and destruction of very expensive aviation infrastructure. This concerns: airlines, airports, air traffic management entities, as well as other key service operators in the aviation subsector, the services of which are interrelated and often interdependent. Nowadays, there is also a general trend to consider cybersecurity issues also through the prism of individual sectors and industry activities in Europe and worldwide, emphasizing the need to develop operational capabilities and information exchange. Therefore, there is a need to look for solutions that, on the one hand, would meet the needs of the actors, and on the other, would be compatible with already existing (or emerging) solutions in the international and national arena. Going to the heart of this issue, in the case of the Polish aviation subsector, a solution could be the creation of an analytical and expert center for cybersecurity in aviation, which would also be an operational support center for national entities of the subsector, in case of an incident. In this regard, high hopes are raised by the idea of creating a specialized Computer Security Incident Response Team with administrative and substantive background in the field of civil aviation in Poland. This direction of action is fully justified, because many sectors mentioned in the Aviation Law of July 2, 2002 and the NIS Directive, are characterized by their own industry specifics. Not all incidents occurring in those sectors may be classified as “critical” according to national legislation on cybersecurity, and thus will not be subject to mandatory reporting to the appropriate national CSIRT. This does not mean that they will be completely without risk of impact to the sector/subsector in question. In addition, country team resources are subject to certain staffing and budgetary constraints. Therefore, it is not possible for representatives of national CSIRTs to actively participate in all national and international cooperation forums within particular sectors or subsectors. It is also unrealistic for such sector-specific competencies to be developed in these units, while they may be of key importance in the case of aviation subsector. Lack of full knowledge about the specifics of the area of civil aviation by specialists from the CSIRT, operating at the national level, may lead to impeding and delaying the response to current threats as well as preventive and corrective actions, when the response time, especially in the case of such areas as air transport, is of key importance. Air transport is a special branch of the transport market and it is justified to undertake actions and search for such solutions that would simultaneously meet the mentioned challenges and be compatible with the national system and initiatives undertaken on the international forum. We can forecast that such a possibility could be the creation of a sectoral team, in which the employed specialists would know the specificity of the entire sector/subsector, the characteristics of systems used in this industry. It would be possible to create a coordinated system of effective and fast transfer as well as circulation of information for the subsector, collective protection would be ensured at an early stage. And it would also be possible for the team to “plug in” to the system of solutions currently being built in European aviation, e.g. cooperation with the European Centre for Cybersecurity in Aviation (ECCSA).

Aleksandra Radomska: In your opinion, should legal regulations concerning the scope of cybersecurity in aviation be implemented in the international aviation law and why?

ICT security specialist at the Civil Aviation Authority: I am definitely in favor of the idea to implement regulations with regard to the use of cyberspace in aviation. The use of ICT systems, data protection, information security are inseparable elements for the proper functioning of modern aviation. This process will continue to grow because the aviation is a very modern sector, and if in other areas of life digitalization progresses, it will also progress in the aviation industry. Attempts to understand this process and the direction in which it is going can be observed in the international arena, as the digitalization of transport was noticed and highlighted for the first time in the NIS Directive. However, in relation to the aviation subsector, both at the global level of the International Civil Aviation Organization (ICAO) and at the European level of EUASA, European Civil Aviation Conference (ECAC), European Organization for the Safety of Air Navigation (EUROCONTROL), cyber security has been one of the most discussed topics in the last two years. Adequate measures have been taken to strengthen international cooperation in this field and it should be expected that solutions will be jointly developed and included in aviation regulations. It is worth mentioning the amendment made to Annex 17 of the Chicago Convention, in which the first standard for cybersecurity appeared. The EUASA is also engaged in the development of projects to supplement the existing aviation regulations with cybersecurity matters. We are dealing with a trend that, although it does not constitute legislation, may become a certain reference point for future provisions in aviation legislation. For example, the Strategy for Cybersecurity in Aviation is being developed by the supranational European Strategic Coordination Platform on cybersecurity in Aviation, which operates under the EUASA and brings together more than 30 international aviation organizations. Implementation of legal regulations on the use of cyberspace in aviation has already begun. However, it is characterized by actions with “soft” specificity (like the mentioned strategy). At the same time, these steps are undeniably right and head in the right direction, and will gain momentum in the near future.

Aleksandra Radomska: Do you think that the development of aviation criminal law and sanctions in terms of conducting illegal activities in the cyberspace against the security of aviation radionavigation aids and global aviation satellite navigation systems and the recognition of cyber threats as acts of unlawful interference are justified and why?

ICT security specialist at the Civil Aviation Authority: Undoubtedly, it is necessary to tighten sanctions and penalties for aviation cyber activities, but as of today, this can be problematic. This is due to the lack of general national and international laws that adequately address the seriousness of cyber threats. There is also no international, coordinated approach to cyber issues in this aspect, whether civil aviation or state aviation. It should be noted that there is a chance to develop a common international approach and attempt to codify this matter, but the fact that some states are developing their competencies in offensive methods of using cyberspace may prove to be an obstacle. The pros of this idea can be held by observing the current trend focused on the "turn to cybersecurity," resulting in an increase in general awareness of cyberspace and its dangers, which is likely to result in the future in even greater pressure to develop a common approach, which would then be reflected in appropriate criminal legislation. Let me refer to the issue regarding the possibility of prosecuting perpetrators of cyber threats in aviation. However, I believe that in the age of modern technology, the perpetrators of such attacks have great opportunities at their disposal to effectively conceal their activities, while their detection and successful prosecution often becomes impossible or requires huge resources. These two aspects: the proper addressing of criminal law and the development of the competence of law enforcement authorities in the capability to detect the perpetrators of cybercrimes should go hand in hand to make the system more efficient and thus safer.

Aleksandra Radomska: In your opinion, how would the creation of institutions in Poland responsible for the operation and use of cyberspace for aviation affect the security level in air traffic management?

ICT security specialist at Civil Aviation Authority: The concept of creating national cybersecurity systems is correct both at the national and European level. As of today, the NIS Directive and the Law on National Cyber Security System (initiated by the Ministry of Digitalization) provide for the assignment of relevant functions to selected entities, such as: competent authorities, national CSIRTs, key service operators and the possibility of creating an additional support line in the form of sectoral CSIRTs. The adoption of the NIS Directive has given Member States some freedom in its implementation by organizing the system in accordance with the national situation. In my opinion, the path chosen by the Ministry of Digitalization seems to be the right one. In operational terms, it is possible to distinguish between the protection at the user and system owner level (i.e. operator of key services) and national CSIRT. The key services operator is required to be the first to provide adequate protection. In the case of critical incidents, the CSIRTs will be the body supporting operators in handling such events. In view of this, I recognize the possibility of establishing a sectoral team, which would be an additional support line for operators also in the case of "minor" incidents or a partner in the case of initiatives to increase the resilience of the subsector (e.g. through joint exercises, training, international cooperation). At the strategic level, Poland has institutions, namely competent authorities, responsible for strategic oversight and coordination of individual sectors, which may also decide to create a sectoral team, and an authority responsible for shaping the country's overall cybersecurity strategy, including the Ministry of Digitization, the Ministry of National Defense, and the Cybersecurity Plenipotentiary. In conclusion, this system is new, it needs to be tested in practice, but the concept alone seems to be absolutely right. And thus, in the case of air traffic management, it is the system owner who knows these systems, operates them and also understands the context of their operation, cooperating with the appropriate response teams, should play the most important role and this approach, in my opinion, is a good formula.

All data has been reserved at the expert's request.

Use of jamming devices against aviation radionavigation systems – interview with Mr Zygmunt R. Trzaskowski, General Manager of Hertz System Ltd. Sp. z o. o.

Aleksandra Radomska: In your opinion, how has the development and emergence of jamming devices impacted the growth of cyberspace as a new environment to impact negative activity?

Zygmunt R. Trzaskowski: Jamming devices should be considered as certain components that have an impact on cyberspace, but do not directly affect it. Above all, they are physical components used, like armaments, to physically reduce or completely block radio signals received or transmitted by a transceiver device. The effects of interference with the signature of electromagnetic waves – lead to physical annihilation of the device functionality, which may be considered as tantamount to its destruction. This category of jamming should be considered as an element of radio-electronic warfare. Moving on, cyberspace is an environment referring mainly to networks and software solutions. If any element of the network is jammed or incapacitated, this action will certainly have a negative effect on the entire functioning of cyberspace. However, the term "cyber warfare" should be used rather than “radio-electronic warfare” at this point. Accordingly, jamming and spoofing are occurrences outside the concept of cyberspace or cyberattack as they relate to radio and radio-telecommunications environments. Of course, they may indirectly affect the elements used to create cyberspace, as both jamming and spoofing of signals affect technical devices in a physical sense, but do not affect networks and software solutions.

Aleksandra Radomska: Taking into account that jamming devices are widely available at a relatively low cost and can be purchased by any user, would you propose restrictions allowing jammer purchases only in legitimate situations and why?

Zygmunt R. Trzaskowski: This question presents a very complex issue. It can be compared to the ownership of firearms by the citizens of a given country. At this point, let me compare the positions of two countries – the United Kingdom and the United States. The first of these countries advocates a total ban, based on casualty statistics, while the second promotes the rights of citizens to self-determination and self-defense. In this situation, of particular importance are the legal regulations in force in Europe, which to a large extent determine the position of state actors within the relevant groups in the European Commission. After this brief introduction and getting to the heart of the problem, let me state that jamming devices are elements of radio-electronic warfare and their trade should be, like armaments, completely controlled. The possibility of obtaining on the open market devices to jam Global Positioning System – Navigation Signal Timing and Ranging (GPS-NAVSTAR) or Global System for Mobile Communications (GSM) signals is a circumvention of the law and should be prohibited. I advocate a complete ban on the distribution of jamming means for Global Navigation Satellite Systems (GNSS) systems. The growing public reliance on GNSS systems and their use in public transportation, including aviation, means that jamming reception can result in incidents and fatal accidents. If jamming and falsification were to be prohibited, it is natural that a network of systems should be developed to monitor any occurrence of disturbance. Currently, such actions are taken in the case of airports or zones subject to special protection. Nothing stands in the way of retrofitting, within the scope of operations of the network of reference stations of ASG EUPOS systems and others, the stations with elements of detection, monitoring and determining the direction of occurrence of large emission intensity, which would prove the use of jamming or spoofing. In the case of criminal events, it is then possible to correlate information from city surveillance systems to determine the perpetrator.

Aleksandra Radomska: In your opinion, how may jamming and spoofing on aviation radionavigation aids and aviation global navigation satellite systems proceed in the future?

Zygmunt R. Trzaskowski: At the beginning, let me emphasize again that jamming and spoofing are not cyber-attacks but constitute armed or terrorist activities and should be treated as such. This is very important from the perspective of the issue of our discussion. In order to introduce the essence of this problem, I will divide the possible attackers into groups that would have different intentions towards carrying out attacks on airborne radio technical means. The first of these groups would include casual electronic engineers, amateurs, who may unknowingly cause RFI phenomena and are not aware of the consequences. These could include people using drones in the vicinity of an airport who unintentionally generate a potential threat to the radionavigation aids around them and to aircraft traffic pattern. The second group would consist of malicious individuals, acting with full intent, who see only entertainment in their actions. It is worth giving an example of individuals deliberately blinding the crew of aircraft – pilots. Potentially they may, also in the form of fun, try to disrupt the work of radionavigation systems. A third group, on the other hand, would aim to deliberately create dangerous situations conducive to their own gain. In that case, it would be an act of aviation terrorism. It is this group that should be regarded as posing a real threat to air operations. Therefore, in the case of airborne radio jamming, for the time being, the first and the second group do not pose a relatively large threat, because modern devices used by Air Traffic Services (ATS) (in Poland, the Polish Air Navigation Services Agency (PANSA) is responsible for their maintenance) or aircraft on-board equipment are able to detect the disturbance, and thus apply the appropriate procedures. Today, the navigation based only on GNSS means is not yet widely used in air navigation. On the largest scale in aviation radionavigation aids such as VOR, DME, ILS, NDB are still in use. However, the potential of "space plane" is noticeable. The trend of using radionavigation aids changes, and also in various plans some of the systems used so far are gradually being phased out. At the same time, it should be emphasized that we are dealing with the development of numerous anti-jamming techniques and services dedicated to air navigation services such as EGNOS v3, which may indicate an attempt to take preparatory measures against interference with technical devices in the future. Coming back to our attack groups, the third one is eager to invest considerable financial resources in appropriate jamming systems. It is important to keep in mind that any attacks from the ground against aircraft are relatively easy to detect and eliminate. The most difficult to defend against are attacks from the air or through assets on the platform under attack.

Aleksandra Radomska: What solutions would you propose to protect and ultimately provide at least an acceptable level of security to airborne radionavigation aids and airborne global navigation satellite systems?

Zygmunt R. Trzaskowski: The only effective way to ensure at least an acceptable level of safety for radionavigation aids and satellite navigation systems is to have appropriate anti-jamming systems, to cover or disperse the spectrum of radio wave signatures and, in the case of satellite navigation systems, to use signals resistant to interference, e.g. encrypted Y-code, M-code in GPS and GALILEO PRS systems. The mature direction should be to install signal detection and monitoring systems at airports and airfields as well as at radio technical resource points. Such detectors would allow immediate transmission of information on the detection of false emissions. This is possible because the detectors have the capability to measure interfering signal power (J/N) and direction (DF). These would allow an initial determination of the threat level. Furthermore, any signal (other than pseudo-satellites) appearing in the GNSS bandwidths that exceeds the noise level should be treated as a jamming signal.

Mr. Zygmunt R. Trzaskowski is the General Manager of Hertz Systems Ltd. Sp. z o. o. in Zielona Góra. The company has been operating on the market since 1989 in the areas of security systems, military ICT systems, GPS satellite navigation systems and space systems. Hertz Systems Ltd. Sp. z o. o. is a Polish manufacturer of GPS receivers with SAASM cryptographic module, designed for combat platforms and soldier equipment. The company has been equipping the Polish Armed Forces since 2006.