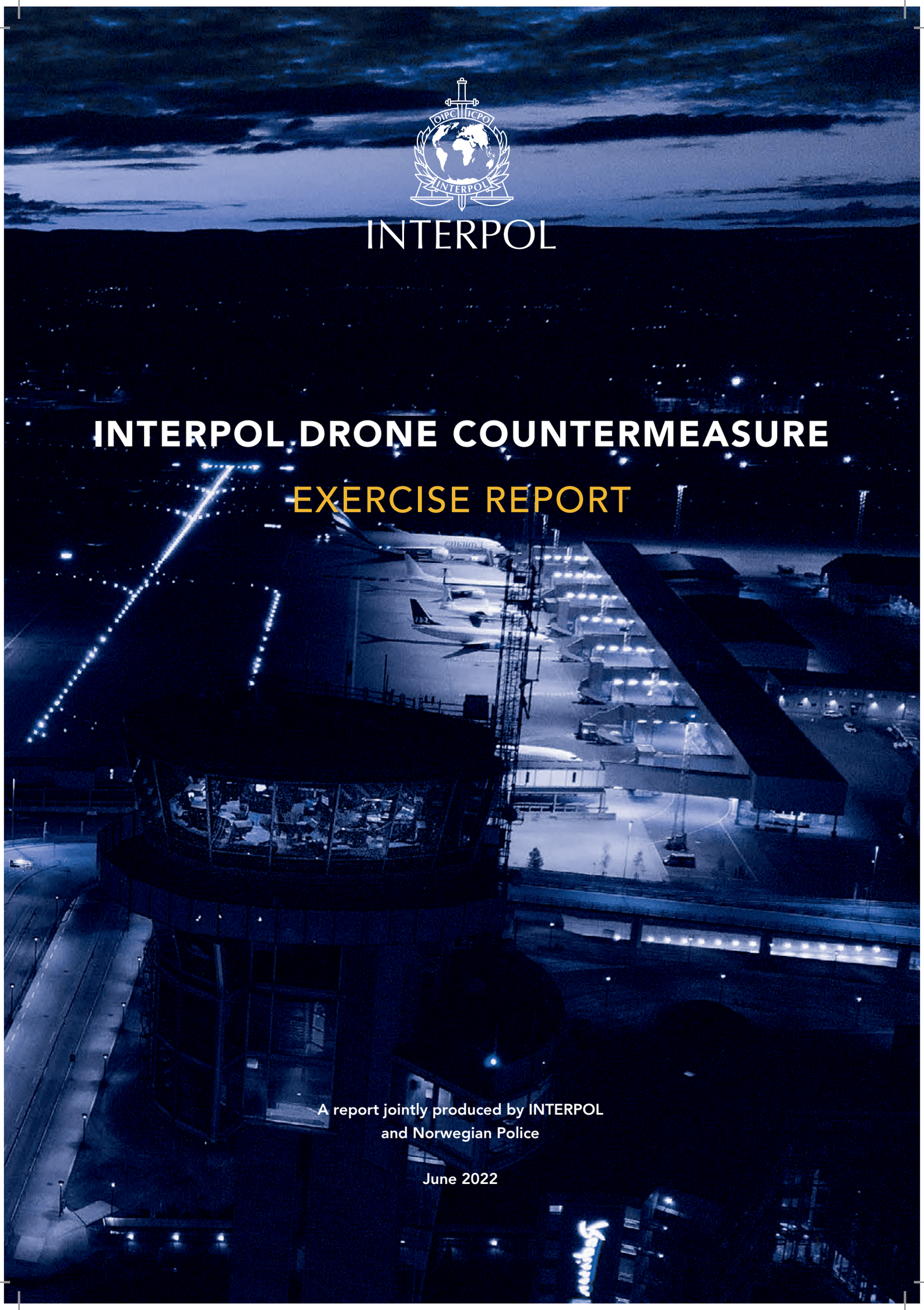

INTERPOL

INTERPOL DRONE COUNTERMEASURE

EXERCISE REPORT

A report jointly produced by INTERPOL
and Norwegian Police

June 2022

Acknowledgements

Many parties were involved in the delivery of the INTERPOL Drone Incursion Exercise 2021 and the drafting of this report. First and foremost, the INTERPOL Innovation Centre (IC) would like to thank the Norwegian Police, Oslo Gardermoen Airport, Avinor, the Norwegian Civil Aviation Authority, the Norwegian Communications Authority, and UAS Norway for their trust, faith and assistance in bringing this project to life. Without their continuous support, the event would not have been possible. This exercise would also not have been possible without the help of the suppliers of the C-UAS, putting their trust in INTERPOL. Finally, INTERPOL would like to extend special thanks to Jan Otto Johansen (C-UAS Manager, Norwegian Police), Martin Mathisen (Technical Security Advisor, TEKDIR AS) and the INTERPOL IC colleagues. Their dedication and contribution to this exercise have been immensely valuable. Finally, INTERPOL would like to recognize the efforts of Michael Hopmeier (President, Unconventional Concepts, Inc.) and Mike Monnik (Drone Cybersecurity and Threat Intel, Drone Sec) in helping to peer review the report to ensure that the technical and factual data were accurate and relevant. INTERPOL would also like to acknowledge and thank the Norwegian Police, TEKDIR AS and UASNorway for hosting and facilitating the C-UAS exercise in September and for their contributions, expertise in the analysis of the data from the tests, and in contributing to this document.

Legal Disclaimer

The objective of this document is to ensure that INTERPOL member countries have the relevant information to assess and evaluate C-UAS systems in aerodrome surroundings safely. This document aims to provide guidance, recommendations, and best practices without affecting the status of legislative and regulatory provisions. This report is not intended and should not be relied upon as any form of warranty, representation, undertaking, contractual or other binding commitment in law upon INTERPOL. INTERPOL does not express or imply any guarantee or assume any liability or responsibility for the accuracy, completeness or usefulness of any information or recommendation included in this document. INTERPOL only presents the findings and observations obtained during and after the testing that took place during the 2021 Drone Exercise. To the extent permitted by Law, INTERPOL shall not be liable for any damages or other claims or demands arising from or in connection with the use of this document. In addition, this document does not represent, define or state the official policy of INTERPOL or any of its affiliated organizations. It only presents the findings and observations obtained during and after the test related to testing procedures and system performance. It should be noted that INTERPOL acknowledges that the exercise performance represented in this document is historical (referenced to September 2021) and is not necessarily a reliable indicator for future performance, simulation or test results. Future implementation of relevant data addressed in this document should be conducted with caution and at the discretion of the parties involved.

Target Audience

This document is mostly a technical assessment and therefore aims to share the findings of the INTERPOL Drone Incursion Exercise held at the Oslo Gardermoen Airport in Norway in September 2021, with specialized and technical staff from law enforcement agencies involved in countermeasures and protecting critical infrastructures.

The Drone Incursion Exercise and the findings of this report represent cooperation between INTERPOL, the Norwegian Police and TEKDIR AS. The report aims to illustrate the preparatory phases, primary challenges, and tangible outcomes from the pre-test and testing phases of the drone incursion exercise to guide INTERPOL member countries in gaining insight and understanding when testing C-UAS technologies and systems.

By working with law enforcement in its member countries, INTERPOL aims to ensure that areas of emerging technology and their implications are thoroughly explored, and that international, regional, and local expertise is shared.

Glossary

Due to the technical nature of this report, a complete glossary of terms, abbreviations and acronyms used throughout the report is available in in Appendix 8.

Contact

Please contact Chris Church, Senior Forensic Specialist, of the INTERPOL Innovation Centre (dfl@interpol.int) for more information or comments.

Acknowledgement of Partners

This initial section of the report is intended to recognize the stakeholders whose roles were crucial in driving together the INTERPOL Drone Incursion Exercise 2021. The success achieved during this exercise would not have been attainable without the unique partnership moulded between Avinor, the Norwegian Police Directorate, UAS Norway, and INTERPOL. It was only through this robust cooperation founded on trust, teamwork, dedication and hard work that the realization of this exercise was possible.

Mr Anders Martinsen, Chief Executive Officer of UAS Norway, expressed the organization's efforts in actively promoting the safe and secure integration of drones in airspaces without jeopardizing safety or airfield operations. Therefore, it was a natural extension of their operations to participate in this exercise and contribute to the testing activities around monitoring and controlling unwanted drone flights. Their technological and industry-relevant expertise were instrumental in the exercise, in providing the necessary knowledge and guidance around countermeasures equipment. UAS Norway will continue to prioritize delivering safe drone solutions to respective sectors that will soon increasingly depend on unmanned technology.

Assistant Chief of Police Mr Per Øyvind Haugen from the Norwegian Police Directorate also conveyed the organization's dedication to protecting society from illegal uses of drones and the necessary close cooperation between law enforcement and other relevant stakeholders to achieve this goal. For several years now, the Norwegian Police, along with neighbouring law enforcement agencies, have monitored the rapidly developing threat from drones and noted the increasingly complex effectiveness of countermeasures due to various environments and crimes ranging from unintended illegal flight to criminal and terror activities. Their long-standing experience in drone countermeasures was influential in this exercise, and their contributions from a law enforcement angle structured the tested responses. Their support for this event was unparalleled.

Just as important was the role that Avinor played in the planning and execution of the exercise. As an airport operator, testing drone countermeasures and detection technology in a real-life airport situation and understanding the potential impacts of unauthorized drone incidents on airport operating systems was paramount. The role Avinor played in acquiring airport space and connecting all the airport operational staff with relevant staff from the exercise was fundamental for the event's success. Their readiness in preparing safety protocols and procedures against potential interference with critical airport infrastructure and coordination with all appropriate authorities and technical personnel provided the foundation for the smooth execution of the exercise.

INTERPOL had the greatest privilege and distinction in bringing together all these stakeholders under the same objective – creating safer skies by testing drone countermeasures technology. INTERPOL expresses its gratitude, appreciation, respect and thanks to all the stakeholders mentioned above, the 195 INTERPOL member countries, and others for their contribution, support and continued trust in INTERPOL and its goal of connecting law enforcement worldwide to enable international collaboration for a safer world.

Table of Contents

1. Introduction

Unmanned aircraft systems (UAS), more commonly known as “drones,” are automated airborne vehicles sometimes described as flying robots or flying cell phones or computers. Drones have quickly proven to be potent tools across all sectors and industries - automating and improving our ability to conduct everyday work in various environments. They have, however, also proven to be incredibly threatening. In the wrong hands, these machines could turn into weapons or mediums to enable criminals to conduct unlawful activities.

In recent years, the threat of drones entering restricted airspaces has become a cause for concern and a policing challenge in many of the 195 INTERPOL member countries. This threat is aggravated when a drone enters the airspace in and around an airport zone. It can cause an interruption in airport activity, the diversion of flights, and other potential incidents. Aerodrome menaces could result in financial losses to airport owners, airlines, and travellers using the airport due to delays and diverted aircraft, and create safety risks. In this context, counter-drone systems, also called counter-UAS systems (or C-UAS systems), are essential in ensuring the security of airports, and commercial providers have already developed a wide range of solutions to address this challenge. C-UAS systems will likely become even more prominent as authorities in member countries create regulations around drones and managed airspace. Despite this growth in importance, there is still insufficient information on assessing C-UAS systems in real-life conditions.

To better understand C-UAS systems, INTERPOL IC, in close collaboration with the Norwegian Police, carried out a three-day exercise at the Oslo Gardermoen Airport in Norway in September 2021. Participants came from law enforcement, academia, and industry from across the world. It was the first time that an exercise was able to test and assess a wide range of C-UAS systems whilst at the same time, the airport remained operational, accepting flights taking off and landing as scheduled with no interruptions to the airport.

2. Problem Definition

Authorities worldwide are reporting the presence of illegal drones near or inside airport perimeters daily. Given the potential threat and disastrous repercussions an unauthorized drone could have on an airfield, airport operators are often forced to halt or restrict runway operations, leading to severe disruptions to air traffic. Inevitably, this has created tough challenges for the law enforcement agencies as they confront the novel threat of drones and the task of policing access to lower airspaces.

Counter-drone systems have been identified as a potential solution to address the challenges of unmanned aircraft systems - otherwise known as C-UAS systems. These C-UAS systems can detect, track, identify and mitigate the threat from a drone entering the monitored airspace. Nevertheless, drone countermeasures are a relatively new technology that uses different forms of automated systems to maintain airspace safety. Despite increased attention toward the potential benefits of C-UAS systems, the capabilities of these systems are still difficult to benchmark. Consequently, end-users find it challenging to match the right counter-drone tools to the specific use cases.

The challenge for airport owners and law enforcement agencies is that they must currently select systems based on limited knowledge, expertise and in-depth testing of C-UAS within an airport environment. Independent testing would benefit not only the buyers but also the suppliers of C-UAS systems, as it would enable them to demonstrate that their equipment is safe to operate in a real-life environment, assessing the effectiveness, safety of use, and operational impact of the system on the user and the facility being defended/protected.

To get a better and more thorough understanding of the threat UAS constitutes to airports and airfields, please consult Appendix 1 prepared by the European Union Aviation Safety Agency (EASA). They are responsible for monitoring, investigations, regulating, and standardizing civil aviation safety. The EASA has included in this report an overview of three frameworks they have developed to protect airports from drones.

For More Information on the Drone Incursion Exercise:

An overview of the entire exercise and the process from ideation to inception is outlined in the report, here onwards. For a more thorough breakdown and detailed account, please consult the appendices. Each appendix is dedicated to a specific component of the exercise and can be accessed here:

- **Appendix 1:** The Threat of Drone to Aircraft and Airports, prepared by the European Aviation Safety Agency (EASA).
- **Appendix 2:** Overview of Counter Drone Technologies, prepared by UAS Norway.
- **Appendix 3:** Overview of the INTERPOL Drone Incursion Exercise 2021, prepared by the Norwegian Police and TEKDIR AS.
- **Appendix 4:** Overview of the Exercise Operations, prepared by the Norwegian Police and TEKDIR AS.
- **Appendix 5:** Evaluation of the Test, prepared by the Norwegian Police and TEKDIR AS.
- **Appendix 6:** Test Results, prepared by the Norwegian Police and TEKDIR AS.
- **Appendix 7:** Challenges of the INTERPOL Drone Incursion Exercise 2021, prepared by INTERPOL and Norwegian Police.
- **Appendix 8:** Glossary of Terms, Abbreviations, and Acronyms.

[1] European Union's Project Abstract for COURAGEOUS

3. INTERPOL IC Work in the Area of Drones

The INTERPOL IC has been working in the unmanned aerial vehicles sector, focusing on drone technologies since 2017. INTERPOL has achieved the following milestones:

- INTERPOL has organized three global expert groups exploring the tools, threats, and evidence aspects of drones in 2017, 2018 and 2019.
- The INTERPOL Drone Forensics Framework Technical Interest Group met in Colorado, United States in 2018. In this meeting, ten member countries gathered to fly and examine multiple makes and models of drones to create a drone forensics framework. This technology interest group was held in collaboration with VTO Labs (USA). This initiative came from the Drone Expert Group that was held in Singapore in 2018. This started the development of the INTERPOL Drone Framework for Responding to a Drone Incident for First Responders and Digital Forensic Specialists.
- In 2020, INTERPOL published the INTERPOL Drone Framework for Responding to a Drone Incident for First Responders and Digital Forensic Specialists in all 195 INTERPOL member countries. The framework explains the threat from drones and provides guidance on the actions required to respond to a drone incident. It also gives an overview of the digital forensic process when recovering data from a drone or associated equipment.
- INTERRPOL IC hosted a Drone Counter Measure (C-UAS) exercise at Oslo International Airport in September 2021 that brought together experts from law enforcement and industry to establish a framework to assist law enforcement in understanding C-UAS systems and their functionality and limitations.
- INTERPOL IC became a partner in a European Union-funded initiative called Project Courageous. The project started in 2021 and aims to develop a standardized methodology for testing and selecting countermeasure systems that can be used to detect and track a drone that enters protected airspace or a no-fly zone for law enforcement. In 2021, INTERPOL IC began leading the European Network of Law Enforcement Services (ENLETS) Drone Forensic Technology Interest Group (TIG) which is part of the ENLETS Countering Unmanned Aircraft Systems Technology Interest Group (TIG).

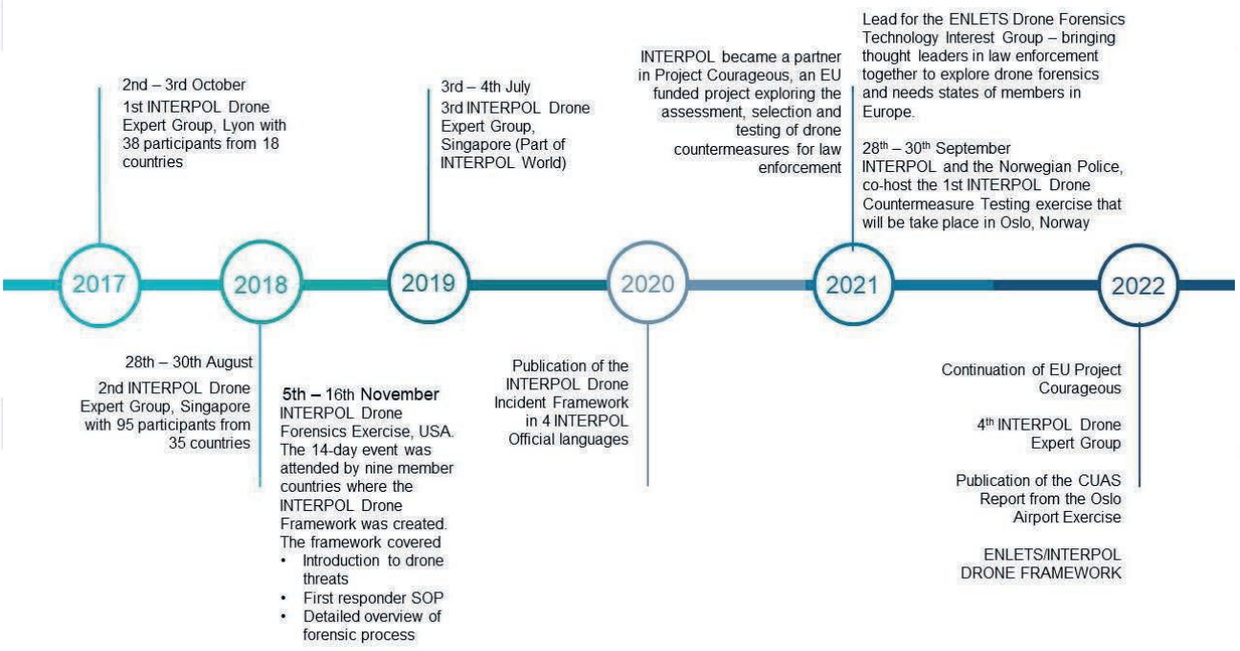

Table 1. Graphic of the INTERPOL IC timeline of work in drone technology.

INTERPOL IC has developed a consistent framework for approaching new technologies and has also implemented this method in the case of drones. This is done to ensure a comprehensive analysis and evaluation of the technology by exploring the following three fundamental components:

1. Threat – Utilizing systems and intelligence to counteract the threat from drones.
2. Tool - Use of drones by Law Enforcement and associated guidance
3. Evidence - The recovery of data and identifiers from drones and associated equipment.

Table 2. INTERPOL technology assessment framework

4. Road to Drone Exercise

Due to the increasing number of drone incursion incidents at civilian airports and their surrounding airspace, INTERPOL IC has received several formal requests from member countries to explore Counter Unmanned Aircraft Systems (C-UAS). INTERPOL started planning the execution of a drone incursion exercise in order to address the current lack of C-UAS system testing resources and to follow the recommendations of the INTERPOL Drone Expert Group for 2019.

The drone incursion exercise aimed from the start to gather experts from law enforcement, industry, and academia to explore the drone landscape as a source of threats, tools, and evidence. This allowed INTERPOL IC to ensure that law enforcement agencies in member countries stayed informed and updated with the latest technological trends and uses of drone devices. In addition, the exercise represented a chance to explore investigative possibilities that a drone may present during and after an incursion. This is both from law enforcement and criminal use perspective.

For a more detailed account of the varying C-UAS technologies and existing counter-drone technologies, please refer to Appendix 2 prepared by UAS Norway. UAS Norway is an independent non-profit organization specializing in UAS and focused on linking Norwegian public and private companies in all matters related to unmanned aircraft. They have contributed to this section by detailing current market UAS and C-UAS technologies.

5. The Drone Incursion Exercise

5.1 Overview and Preparation

The INTERPOL Drone Incursion Exercise 2021 was held during the active operation of Oslo Airport Gardermoen from 28 to 30 September 2021. The exercise gathered law enforcement, academia, and industry experts from INTERPOL member countries to test and assess the abilities of seventeen (17) counter-drone systems and determine their effectiveness in ensuring the safety of an airport environment. This was done through the detection, tracking and identification of drones and the locations of their pilots. An essential takeaway from this exercise was demonstrating how different C-UAS technologies could add value to law enforcement agencies involved in managing drone incidents at airports. In addition to the exercises, the incursion event also included workshops and expert presentations to address the challenge of evidence retention. Participants in these sessions shared best practices and discussed possible future solutions to drone incursions.

Please find at Appendix 3 a thorough overview and detailed description of the preparations of scenarios, drones, pilots and the processes that were incorporated into this exercise. This was drafted by the Norwegian Police in collaboration with TEKDIR AS. TEKDIR AS provides strategic security services to the public services and has vast experience in emerging technology in protecting critical infrastructure and sensitive sites.

5.2 Testing

During the three days, more than 2,025 aircraft took off and landed during the operational exercise. INTERPOL IC, in close cooperation with its partners, conducted the testing phase of the drone exercise and was able to execute several test assessments, namely:

- Test 1 addressed the different passive detection systems.
- Test 2 dealt with radars.
- Test 3 addressed multi-sensory systems.
- Test 4 focused on different countermeasures.

The following data sources were used to evaluate each test:
Video grabbing tool to record the actual screen the C-UAS operator sees during the test

- Logs from the C-UAS system
- Flight logs from the drone
- Notes and records from the observers, including start time, drone discovery, positions, etc.

Flight logs, paths and metadata were used to generate a video file containing a visual representation of the flight path and the relevant metrics from the drone. With these recordings on a timeline, a real-time representation was generated to display a side-by-side comparison of what the drone did and what the C-UAS system identified. The result was extensive documentation of 61 exercises/tests.

The on-ground sequence of events, roles and responsibilities, as well as a step-by-step guide of the exercise can be found at Appendix 4, which was jointly prepared by the Norwegian Police and TEKDIR AS.

5.3 Evaluation

For the purpose of the exercise, drones were deployed in a non-hostile manner but successfully created an unwanted safety risk. Through applying countermeasures, the aim was primarily to provide decision-makers with the information needed to shut down portions of the airport or the facility as a whole.

As the purpose of this exercise was to evaluate different types of technologies, it did not award a winner. However, in order to determine whether a system is usable in an airport scenario, specific scoring parameters were identified, and data points were extracted to determine the effectiveness of varying C-UAS solutions. Those parameters included whether or not the drone and drone pilots were located, the detection and localization point of time, the accuracy of the position, the number of false positives, to name but a few.

The complete list of scoring parameters is included at Appendix 5 as part of a report kindly prepared by the Norwegian Police and TEKDIR AS.

5.4 Test Results

The exercise conducted four tests that assessed passive, active, multi-sensors, and jamming systems. Passive sensors do not have an external effect or do not interfere with other sensors, systems, or technologies and were therefore tested simultaneously. Active and multi-sensors disturb or interfere with each other, so each participating C-UAS system was tested individually.

The likelihood of detecting drones manufactured by the most popular producers in the world, was, as expected, higher than the likelihood of detecting drones manufactured by other less popular companies. This is because all C-UAS systems that use radio frequency (RF)-based detection have the most popular drone signatures in their libraries. The test results might have been different if custom-built or modified commercial off-the-shelf (COTS) drones were used.

The Norwegian Police and TEKDIR AS have kindly summarized and presented all the test results in their report, see Appendix 6. The document includes screenshots of the recorded data points using various software deployed during the exercise.

6. Challenges from the INTERPOL Drone Incursion Exercise 2021

At the beginning of the planning phase of the drone incursion exercise, INTERPOL IC faced the challenge of limited information, knowledge and expertise available on conducting drone incursion testing. Over the past three years, INTERPOL IC has collaborated with its partners to close this knowledge gap. In addition, it has aimed to lead drone device testing in order to make it accessible to member countries.

INTERPOL IC worked with the Norwegian Police and relevant partners to ensure that the INTERPOL Drone Incursion Exercise addressed the fundamental issues that law enforcement in INTERPOL member countries had previously shared. The objective of the assessment was to have a neutral approach and ensure that the testing criteria and validation of the systems were met. In doing so, INTERPOL IC was able to identify challenges and best practices to be taken into consideration when performing C-UAS.

In this regard, several complex situations and elements emerged during the pre-test evaluation and analysis phase. The following provides a summarized list of scenarios of challenges that should be taken into account for future C-UAS exercises to prevent the alteration of testing results.

1) Identification of Stakeholders
2) Pre-Event Testing of Equipment
3) Establishing Standardized Testing Criteria
4) Disruption of Airport Activity
5) Operating Restrictions for C-UAS
6) Certification and Licensing of C-UAS
7) Drones Required for Test
8) Testing of Frequency Scanning and Monitoring

A more comprehensive and detailed account of the challenges can be found at Appendix 7, prepared by INTERPOL IC and the Norwegian Police.

7. Findings

During the INTERPOL Drone Incursion Exercise, law enforcement, industry, and academia were invited to come together to share knowledge and information on C-UAS and test the capability of these systems to detect, track and identify (DTI) drones entering the airport airspace. A number of relevant technical and operational findings emerged from this event that hold significant relevance in connection to the implementation of drone countermeasures.

1. Regular Testing of C-UAS and Operational Envelope

When the C-UAS is installed at a location the system may need constant or regular adjustments to ensure that it operates at its most effective capability and ensure that any existing or new infrastructure that is constructed within the detection range of the system does not reduce its operational envelope. Each C-UAS also needs to be regularly tested to ensure it meets the operational needs of law enforcement by confirming its operability to detect, track, identify and mitigate drones. These tests should take into account the emerging drone threat and evolution of the drone market to ensure that any system's capability matches the evolving threat from criminal use of drones.

2. Understand the types of threat

A majority of drone incursions are from unintendedly and unintentionally piloted drones but during an incident it is very difficult to determine if the drone threat is present. Law enforcement agencies and owners of areas where C-UAS are installed should develop a framework for responding to the drone incident to ensure any affected parties that may be a target from a drone threat understand the response protocol to a drone threat.

3. Testing of C-UAS in Real Time Environments

When evaluating a C-UAS system it should be tested in the environment that it is intended to be operating in to ensure its effectiveness and reliability to detect, track, identify or mitigate drones. If the system is tested in a different environment than its intended operation, the results and the effectiveness of the C-UAS may be compromised.

4. Different Types of Drone Devices

During the tests, off-the-shelf drones were used. These devices did not feature any modifications or enhanced capability to avoid detection, tracking and identification. If LEAs wish to ensure that a C-UAS system is capable of detecting a drone threat, it would be fundamental to ensure that the known drone threat is understood through threat reporting or monitoring of criminal activities in relation to drone devices.

5. Drone Operators

When conducting the tests, trained users from the C-UAS system suppliers were used to operate the systems. In a real-life environment, however, the operator would most likely be the owner or responsible parties of the facility or a member of an LEA protecting the area. Hence, these individuals would require training and extensive evaluation of the system and its capability and limitations to ensure its most effective use.

8. Conclusions

During the plenary sessions and discussions during the 2021 Drone Incursion exercise, the participants underlined that drone technology had already become a major asymmetrical threat, and the associated enforcement to protect airspace is challenging for law enforcement.

After conducting the C-UAS exercise it became apparent that for a test to be a success there needs to be a multi-stakeholder approach where all parties that are operating in the area to be tested need to be involved from the outset. This ensures that each stakeholder understands their role and responsibility during the C-UAS test and when a real drone incursion occurs. There is a wide variety of C-UAS technology, and this must be a consideration depending on where the systems are installed and what they are protecting. Each system has its advantages and disadvantages depending on the operational environment and the existing infrastructure and digital signal landscape. The testing of these systems is a complex undertaking and requires huge resources and capabilities to conduct any exercise. For this reason, there is currently limited knowledge and operational testing data in relation to C-UAS systems.

While the INTERPOL Drone Incursion Exercise provided a critical opportunity to test and explore the dynamics of the use of C-UAS in the context of an operational civilian airport, it also demonstrated that further research and development is needed. The exercise highlighted that the operational capability of the C-UAS systems often does not match real-life applications due to a majority of testing being carried out off-site in very open environments which does not match the intended location for the operation. The difficulties in testing C-UAS systems emerge from various elements, both technical (e.g., different installation processes, configuration and optimization, or different drone devices) and external (e.g., weather conditions, location of various test environments). Further research within these domains will ensure that C-UAS are effective in ensuring the safety and security of critical infrastructures and ensure minimal disruption to the day-to-day operation that the C-UAS system is protecting.

9. Recommendations for C-UAS Testing Within Law Enforcement

9.1 Recommendations for Drone Countermeasure Testing

Based on the contributions of the drone experts' discussions during the sessions and the testing results, the following fundamental recommendations have been identified that industry, academia and law enforcement agencies of INTERPOL member countries should consider in relation to future C-UAS testing exercises.

9.1.1 Recommendations for the Preparatory Phase

1. Unified Drone Threat Reporting Systems

As drones become more technically sophisticated, it is recommended that LEAs create unified drone threat reporting systems for sightings and incidents. Law enforcement, aviation agencies and relevant stakeholders should use this reporting system to ensure a cohesive drone threat reporting system. This course of action will enable stakeholders to identify drone incidents effectively and address the modus operandi of criminals utilizing this technology. In addition, it will further help in classifying the risks created by irresponsible drone pilots compared to criminals and terrorist threats relating to airway environments.

2. Engagement with Industry

Law enforcement agencies are required to specify their operational requirements to the C-UAS companies and ensure that the proposed solution meets their specific needs. This is because a majority of C-UAS systems were initially built to respond to military needs and only later adapted for civilian use. This has generated severe issues, considering that an incident or episode of collateral damage might be considered acceptable during a military operation. However, this may result in irreparable damage in a civilian/public area context.

In addition, as the evaluation of potential risks for the use of airspace for criminal activities is currently challenging to assess, it is further recommended that LEAs respond to these issues by engaging with relevant industries and creating a unified response to drone incursion threats.

9.1.2 Recommendations for the Implementation Phase

3. Multi-Latitudinal Environments

Law enforcement agencies should consider the fact that C-UAS solutions can be effective within one environment but may be limited in another. For instance, the use of C-UAS within an urban environment could be particularly complex due to the interference from existing devices and radiofrequency landscape and infrastructure limitations, including glass-fronted buildings, skyscrapers, and frequency absorbing materials. This could severely affect the range and capability of the C-UAS solution.

In addition, most C-UAS tests are conducted in limited environments (e.g., countryside and semi-urban environments). Therefore, the solution developed during this assessment might work well during the tests but may not perform as expected when adapted to more complex operational environments. This is due to location changes and existing infrastructure.

4. Deployment of C-UAS

It is recommended that LEAs interested in using C-UAS systems address the need for fixed and mobile solutions. This recommendation presents a challenge as most systems are intended to be fixed and require time to be calibrated, tested and optimized for efficient use in different environments. For instance, during the tests at the Oslo Gardermoen Airport, suppliers were given nine hours for testing and system initialization. However, many suppliers required more time to ensure that the systems operated efficiently and maximized their range and detection capabilities.

As a result, LEAs may need to utilize a multiple solutions approach that could provide different capabilities and deployment options. Moreover, LEAs should consider that most case scenarios require a multi-layered detection system that covers long, mid and short-range detection capabilities to secure airspace.

9.1.3 Recommendations following the Exercise

5. Response Plans

It is recommended that any critical area, building or event be equipped with a drone incident response framework. This will allow any individual within the area affected by a drone incident to be prepared for specific security measures and protocols. This will ensure their safety and avoid risks of collateral damage. This framework should contain ad hoc information according to the demands of the different stakeholders to better respond to each environment. For example, the European Aviation Safety Agency has developed three guides for airport owners to manage a drone threat.

6. Evolution of C-UAS Technology

The asymmetrical threat posed by drone incursions is growing, it is therefore recommended that LEAs pay close attention to C-UAS solutions. From a detection, tracking, identification and neutralization perspective, these technologies should further become a baseline contingency practice for all member countries. Since drone technology is rapidly becoming mainstream to the public, criminals can easily upgrade a device to evade detection and identification thanks to basic knowledge and expertise acquired online. By upgrading the device, it is possible to alter the drone's behaviour to minimize the likelihood of detection and identification. This is achievable by simply modifying the operating frequencies of the command to control the system or by controlling the drone through pre-planned flight paths or via a 3/4/5 G modem. This information can be readily found and accessed through online forums and platforms (e.g., YouTube). Users can obtain tutorials and information on modifying the drone's airframe, control systems and components to improve its speed, range and operational capability.

7. Legislation and Regulation

There is a strong need for legislation and related regulations to protect restricted airspaces, areas of national interest, or to safeguard the public at events such as football matches, music concerts or mass gatherings from the threat of drones. These can be temporary no-fly zones, enforced/voluntary registration of drones or temporary restricted use of airspace orders. The legislation and regulation around the use of drones and integration of C-UAS in both a civilian and LE context, for regulatory frameworks needs to stay updated and evolve alongside drone technology. As many member countries move towards integrating drones into their day-to-day activities, legislation and regulations should naturally follow. This would guarantee that any evolving use cases around the use of drones and responses to the threat from drones should be included within drone legislation and control. It is also recommended that member countries try to harmonize these norms to ensure cross-border functionality and acceptance. Also, legislation and regulations should be harmonized within regions or countries to ensure cohesive and coherent implementation of the laws and regulatory requirements for the safe use of drones and C-UAS

[2] https://www.easa.europa.eu/newsroom-and-events/press-releases/easa-issues-guidelines-management-drone-incidents-airports

8. Drone Operational Capabilities

The capability and functionality of drones are expanding. With the dawn of Beyond Visual Line of Sight flight operations (BVLOS, a term relating to the operation of (UAVs) and drones at distances outside the normal visible range of the pilot), drone corridors, package delivery, shore to ship, and shore to island deliveries are becoming commonplace. Consequently, it is recommended that law enforcement's response to such incidents be adapted and improved to ensure that any incident involving a drone device would be handled and investigated according to appropriate measures and protocols.

9. Societal Implications[3]

As drones start to populate all kinds of airspaces worldwide, it is also crucial to consider the societal implications of counter-drone measures. Three critical points were identified for law enforcement to be mindful of:

- Psychological perception: the sighting of counter-drone systems increases threat perception and may generate psychological stress. Some of these systems have a distinct military appearance, and their deployment in civilian contexts may trigger uneasy feelings.
- Surveillance systems: counter-drone systems are surveillance systems and should be treated as such. They collect information about drone users, generate visual data and provide geolocation information. Therefore, their use must comply with the applicable data protection rules.
- Military Approach: even though most contemporary drones and counter-drone R&D occur in the civilian and commercial sectors, these fields are still marked by a military logic, testimony to the environment in which drones were first used and created.

9.2 Next steps

The INTERPOL Innovation Centre continues to be dedicated to connecting member countries' LEAs with experts and academia worldwide to bring together the latest and most updated knowledge and expertise and is ready to fully support, assist and guide any member country's request regarding drone technology and C-UAS.

For 2022, INTERPOL IC's ambitions concerning drones and associated emerging technology are as follows:

- Involvement in the European Union Project Courageous and testing of drone countermeasures based on the scenarios developed as part of the programme.
- Publication of an updated INTERPOL Global drone framework in close cooperation with our partners such as, ENLETS.
- INTERPOL IC will continue to build upon the findings of the Drone Expert Group and continue to assist the 195 INTERPOL member countries.

[3] Bruno Oliveira Martins from the Peace Research Institute Oslo

Appendix 1: The Threat of Drone to Aircraft and Airports prepared by the European Aviation Safety Agency (EASA)

1.1 Introduction

One of the major developments that is taking place in the field of aviation is the proliferation of Unmanned Aircraft Systems (UAS[4]) operations (commonly known as "drones"), particularly within the EU. According to estimations, those operations will provide a significant boost to the economy of the EU Member States (MS), as the European drone market will reach a value of around EUR 10 billion per year[5] by 2050. Moreover, the use of drones will be able to cover a wide spectrum of operations, including, but not limited to, inspection and surveillance (usually, but not always, smaller in size UAS), security and defense related operations (usually, smaller or medium sized UAS) as well as transport of people in urban environments and smart cities (large-sized UAS).

This ongoing proliferation of UAS operations, however, bears also a significant challenge to aviation safety and security. Under this aspect, the number of incidents involving drones in the European region is increasing as well, including a number of incidents in the vicinity of airports or even within the airports[6]. Unauthorized UAS operations in the vicinity of airports may in turn lead to an increased risk for other aircraft (air risk) and (uninvolved) persons or infrastructures (ground risk) and thus to major disruptions to air traffic, potentially leading to a restriction of operations and considerable economic losses.

Given the above, it is important that the stakeholders involved in the aviation safety and security community possess the necessary tools as well as the required awareness in order to implement effective mitigation measures in a cooperative manner as a response to those threats.

Finally, it is important to note that as **security lies largely in the core of each MS national interests,** and apart from the relevant applicable EU rules, the proposed mitigation measures, although representing the outcome of discussions of various experts in this domain across the EU, are of indicative nature and remains a choice of each MS to use, build on, and tailor those to its unique (security) needs.

1.2 Landscape, Stakeholders, and Potential Threat Actors

In order to be able to highlight the challenges that aerodromes are currently facing due to the conduction of unauthorized UAS operations, and correlate these to corresponding mitigation measures, it is important to briefly map the different actors and stakeholders involved in this broader landscape. This mapping should include the organizations that are affected by such operations as well as the categories of offenders that are the main drivers behind such operations. It is important to understand that aviation safety and security is not a static environment but instead a very dynamic one, safeguarded by a series of different and clearly defined procedures that are in turn undertaken by numerous actors in a cooperative manned, under a holistic approach.

1.2.1 The growing concern

According to the manual "Drone Incident Management at Aerodromes"[7] published by the European Union Aviation Safety Agency (EASA) in 2021, while unauthorized UAS operations were already considered a threat at airports during the previous decade, it was not until the events at London's Gatwick Airport in 2018 that the wider public became aware of such risks. In particular, between 19 and 21 December 2018, more than 100 drone sightings were reported over the aforementioned airport; this unauthorized drone activity led to the closure of the airport's single runway. The disruption lasted 33 hours, resulted in the cancellation of more than 1,000 flights, and affected 140,000 passengers. When calculating the cost of this disruption, consider that the average cost of a one-hour delay can be as high as EUR 6,600; the cost of a single flight cancellation can be as high as EUR 17,650[8].

[4] The term UAS is used in the EASA Basic Regulation as the legal and technical term as well as in the relevant delegated and implementing acts adopted. The term "Drones" is the popular term used normally by people with not relevant aviation background. In this document, both terms are used interchangeably. [5] European Drones Outlook Study, by SESAR JU, available here; [6] The term "airport" includes both the landside and the airside. On the other hand, the term "aerodrome" concerns only the airside. The EASA rules according to Regulation (EU) 139/2014 currently only regulate the safety of aerodromes.

A number of drone incidents occurred across the EU in previous years, leading to similar disruptions in airport operations. Those include, but are not limited to, the following:

- At **Madrid Barajas Airport**, 3 out of 4 runways were temporarily inoperable on 3 February 2020 after a drone sighting, resulting in the re-routing of 26 flights.
- At **Frankfurt Airport**, runway operations were suspended on 8 February 2020 and again on 2 March 2020 due to a reported UAS.
- In spite of the COVID-19 crisis and the resulting decrease of traffic in the EU, **92 drones were observed** within a 1.5-km radius of DFS Airport **in 2020** [9].
- More than **100 drone incidents** within the vicinity of airports (27% of total rogue operations) were reported **worldwide** in 2021 and the first quarter of 2022; many were reported in the EU[10].

Consequently, it appears that incidents of drones in the proximity of airports have increased during the last few years in both volume and impact. This trend is projected to continue, highlighting the need for the implementation of mitigation measures by the relevant stakeholders involved.

1.2.2 The Stakeholders and the need for cooperation

The primary stakeholders that participate in the ecosystem of aerodromes and are thus influenced by unauthorized operations in the vicinity of airports include, but are not limited to, the following:

- **European aerodrome operators:** Responsible for protecting the aerodromes from such incidents.
- **Air Traffic Services (ATS):** Control Towers ensure the safety and security of air traffic.
- **Aircraft operators:** Responsible for informing Air Traffic Control of UAS sightings
- **National competent authorities of MS:** Provide national oversight of aviation safety and security
- **Law Enforcement Agencies (LEAs):** Often in charge of surveillance and patrols of landside areas or airport surroundings; ensure public order and compliance with applicable restrictions
- **EU Agencies and Institutions:** Include authorities involved, at least to a certain extent, in EU aviation and/or security in the wider ecosystem; groups include EASA, EUROCONTROL, the EC, EUROPOL, and others
- **Travelers/Citizens:** Affected by disruptions and potential incidents or accidents As the rulemaking for operations of civil drones in the EU fall under EASA's competence, the Agency is acting as the European Coordinator for supporting those stakeholders by proposing certain objectives and recommended actions under this aspect (Section 3:

1.3 EASA´s Counter – UAS (C-UAS) & Recommendations).

It is critical to ensure appropriate level of cooperation and efficient coordination mechanisms at national and local level between all actors involved so that preparedness and mitigation measures are properly developed and implemented taking into consideration local characteristics and responsibilities.

[7] Available here [8] Drone Incident Management at Aerodromes, EASA [9] Ibid. [10] D-Fend Solutions - according to the company's incident track report

1.2.3 Drone incident offenders and their motives

Offenders can be categorized by taking into account their motives. Those are briefly, the acts that are the result of negligence, non-criminal motivated acts, and criminal or terrorist motivated acts for such unauthorized operations. In particular, these motives and reasons may include:

- Pure negligence: Persons who do not know or understand the applicable regulations and restrictions.
- Careless individuals: Persons that may know the applicable regulations but do not care respecting them, through either their fault or negligence, normally with no intent to disrupt civil aviation.
- Reckless individuals: Persons who know the applicable regulations but do not follow the rules in purpose, in order to satisfy their personal interests (e.g., professional, economic).
- Activists/Protesters: Persons motivated to disrupt flight operations for ideological or political reasons and their actions may have unintended consequences on aviation safety. They have no intent to influence aviation safety and security that may result in the loss of human lives.
- Criminal or Terrorist motivation: Persons who intent to use drones in a malicious way at the expense of aviation safety and/or security that may result in the loss of human lives.

While it is difficult to identify the motive behind an unauthorized operation, these inputs should be taken into account during the scenarios developed as part of the necessary risk assessments that will need to be conducted on such occasions by the relevant authorities involved in each MS.

1.3 EASA´s Counter – UAS (C-UAS) task force

In 2020 an EASA C-UAS Task Force was established to develop guidance and recommendations to ensure that the aerodrome and aircraft operators as well as the ATS are prepared to prevent or react to unauthorized operations taking place at the vicinity of airports with minimum disruption of operations11. As a result, EASA and the Task Force delivered to the aviation community and law enforcement stakeholders a manual in three parts:

- **Part 1:** Drone Incident Management at Aerodromes: The challenge of unauthorized drones in the surroundings of aerodromes.
- **Part 2:** Drone Incident Management at Aerodromes – guidance and recommendations.
- **Part 3:** Drone Incident Management at Aerodromes – resources and practical tools.

Part 1 is published on the EASA webpage and therefore, accessible to the public. Part 2 and part 3 of the manual are provided as one document, but their distribution is more restricted due to the sensitive nature of the subject.

The material in **part 2** and **3** is suitable for use by small, midsize, and large aerodromes in the scope of the European aviation system and is suitable for those aerodromes which have not yet prepared for drone incidents. At the same time, even aerodrome operators who have already put in place some procedures, can also benefit from the resources and tools.

Due to the sensitive nature of the subject matter, EASA decided that material found in parts 2 and 3 of the manual should only be made available to the relevant stakeholders and the national competent authorities of the EASA Member States, so that they share it with the relevant aviation organizations under their oversight. Meanwhile, the entire manual will also be made available to DG HOME and DG MOVE and EASA´s partner countries. Besides this distribution list other duly motivated requests for access to all parts of the manual may be sent to:

Aerodromes@easa.europa.eu

[11] European Plan for Aviation Safety (EPAS) 2020–2024, available here. [12] More information to be found in EASA Manual Part 1: Drone Incident Management at Aerodromes: The challenge of unauthorized drones in the surroundings of aerodromes. [13] There are also other EU and international rules, standards or guidance material with applicability in this domain. Given the length of this report, only the most relevant EU rules are presented. [14] More information to be found in EASA Manual Part 2: Drone Incident Management at Aerodromes – guidance and recommendations.

1.3.1 The regulatory framework[12]

The issue of unauthorized UAS operations is a transversal issue with applicability on both aviation safety and security and one of a multi-faceted nature. The main instruments to mitigate these threats can be found in **Regulation (EU) 2019/947** (rules and procedures for the operation of UAS) as well as **Regulation (EU) 2019/945** on UAS and on third-country operators of UAS[13]. These rules follow a riskbased approach and define three different categories that are considered proportionate to the level of risk of the operation, i.e., the open, specific and certified category. It is important to note that in the higher-risk category (certified category) the risk is considered similar to manned aircrafts, and as a result the aim is to integrate those operations in the "manned aviation eco-system" following thus similar rules when it comes to relevant ATM rules and procedures, including security aspects as well.

As it can be derived from the above, the open and specific categories provide higher flexibility to the remote pilot in case the latter wishes to operate them in an unauthorized way and disrespects the rules for the reasons aforementioned in Section **1.2.3 Drone incident offenders and their motives.** It is therefore important for the national authorities of MS to ensure the full implementation of the EU Drone legislation when it comes in open and specific category operations. In particular those rules concern, mainly:

- The registration of drone operators
- A minimum required training for drone pilots
- The fitting of a remote identification feature on most commercial drones
- Several operating limitations (e.g., flight in Visual Line of Sight – VLOS, at a maximum height of 120 meters for UAS operated in the "open" category)
- The introduction of the concept of "UAS geographical zones", where drone operations are restricted
- Minimum age of the remote pilot requirements (possibility to adjust this in the level of MS)

In addition to the above, following a safety and/or a security risk assessment conducted at the national level, national authorities may consider adding provisions related to drone incident management to the National Civil Aviation Security Program (NCASP). These can include a description of the response that the involved actors should perform in order to mitigate a threat posed by a negligent or malicious drone operation. Moreover, further requirements may be added at a national level including further operating limitations and restrictions, especially in the vicinity of airports, insurance and liability from non-commercial drone operators, and imposing sanctions for relevant criminal offenses and laws. Finally, it is of utmost importance to raise awareness about these rules and restrictions at the national level in each EU MS.

1.3.3 The role and responsibilities of stakeholders involved[14]

The measures that need to be implemented include preparedness measures at a local/airport level, measures during the incident including information collection as well post incident measures. In the aviation domain, all these measures are undertaken by a certain stakeholder based each time on its applicable field (e.g., aerodrome, aircraft operator, Air Navigation Service Providers - ANSPs, etc.) and each actor should cooperate closely with the other as part of this structured process in order to achieve optimum results.

During unauthorized UAS operations close to airports, it is necessary to clarify the aerodrome operator's responsibilities, as well as those of other relevant actors in order to facilitate collaboration of the different actors during the whole course of an event.

When it comes to the **detection of drones near airports**, national authorities ought to decide which aerodromes under their jurisdiction may require drone detection technologies and who will be responsible for these drone detection systems. Moreover, they should determine which detection capabilities are needed in order to perform this task adequately. Those solutions might range from the ability to locate, detect and classify drones at the vicinity of an aerodrome area, to geo-fencing to protect airports of strategic importance.

Regarding the **suspension and restoration of operations**, and depending on the jurisdiction, the leading role would normally be allocated to LEAs. The latter should closely cooperate with the rest of stakeholders at the aerodrome, based on clear procedures provided by the relevant national authorities.

Concerning the implementation of C-UAS technologies such as the **neutralization of unauthorized drones**, it is again expected that LEAs will have the leading role in most MS and therefore it is essential that the latter should expand their knowledge in responding to drone incidents in an airport environment. Currently, many enforcement authorities lack sufficient understanding and awareness on how to respond to such incidents in an airport environment. As a response to this, the **INTERPOL IC** (the Digital Forensics Laboratory) has prepared a framework[15] based on best practices among their member countries as a reference tool for law enforcement worldwide which together with the EASA manual creates a solid basis for a proper framework to face challenges of unauthorized drones in the surroundings of aerodromes. It is recommended that airport operators, ANSPs, and LEAs actively engage with each other by developing a "concept of operations" (CONOPS) defining what types of actions might be taken and by which actor. The CONOPS might also establish general procedures for the retention and extraction of flight data, which could be useful in a post-incident investigatory context.

After the roles of each stakeholder have been defined, the ANSPs may assist the ATS units by preparing **operational instructions for inclusion in their manual of operations**. In particular, those measures might include specific instructions for the local Air Traffic Control (ATC) unit to communicate with the airport operator and LEAs for the management of drone incidents, the provision of an aerodrome specific threat zone map, the use of categorization on threat levels based on the severity of the incidents, as well as guidance for other factors to be considered as part of the relevant threat and risk assessment.

Moreover, MS should define certain **geographical zones that would prohibit or restrict UAS operations**[16], and aerodromes are at the top of such a list. To prevent drone incidents by negligent behavior of clueless and/or careless individuals, the airport and/or the ANSP should raise awareness to the public regarding the UAS geographical zones which ensures the safety and security of aerodromes with respect to drones and other threats. In the near future, apart from the requirement on most of the drones of the open category to have geo-awareness functionalities, it is possible that a geo-fencing functionality will be added as well.

Last but not least, it is the role of the aerodrome operator to safeguard the principles of the safety management framework and coordinate communication with the rest of the key actors at an airport. The approach of the aerodrome operator to these threats should be an **integrated safety management approach**, jointly developed and executed with the ATC, the LEAs and the national competent authorities in order for the perspectives of aviation safety and security to be considered equally. Those authorities may form a **Drone Incident Management Cell (DIMC)** established in each airport, with the mandate of safeguarding the safety and security of air operations at an airport. The actors of the DIMC are encouraged to participate in relevant **retical and practical training including tabletop exercises developed by the aerodrome operator in dealing with drone incidents in airports**.

The aforementioned measures although the outcome of experts' discussions by the involved stakeholders and thus highly recommended as guidance to the aerodrome operators and other stakeholders participating in this ecosystem, are of indicative nature, and as it can be understood, provide a degree of flexibility and allow for adjustments to the unique criteria of each MS and/or airport. It can be concluded that all stakeholders should be assigned clear and definite roles by the responsible authority and act in a cooperative way in order to mitigate this threat.

1.4 Technological C-UAS solutions[17]

A number of different security and safety related incidents can derive from unauthorized operations of drones. This can be hovering of one or more UAS in a critical section of the airspace, such as the final part of a runway or in any zone in the airport vicinity that is considered unsafe for an UAS to operate due to the risk of collision. Another example could be a flight over a critical ground infrastructure, which could be classified as both a security and a safety event, as this security breach could lead to unpredictable impact in the services of flight operations, air navigation services, etc., with in turn an impact to safety.

In order to protect people and infrastructure and ensure the efficient operation of the airport, there are a number of technologies providing C-UAS solutions. Those solutions are varying in technical design, services, and capabilities

[14] More information to be found in EASA Manual **Part 2:** Drone Incident Management at Aerodromes – guidance and recommendations. [15] The report may be downloaded from here [16] Article 15 of Regulation (EU) 2019/ 947. [17] More information to be found in EASA Manual Part 3: Drone Incident Management at Aerodromes – resources and practical tools.

based on the needs of the airport. The implementation and use of technologies must be proportionate to the level of threat defined. As every airport has different needs (geography, environment, and economics) all counter UAS solutions will differ from one another. A complete C-UAS system solution could take into consideration the following elements to prevent the disruption of airport operations and/or would assist the restoration of normal operations:

- Detection.
- Tracking.
- Identification, Threat Assessment and Classification.
- Neutralization or interceptions.
- Command and control.
- Operational instructions.
- Integration into normal operation (ATM, local authorities…).
- Training of operators.

For an airport, the objectives of these solutions are to:

- Protect people and infrastructure.
- Prevent accidents.
- Ensure efficient operation.
- Integrate into the normal operation the airport systems and operations

The C-UAS detection systems can be in turn based on different technologies. Many combine a set of these different technologies in order to provide a more robust detection, tracking, and identification capability. Identification technologies are comparable to detection systems. All solutions have potential limitations and possible impacts that need to be explored for the specific environment and understood before deployment. All solutions have a limited detection performance which depends on different factors according to the type of sensor, configuration, etc.

Consequently, the installation of Counter-UAS systems in airports needs careful consideration as every technological solution such as neutralization technologies cannot be a “stand-alone” option for decision-makers as it presents both advantages and disadvantages. For this reason, numerous factors should be taken into account before its implementation as every airport has different needs. Testing of various technologies might certainly contribute to having an informed decision-making process in place and INTERPOL initiative should be welcomed in that context.

1.5 Conclusions

The EU MS and all involved stakeholders ought to safeguard the full implementation of the EU common rules concerning drone operations and if deemed necessary, to supplement those rules with their own mitigation measures and C-UAS technologies of their choice considering their needs in terms of aviation security and safety close to airports, following relevant and tailor-made risk assessments. Moreover, a structured allocation of roles and cooperative response by all the stakeholders involved is essential.

Finally, raising awareness not only to the stakeholders that are directly involved or affected by these phenomena but, in order to achieve optimum results, to all citizens at a national level that are nowadays eventually becoming stakeholders in UAS operations. Finally, it must be understood that EASA´s manual is technology-neutral and does not recommend a specific detection technology or other technological C-UAS solutions. Numerous technological C-UAS solutions are under development with varying degrees of maturity and reliability. The suitability of such solutions depends on aerodrome-related specificities, so that the Agency remains neutral as to which aerodrome operators should consider supporting their drone incident management processes with technological C-UAS solutions, because the deployment of such solutions ought to be a risk-based decision, which should be left to the Member States and aerodromes locally responsible.

Appendix 2: Overview of Counter Drone Technologies prepared by UAS Norway

2.1 Introduction

This report has been prepared by UAS Norway – the Norwegian association for unmanned systems and provides a detailed and thorough account of the current market of counter-drone systems and their effectiveness. UAS Norway covers Passive Detection Systems, Active Detection Systems and Multi Sensor systems.

2.2 Market for Counter-Drone Systems

Given that the demand for counter-drone technology has emerged only in the past few years, many of the C-UAS products offered by the companies that we identified have not yet had time to mature. Thus, there may be significant variations between the performance and reliability of systems that might appear to be very similar based on comparisons of their specification sheets.

The absence of standards also raises questions about the safety of these systems. For example, INTERPOL's current understanding is that some systems under test would find it difficult to meet electromagnetic radiation exposure standards.

Another issue is the lack of clear requirements at any level, combined with the widely varying operational, legislative, and regulatory environments extant throughout the INTERPOL community. Due to the relatively new field of C-UAS, the technical aspect of the community is still evolving, and the operational side is only just beginning to appreciate the challenges, benefits, and operational milieu that drones and counter-drone systems present. The lack of clear operational requirements combined with standards for test and evaluation poses a significant challenge to developers who create, field, and support C-UAS systems for the wide array of potential applications.

2.3 Counter-Drone Technologies

C-UAS systems today are based on different types of technology, and the cost and staff time needed to operate them will therefore vary. As the purpose of the test was to demonstrate different C-UAS technologies (and not specific systems), participating systems have been anonymized in order to reduce the risk of negative perceptions for those concerned. In order to demonstrate and compare effectiveness, systems were divided into three categories:

- Passive Detection Systems
- Active Detection Systems
- Multi Sensor Systems

Also, some countermeasure kinetic and non-kinetic countermeasures were tested on the last day.

2.3.1 Passive detection systems

Systems that detect and locate drones, and in some cases also identify the pilot's position, by scanning for emissions from drones or their controllers. These systems "look" and "listen" for signals that drones emit. The signals can include radio, sound, and even light. Passive detection systems may use different detection methods, such as triangulation, protocol-analysis, or direction-finding; the sensors do not include actively emitting radio-frequency elements that could cause severe interference with other navigation or communication links. Examples of such technology are cameras, acoustic sensors, and RF receivers. RF sensors operate by collecting and interpreting information within range of the sensor. All defined parameters may be measured simultaneously by either a single or multiple sensors; the sensor deduces the nature and behavior of the invading drone(s) from the resulting signature. The space of interest is defined by a radio frequency antenna which is tuned to the sensor electronics.

2.3.2 Active detection systems

Systems that detect the presence of any moving object generated when the object encounters and reflects signals emitted by the detector. Some of these systems include algorithms that enable the system to distinguish drones from other low-flying objects. A typical example of such a system is RADAR.

Radar (radio detection and ranging) is a detection system that uses radio waves to determine the distance (ranging), angle, and radial velocity of objects relative to the site. It can be used to detect a multitude of objects, including drones. A radar system consists of a transmitter producing electromagnetic waves in the radio or microwaves domain, a transmitting antenna, a receiving antenna (often the same antenna is used for transmitting and receiving) and a receiver and processor to determine properties of the object(s). Radio waves (pulsed or continuous) from the transmitter reflect off the object and return to the receiver, giving information about the object's location and speed. LIDAR is similar but uses lasers instead of radio waves.

2.3.3 Multi-Sensor detection systems

Systems that use a combination of library-based and/or radar systems with electro-optical or electrooptical/ infrared cameras, which identify drones based on their visual signature, and/or acoustic sensors, which recognize the unique sounds produced by different types and model of drones.

2.3.4 Countermeasures

There are many different types of kinetic and non-kinetic countermeasures available. Nevertheless, many of these systems are unfit for use at an operational airport due to the imminent risk of collateral damage. As of today, radio frequency "jammers" are the most common active C-UAS systems. When the radio frequency link between the drone and the controller is severed, most drones are designed to either hover in place, land, or return to home; drones without such fail-safes will either fall to the ground (crash) or fly away in an uncontrolled manner. However, a major challenge is the unreliability of these responses, as current drone technology does not reliably follow these design protocols. However, this will change over time as drones become increasingly more resilient with the implementation of 5G and Internet of Things (IoT). All countermeasures participating in the exercise were "jammers", but other types of countermeasures exist, such as hacking, taking control of the drone and forcing it to land at a pre-defined place, and a drone with a netgun that can successfully intercept the target drone.

Countermeasures are generally divided into two broad categories: cooperative and non-cooperative. Cooperative countermeasures rely on the drone to behave as designed. Examples include breaking the command datalink, and the drone landing or returning home as it has been programmed to do. Non-cooperative countermeasures do not rely on the drone design; instead, they physically force the drone to behave in a desired manner. Examples of non-cooperative countermeasures include kinetic destruction and net capture.

Appendix 3: Overview of the INTERPOL Drone Incursion Exercise 2021 prepared by the Norwegian Police and TEKDIR AS.

3.1 Introduction

This section provides a thorough rundown of the entire INTERPOL Drone Incursion Exercise held in Norway, in September 2021.

3.2 Overview

INTERPOL Drone Incursion Exercise 2021 was held at Oslo Airport Gardermoen, located approximately 47 km (about 29.2 mi) north of Oslo, in the largest airport in Norway, with an annual passenger capacity of approximately 32 million from 28 to 30 September 2021. The real-life exercise gathered law enforcement, academia, and industry experts from sixteen INTERPOL member countries to test and assess the ability of seventeen (17) counter-drone systems to determine the effectiveness of their technologies as well as ensure the safety of an airport environment through the detection, tracking, and identification of drones and the locations of their pilots. These counter-drone systems are emerging as essential elements in ensuring the security of airports and airspaces and protecting nofly zones above cities, prisons, and critical infrastructure.

The exercise was held at Norway's main airport, Gardermoen Airport, located approximately 47 km north of Oslo. The airport has an annual passenger capacity of approximately 32 million; it had 244,000 arrivals/departures in 2019 and employs more than 15,000 people who keep the airport running 24 hours a day.

Due to the complexity of the exercise, the event required close collaboration with airport owner Avinor, the Norwegian Communications Authority, the Civil Aviation Authority, and UAS Norway to ensure that all systems and tests were held to a required standard and did not affect airport operations.

Figure 1: Map of Flying Zone

3.4 Preparation Phase

While the exercise was solely an INTERPOL initiative, the event was nevertheless fully dependent on close cooperation and support from the Norwegian Police, Oslo Airport, Avinor, the Norwegian Communications Authority, and the Norwegian Civil Aviation Authority. The scope of creating an event of this complexity at an operational airport created legal, logistical, and technical challenges. Some of these challenges were potential showstoppers, and the importance of having integrated stakeholders from both the public and private sectors proved invaluable in solving challenges and pushing the project forward.

3.4.1 Risk management

Extensive work was carried out to perform a risk analysis for the exercise. A preliminary risk analysis, also known as a preliminary hazard analysis, is a qualitative method of analysis, usually done in groups and within a relatively short period of time to establish a primary risk picture. The purpose of such an analysis is to reveal potential risks and undesirable events as early in the process as possible in order to eliminate, reduce, or control them. Avinor's risk management system complies with ISO31000[18], which enabled stakeholders to gain a deep understanding of the risks involved in the project. By further enhancing this system with the Bowtie model, the results could be presented in a logical and structured manner. Avinor provided this risk management system as a framework, and subsequently incorporated all of the project's potential risks into the organization. By doing so, we were able to receive feedback from all relevant operational stakeholders throughout the airport. The risk management process was supervised by a risk officer from OSL that continuously gathered and shared relevant information both internally at the airport, and externally among the project's organizers. We firmly believe this was a crucial success factor in gaining the trust and cooperation of airport management.

3.4.3 Identified risk

When the project began assessing and identifying risks, it became clear that there were several key components and functions at an airport that were not necessarily obvious. For example, fueling an airplane requires WIFI, which operates on the exact same frequencies we intended to jam. Thus, identifying and managing risk was an ongoing process throughout the event. We identified approximately 100 individual risks during the planning phase of this event. Typical examples include:

- External participants in an operational area
- Foreign object debris
- Transitioning between exercise and airport operations
- Active fly zones
- Uncontrolled drones
- Interference with Air Traffic Control (ATC) infrastructure
- Radio interference
- Ground radar interference

Many, if not all, drone countermeasures can be dangerous in certain circumstances. Drones may fall down or fly away. Jamming systems can interfere with legitimate communications links in their vicinity, and even kinetic countermeasures that shoot a small net equipped with a parachute to bring the ensnared drone to the ground in a controlled manner may be risky if the parachute fails to deploy correctly or if the interception occurs at a low altitude.

Counter-drone systems, in general, use a wide range of different frequency bands. These frequency bands are often shared by various other communications systems and are also used commercially,

leading to an increased risk of interference. Sources of interference with other systems must be identified and located to facilitate frequency deconfliction. Furthermore, it is necessary to obtain authorization to provisionally use these frequencies. Authorization for this event was secured by the Norwegian Police.

To prevent and mitigate any interference, the radio frequency spectrum was monitored both before and during the exercise by the Norwegian Communications Authority.
In order to mitigate the risk of interference, participating counter-drone systems were only allowed to interfere

[18] https://www.iso.org/iso-31000-risk-management.html

with 2.4 GHz and 5.8 GHz frequencies. Any interference with global navigation satellite systems (GNSS) such as global positioning systems (GPS), GLONASS or GALILEO resulted in the counterdrone system being disqualified from the event, as interference in the frequencies used by those systems could pose a potential threat to the safe operation of manned air traffic at Oslo Airport. From an operational point of view, experts involved in the planning process found it sufficient to limit signal interference (jamming) to those frequencies, as they are the most common and also the most difficult frequencies to disrupt. As most of the counter-drone system suppliers were not able to manually select frequencies to interfere with, limitation of the operation frequencies of the counter-drone systems under test had to be done in advance of the test event. By taking such measures, it was possible to limit the risk of interference of critical infrastructure to a minimum. Nevertheless, it was still necessary to have procedures in place for how to address other types of unforeseen disturbances.

Based on the preliminary risk assessment and detailed information from the system operators, the police were able to request permission from the national frequency provider to temporarily use the following frequencies:

- 2400 – 2483.5 MHz
- 5725 – 5875 MHz
- 8.5 – 9.1 GHz
- 9.0 – 9.5 GHz
- 9.2 – 10 GHz
- 9.3 – 9.6 GHz
- 15.4 – 16.5 GHz
- 15.4 –16.7 GHz
- 24.45 – 24.65 GHz

*Please note that legislation and use of frequencies may vary among the different member countries.

3.4.4 Selection requirements for suppliers

As of the writing of this report, there are no international standards for the proper design, evaluation, and use of C-UAS systems at airports, or for the use of C-UAS systems at all. It is our belief that although the suppliers of C-UAS systems tend to market their products as being fit for any use or application, the reality is that there is a large difference in both requirements and challenges for the different use cases of C-UAS systems. For example, an airport has different needs and challenges than a rapidly deployed tactical system. Thus, in order to establish a common understanding of the scope of the event, we specified our operational and safety requirements and preferences in as much detail as possible during our communications with the C-UAS system suppliers. All suppliers were informed that the different scenarios would be simple, and would demonstrate various angles, distances, and altitudes of approach possible for common, commercial off the shelf (COTS) drones in a real-life airport environment. Furthermore, suppliers were informed that the test would include different types of drones, potentially in different numbers. A map of the area was provided; the map included the locations of control systems, deployment options, and the flight area. It must be noted that on-site inspection would not be possible during the selection phase. However, prior to the exercise, the suppliers were given the opportunity to choose the locations of their own sensors as long as they did not interfere with other infrastructure or operations. The suppliers had to deploy and operate their own systems during the exercise. The exercise planning team also issued a list of requirements that the C-UAS system under test had to meet to be considered for participation in the event. All requirements were due to safety concerns. Requirements were as follows:

A. The system shall interfere as little as possible with other systems at the airport. The system should be tested against EMC / EMS / EMI standards. The supplier should indicate what standards the system was tested against and, if possible, include reports from a third-party accredited laboratory.

B. All systems participating in this demonstration must be safe to use in accordance with electromagnetic radiation exposure standards such as ICNIRP7/99 General Public Exposure, or other equivalent standards. Although not a requirement, it is preferred that this information is verified by a third-party accredited laboratory. Equipment with active RF elements may be subject to Radiation Hazard testing by us, and the supplier must therefore be prepared to deliver their C-UAS system 14 days before the event for this testing.

The suppliers were also asked to answer a list of questions that would form the basis of the evaluation, as follows:

A. For this exercise, the system should have TRL9 status. Please indicate if your system complies with this requirement. If not, please indicate what status you consider that your product has. (TRL-status is defined in the EU-H2020 statement, attached to this document.)

B. Based on the supplier estimate, how long will it take to set up the system for the demonstration?

C. The system submitted for this demonstration should be able to detect the most common COTS drones. Please describe which drones the system will detect.

D. Does the system have a module that generates a time-stamped log with details of each alert or action a detection system or jammer has been involved in? Please inform us of your system's logging capabilities, and how the data is exported from the unit.

E. If the system has an active RF jammer, is it possible to manually select frequencies?

F. Systems that contain RF effectors should be able to block all drone frequencies that are commercially available in Europe. Please indicate the frequencies your system can emit in. If possible, provide the corresponding report from a third-party accredited laboratory.

G. Is the system able to detect, classify, and position both the drone and the operator?

H. Is the system that you propose to bring to the exercise GDPR-compliant?

I. If your detection system contains active RF elements such as radar, lidar, or similar, please provide information about modulation, power, Radiation Hazard safety distance, etc. If possible, please provide a corresponding report from a third-party accredited laboratory.

3.4.5 Suppliers

The following suppliers were chosen to participate in the exercise based on the criteria detailed in section 3.2.4:

Vendor	Country	Brand Represented
Dark Matter Norway AS	Norway	IXI
Dedrone GmbH	Germany	Dedrone and H.P. Marketing & Consulting
D-Fend Solutions	Israel	D-Fend
Drone Protection Solutions AS	Norway	Fortem
Frequentis AG	Austria	Hensloldt and Rohde & Schwarz
Heatsec AS	Norway	FLIR
Mydefence Communications ApS	Denmark	Mydefence
Rohde & Schwarz	Norway	Rohde & Schwarz
Sesofusion Oy	Finland	Sensofusion
Siphon AS	Norway	Droneshield and Squarehead Technologies
Stanley Security Norge AS	Norway	Stanley
Steel Rock Technologies Ltd	United Kingdom	Steel Rock
Saab AB	Sweden	SAAB
Weibel Scientific	Denmark	Weibel

Table 1: C-UAS systems tested

It should be noted that the C-UAS systems were selected based on the criteria's defined for this specific exercise. Every airport and/or purchaser of a C-UAS system must verify if the system is usable for the intended application and if the system meets formal and legal requirements.

3.5 Initial exercise schedule

The suppliers were invited to a site survey at OSL on 1 September 2021, where the suppliers were briefed by the Avinor team on the technical facilities available and individual requests were discussed throughout the day.

The capacity of having several Avinor staff members present was very valuable, as requests could instantly be agreed to or refused. The suppliers were given access to the Air-side zone to inspect potential deployment areas. Lastly, the suppliers were informed of the schedule:

- Day 1 - 08:00 till 17:00: Installation and testing of systems.
- Day 2 - 08:00 till 16:00: Live exercise for stand-alone RF and radar sensors.
- Day 3 – 08:00 till 16:00: Live exercise for multisensory systems.
- Day 4 – Live exercise for mitigation systems.
- Day 5 – De-rig and removal of equipment.

It must be noted that based on these criteria, it was expected that each supplier would dimension the scope of their system accordingly to manage installation time, required testing, and subsequent readiness for the exercise. The suppliers were not given the criteria on how their systems would be scored.

3.5.1 Scenarios

In practice, it is very challenging to identify a drone, and even more difficult to ascertain the motivation and intent of the offender[19]. Nevertheless, one could assume that most drone incidents in aerodrome surroundings are caused by either clueless or careless individuals with no intent to disrupt civil aviation. It was therefore decided by the organizers to use scenarios that were quite simple in scheme, demonstrating various angels, altitudes (200 ft. or 400 ft. AGL), and distances of approach without trying to be outmaneuvering the system operators, as the main objective of the exercise was to demonstrate the effectiveness of the different C-UAS systems.

The exercise specifies the threat to be an individual with no hostile intent as such, but will possibly through reckless and illegal flying, create a dangerous safety situation or cause disruption.

One scenario in each category included two drones simultaneously, another had a 60-second pause initially before the drone and controller were switched on. The purpose of these scenarios was to see whether some systems detected drones “automatically” after a certain period of time.

Based on experiences from the dry run, five scenarios were selected. Maps of the flight path for each scenario are provided in Figures 2 – 6.

Figure 2: Jamming Flight Path

Figure 3: RED Flight Path

INTERPOL INTERPOL INTERPOL

Figure 4: YELLOW Flight Path

Figure 5: BLUE Flight Path

INTERPOL INTERPOL INTERPOL

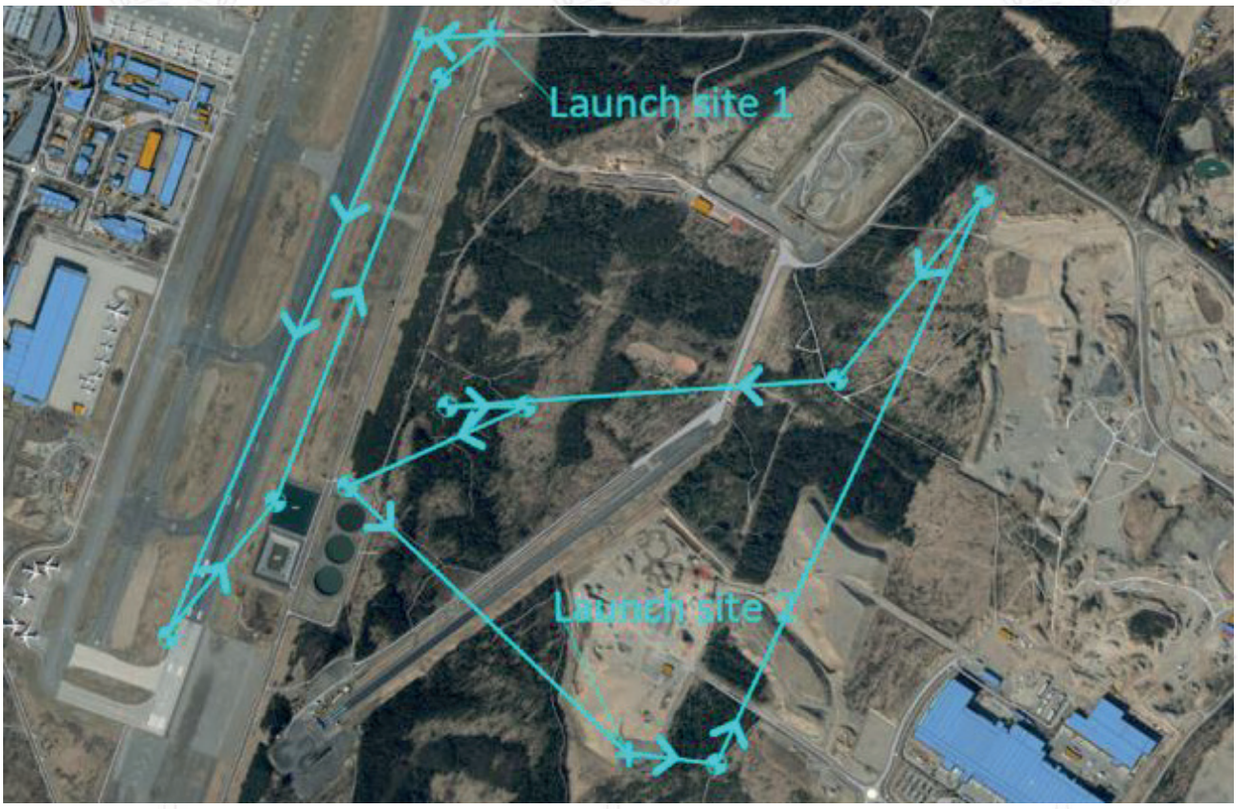

Figure 6: CYAN Flight Path; includes two drones

3.5.2 Selection of drones

In general, commercially available C-UAS systems detect and defeat COTS drones flying at normal speeds. One could also argue that a skilled individual with hostile intent would most likely bypass any commercial detection and defeat system(s), and thus a planned drone incursion would be successful before the airport operator or law enforcement agencies were able to address the threat.

In an attempt to reflect the current threat picture, the Norwegian Police conducted a preliminary test at Oslo Airport in July 2021 in collaboration with Avinor and the Norwegian National Security Authority using a variety of drone detection systems. During this period, 32 non-authorized drones were detected flying a total of 125 illegal flights inside the 5-km no-fly zone.

These results were later compared with information from the global drone reporting and intelligence system DroneALERT **(https://www.drone-detectives.com/)**. Based on this information, INTERPOL selected a range of commonly available COTS drones to use in the exercise.

As most passive detection systems are library-based, C-UAS system suppliers must constantly update their knowledge of the software that drone manufacturers use to control their drones. For IDIEX21, drone software was updated three weeks prior to the exercise. No information about the drones used in the exercise was provided to the suppliers other than that there would be one or more common COTS drones, using software that had been updated no later than three weeks prior to the exercise.

The ability of counter-drone systems to detect and defeat types of rare drones was not part of the scope of this exercise; the exercise focused instead on the most likely drone threats instead of rare exceptions under the assumption that most drone incidents will use one of those commonly available drones.

INTERPOL INTERPOL INTERPOL

Based on this assumption, the following drones were selected for the exercise; an image of each drone is provided in the referenced figure:

- DJI Mini (Figure 7)
- Parrot Anafi (Figure 8)
- DJI Mavic 2 Air (Figure 9)
- DJI Phantom 3/4 (figure 10)
- DJI Mavic 2 Enterprise (Figure 11)
- DJI Matrice 210 (Figure 12)

Figure 8: DJI Mini 2 (249 grams)

Figure 9: Parrot Anafi (320 grams)

Figure 10: DJI Mavic 2 (570 grams)

Figure 11: DJI Phantom 3/4 (1380 grams)

Figure 12: DJI Mavic Enterprise (899 grams)

Figure 13: DJI Matric 210 (3840 grams)

3.5.3 Pilots

The drones were operated by trained drone pilots from the Norwegian Police. Having skilled and experienced pilots later proved to be vital in order to safely perform over 100 high-risk drone flights in a no-fly zone over a period of three days under occasionally harsh weather conditions.

3.4.4 Risk assessment – drone flights

All flights were assessed using a standardized risk assessment, which is a multi-stage process of risk assessment aimed at risk analysis of certain unmanned aircraft operations, as well as defining necessary mitigations and robustness levels. An example of a standardized risk assessment is provided in Annex Z, Standardized Risk Assessment V2.

https://www-cognitoformscom.translate.goog/PolitietHelikoptertjenesten/standardisertrisikovurderingv2?_x_tr_sl=no&_x_tr_tl=en&_x_tr_hl=no&_x_tr_pto=wapp

3.4.5 Pilot practice

A dry run, or practice run, is a testing process where the effects of a possible failure are intentionally mitigated. At Oslo Airport, this was done approximately one month prior to the exercise to test various scenarios and practice the transition from the active to the inactive flying zone. The dry run proved to be valuable, as areas that required adjustment were identified; adjustments were made accordingly.

3.6 Installation of equipment

As all equipment and personnel must go through the standard airport security checks before entering the restricted area airside, suppliers were requested to deliver their equipment to the test site the week before the event in order to avoid any unnecessary delays during the day of deployment. By having the suppliers provide detailed information about their technical and practical needs prior to the event, the day of deployment mostly consisted of deployment of the counter-drone systems. Based on experience from previous airport incursions (such as the Gatwick incident in 2019), law enforcement response to drone incursions at airports would most likely take place shortly after an incident. One could therefore argue that the primary objective for law enforcement agencies should be to optimize the time between the occurrence of a drone incident and the time when law enforcement is able to normalize the situation.

As a large proportion of the C-UAS suppliers actively market their products to law enforcement agencies for this and similar scenarios, deployment time was one of the questions the suppliers were requested to answer before being invited to participate in this event. It was communicated to all suppliers that the exercise had a strict schedule, and thus deployment time was limited to a total of 9 hours. Suppliers concerned about the time limitation were told to either increase their manpower during set-up or reduce the size or complexity of the system they deployed for the event. Nevertheless, the time provided for system deployment was not sufficient for some suppliers. To some extent, some suppliers' need for additional deployment time could be explained by either the variations in the complexity of the various counter-drone systems deploying, technical skills, and/or the level of operational experience of the supplier deployment teams. However, the primary culprit was the suppliers' eagerness to demonstrate their product, combined with a large amount of unjustified optimism.

Clarification of the location of each deploying system prior to the exercise proved to be a necessity in order to map any potential conflicts between the different systems based on technology and safe operating distance.

Appendix 4: Overview of the Exercise Operations prepared by the Norwegian Police and TEKDIR AS.

4.1 Introduction

This section details the step-by-step process behind the operations on the day of the exercise. This section covers the division of tasks and responsibilities, communication, and documentation of the exercise.

4.2 Exercise Organization

A diagram of the organization of the exercise is provided in Figure 13. The test and evaluation event were led by the Exercise Commander. Each test was managed from an Exercise Operation Centre under the supervision of the Battle Captain. His role was to manage the command and control of current operations. Thus, he ran a centralized hub that served to supervise, monitor, and log each test, and to relay relevant information to all stakeholders throughout the exercise on the orders of the Commander. The suppliers operated their own systems under the supervision of observers from the organizer (blue team). Once each test was completed, the Documentation Supervisor collected notes from the observers, logs from the suppliers, flightlogs, and verified that recordings from each test had been received.

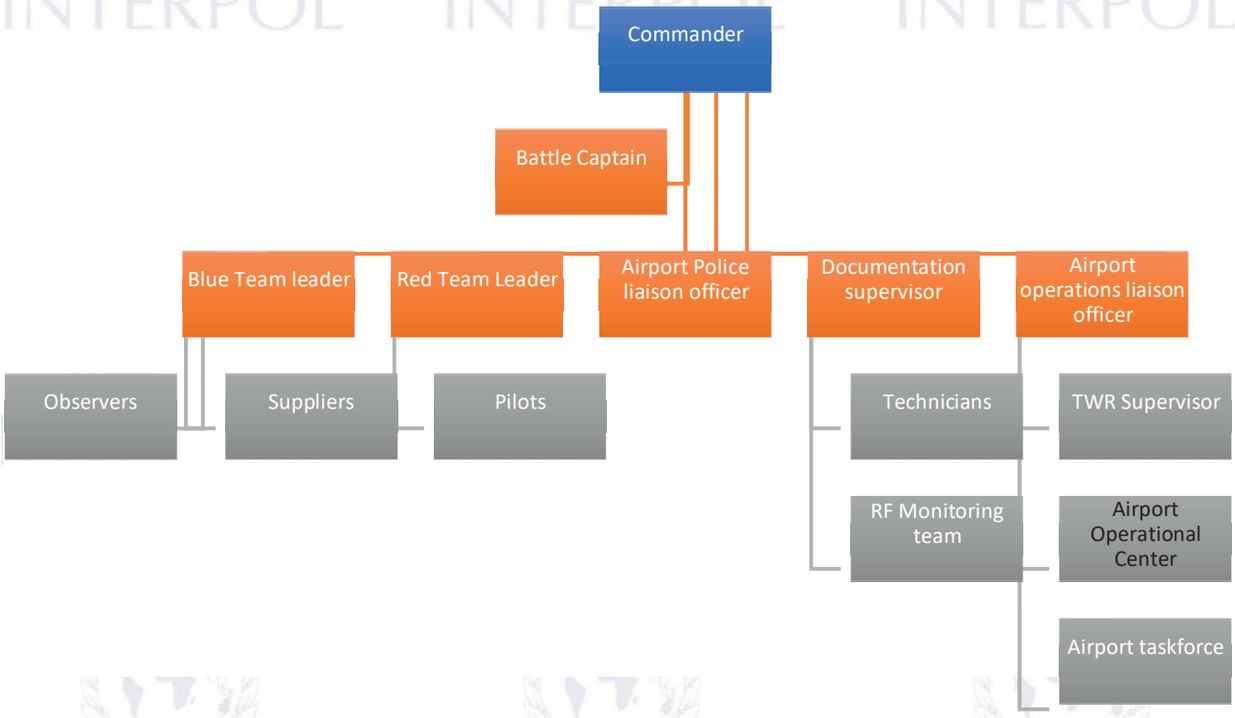

Figure 14:Diagram of the organization of test personnel

Different roles had different responsibilities, as follows:

- **Commander** – in charge of the planning, execution, and evaluation of the exercise. Single point of contact for the airport operator.

- **Battle Captain** – assistant to the commander, general manager of the tactical operations, responsible for the timeline of the exercise

- **Blue Team leader** – in charge of the documentation of the tests and making sure suppliers were compliant at all times during the exercise

- **Red Team Leader** – responsible for the planning and execution of all drone operations during the exercise

- **Airport police liaison officer** – responsible for enhanced safety and security in proximity to the exercise
- **Documentation supervisor** – responsible for collecting and storing all the reports, logs, files, images, etc., that were collected during the exercise
- **Airport operations liaison officer** – in charge of assessing and coordinating the daily airport operations
- **Blue Team Observers** – Responsible for monitoring the C-UAS systems during each test and relaying information from the Battle Captain and Blue Team leader to the suppliers
- **Suppliers** – Responsible for installation and operation of their C-UAS systems
- **Red Team Pilots** – Responsible for conducting all drone operations during the exercise
- **Technicians** – Responsible for installing and operating the video recording system, the technical equipment for the control room, and radio communications.
- **RF Monitoring team** – Responsible for monitoring and reporting any violations of the RF spectrum during the exercise
- **TWR Supervisor** – Responsible for all air traffic within the airport control zone
- **Airport Operational Center** – Responsible for all technical operations at the airport
- **Airport task force** – Responsible for addressing any unforeseen challenge during the exercise

4.3 Exercise Communication

When several organizations and individuals are required to communicate in a potentially dangerous location, effective and simple procedures are needed. The importance of good, clear communication is summarized by the saying: "Without effective communication, a message can turn into an error, misunderstanding, or even a disaster by being misinterpreted or poorly delivered." The exercise management understood the importance of ensuring good communication at all levels during the exercise. Subsequently, it was considered equally important to make sure to assign responsibilities, functions, and means of communication as clearly and accurately as possible to avoid any misunderstanding that could jeopardize manned air traffic.

4.3.1 Example of the communication procedure to define the exercise area as operational

Timeline	Incident	Responsible	Phraseology
00:00	Supervisor request the operational commander to close "Flying Zone" and hand it over to airport duty officer	TWR Supervisor	TWR LIASON, SUPERVISOR, REQUEST THAT "FLYING ZONE" CLOSE. MOVE TO LVP READY
00:01	Supervisor calls APOC Safety, and asks to transition to two runways (SPO/MPO) from xx:15 APOC Safety execution procedure: A.0X-X. Reset to normal operations on both runways	TWR Supervisor	APOC SAFETY, THIS IS TWR SUPERVISOR. INITIATE RESET NORMAL OPERATIONS BOTH RUNWAYS FROM XX:15,
00:01	APOC Safety acknowledges message received and notify that he/she will notify when ready "ready normal operations both runways". APOC	APOC Safety	

	Safety execute procedure "A.0X-X. Transition normal operations both runways"		
00:01	Liaison request operational commander and ask him/her to close the flying zone and report when all units are on the ground and switched off.	TWR liaison	OPERATIONAL COMMANDER, TWR LIASON. CLOSE "FLYING ZONE" REPORT ALL UNITS ON GROUND AND SWITCHED OFF, READY TO HAND OVER
00:01	*Operational commander orders all units to be grounded and switched off. Confirmation from all units that exercise is put on standby.*	Operational Commander	ALL UNITS, ALL UNITS, THIS IS COMMANDER, NO PLAY, I SAY AGAIN, NO PLAY. REPORT ALL UNITS ON GROUND AND OFF
00:03	*RED TEAM leader makes sure and signs that units are passive and on ground*	RED TEAM leader	RED TEAM LEADER, ALL UNITS ON GROUND and OFF, OVER
00:03	*BLUE TEAM leader makes sure and signs that all units are passive and on ground*	BLUE TEAM leader	BLUE TEAM LEADER, ALL UNITS ON GROUND AND OFF, OVER
00:04	*Green flag hoisted; when the flag is hoisted and confirmations have been received from Red team and Blue team that all units that could affect infrastructure are on the ground and off, the Flying Zone is handed over to the TWR Liaison*	Operational Commander	TWR LIASON, THIS IS COMMANDER, "FLYING ZONE" IS YOURS.

Table 1: Example of the communication procedure to define the exercise area as operational

4.3.2 Example procedure: Blue Team, how to ensure all C-UAS systems are grounded and switched off

Timeline	Incident	Responsible	Phraseology
00:03	*BLUE TEAM leader makes sure and signs that all units are passive and on the ground*	BLUE TEAM leader	THIS IS BLUE LEADER, ALL UNITS ARE TO BE
00:03	*Blue team representative located with C-UAS supplier 2 makes sure the all their units are off*	BLUE TEAM 2 – supplier Y	THIS IS BLUE 2 SUPPLIER Y, ALL UNITS ARE OFF
00:03	*When all has reported, BLUE TEAM leader has representatives from the frequency regulators (NKOM) double-check using a spectrum analyzer*	BLUE TEAM leader	THIS IS BLUE LEADER, NKOM VERIFY THAT ALL UNITS ARE OFF, REPORT
00:03	*Frequency regulators (NKOM) check each supplier using a spectrum analyzer to make sure all units are off*	Frequency regulators (NKOM)	THIS IS NKOM, CONFIRM ALL UNITS ARE OFF
00:03	*BLUE TEAM leader makes sure and signs that all units are on the ground and switched off*	BLUE TEAM leader	BLUE TEAM LEADER, ALL UNITS ON GROUND AND OFF

Table: Example procedure of how to make sure all C-UAS systems are on the ground and switched off.

4.4 Documenting the Tests

To evaluate each test, the following data sources were used:

- Video grabbing tool to record the actual screen the C-UAS operator sees during the test
- Logs from the C-UAS system
- Flight logs from the drone
- Notes and records from the Blue Team observers including:
  - o Relevant times for test start, drone discovery, positions, etc.
  - o Relevant information from the C-UAS system
  - o Blue Team Observers own notes for the test and the system used

All documentation was stored on a server on-site for safekeeping. At the conclusion of the exercise, all recordings were imported into a video editing timeline based on the time information visible in the actual recording. Most systems have a defined server-time visual on their operator screens. For the single system that did not have this information, the logs were used to identify actual events on the screen, and those events were paired with log entries showing time stamps.

The flight logs, paths, and metadata were used to generate a video file containing a visual representation for the flight path and the relevant metrics from the drone.

With these recordings on a timeline, a real-time representation could be generated to display a sideby- side comparison of what the drone did and what the C-UAS system identified. The result was extensive documentation of 61 exercises over 52 flights. The lower number of flights was due to the simultaneous testing of the passive systems. A total of 7 TB of data was generated during the exercise; all data generated had to be verified after the event.

Appendix 5: Evaluation of the Test prepared by the Norwegian Police and TEKDIR AS.

5.1 Introduction

This section describes the parameters devised for the evaluation of the various technologies in the prepared scenarios, along with the scoring and point scaling. This was developed in consultation with several member countries that were already testing C-UAS and be leveraging their knowledge and expertise we were able to create a neutral framework for testing based on their experiences and challenges that they had encountered during their C-UAS testing and assessments.

5.2 Scoring the Tests

The overall scenario of the exercise was the use of a drone in a non-hostile manner but creating an unwanted safety risk by doing so. By applying countermeasures, the purpose was primarily to give decision-makers the information needed to shut down parts of or the entire airport. Within that scope, exercise management selected the information that was absolutely crucial, what information was relevant, and what information was "nice to have". The points given for each parameter were scaled to indicate each parameter's relative importance. As an example, one can argue that a false positive is comparative to the threat of an actual drone. As the purpose of this exercise was to evaluate different types of technology, this exercise did not score a winner. However, to practically assess whether a system is usable in an airport scenario; datapoints for each exercise were identified to be extracted, and they are discussed in the next section.

5.3 Scoring Parameters

Length of the test: The duration of the test, recorded as in seconds. This parameter was used to score the detection and localization point of time.

Detection points of time: Time of detection. The definition of "detection" for this event was the notification that there were clear indications a drone was present, but the drone was not necessarily identified by type or defined position. Recorded as seconds. If the system did not detect the drone, an N/A was recorded. The score was calculated by dividing the seconds of detection time by the length of the test.

Localization points of time: Time at which the system localized the drone. For the test, the definition of "localized" was that the C-UAS provided a visual indication of where the drone was geographically. It was recorded in seconds. If the system did not localize the drone, a N/A was recorded. The score was calculated by dividing the seconds of localization time by the length of the test.

Drone detected: Did the C-UAS detect the drone? Recorded as YES or NO. If detected, 50 points were given.

Position accuracy: Did the C-UAS display an accurate position of the drone within 100 meters? Recorded as YES or NO. If accurate, 50 points were given.

Speed: Did the C-UAS system display the speed of the drone? Recorded as YES or NO. If the C-UAS did this, 25 points were given.

Altitude: Did the C-UAS system display the altitude of the drone? Recorded as YES or NO. If the C-UAS did this, 25 points were given.

Direction: Did the C-UAS system display the travel direction of the drone, either with an arrow or with a compass? Recorded as YES or NO. If the C-UAS did this, 25 points were given.

Path map: Did the C-UAS system display the path the drone had already travelled? Recorded as YES or NO. If the C-UAS did this, 25 points were given

Producer of drone: Did the C-UAS system display the manufacturer of the drone detected? Recorded as YES or NO. If the C-UAS did this, 10 points were given.

Model: Did the C-UAS system display the model of the drone detected? Recorded as YES or NO. If the C-UAS did this, 10 points were given.

Drone ID/Serial: Did the C-UAS system display the droneID, MAC address, or serial number of the drone detected? Recorded as YES or NO. If the C-UAS did this, 10 points was given.

Pilot position located: Did the C-UAS system display the position of the pilot's remote control? Recorded as YES or NO. If the C-UAS did this, 25 points were given.

Wrong pilot position: If the C-UAS system showed the pilot's position, did it show the wrong pilot position during the test? Recorded as YES or NO. If the pilot's position was incorrect, -25 points were given (to void the score given for the pilot's position; see previous scoring criterion).

Number of false positives: Did the C-UAS system give false positives during the test? Recorded with number of incidents. Scored with -3 points per false positive.

Position lost more than 3 sec: Did the C-UAS system lose the ability to locate the drone for between 3 and 5 seconds after it located the drone? Recorded with number of incidents. Scored with -3 points per incident.

Loss of signal 6-10 sec: Did the C-UAS system lose the ability to locate the drone for between 6 and 10 seconds after it located the drone? Recorded with number of incidents. Scored with -5 points per incident.

Loss of signal 11+ sec: Did the C-UAS system lose the ability to locate the drone for more than 11 seconds after it located the drone? Recorded with number of incidents. Scored with -7 points per incident.

Criteria	Unit	Point Scaling	POS/NEG
Flight length	Seconds	-	-
Detection point of time	Seconds	-	-
Position point of time	Seconds	-	-
Is the drone detected	Points	50	POS
Position accuracy +-R100m	Points	50	POS
Shown Data: Speed	Points	25	POS
Shown Data: Height	Points	25	POS
Shown Data: Direction	Points	25	POS
Shown Data: Path map	Points	25	POS
Shown Data: Producer of drone	Points	10	POS
Model	Points	10	POS
Shown Data: Drone ID/Serial	Points	10	POS
Shown Data: Pilot position located	Points	25	POS
Wrong pilot position	Points	25	NEG
Number of false positives	Points	3	NEG
Position lost 3-5 sec	Points	3	NEG
Loss of signal 6-10 sec	Points	5	NEG
Loss of signal 11+ sec	Points	7	NEG

Table 3: Scoring criteria, and point values for each criterion

5.4 Analyzing Data for Scoring

The data from the exercise is primarily provided from devices that recorded the live video footage of each system as the exercises took place. It was also asked all suppliers to provide the logs from their system directly after each exercise. The exercise had blue team observers that monitored each exercise and manually recorded key data.

Both the recordings and the logs were stored on a server on site for safekeeping. When the exercise was finished, the recordings were inserted into a video editing timeline based on the time-information visible in the actual recording. Most systems had a defined server-time visual on their operator screens. On the system that did not have this information displayed, the commander used the logs to identify actual events on the screen and paired them with log entries showing time.

Flight logs were then analyzed, data were extracted, and a video with a visual path and system notifications was created. With all of the available videos, a recorded, real-time representation of what actually happened was generated and compared to the visual representation provided by each system.

5.5 C-UAS System Supplier Code Names

Participating systems were anonymized by giving them code names. A list of code names and type of system is provided in Table 4.

Codename	Sensor Type
BALDER	RF Sensors, Radar, and Jammer
BRAGE	RF Sensors, Optical, and Jammer
FRIGG	Radar and Optical
FROYA	RF Sensors, Acoustic, Optical, and Jammer
HEIMDALLR	Radar
LOKE	RF Sensor and Optical
LODUR	Radar
NJORD	RF Sensor, Optical, and Radar
ODIN	RF-Sensor
TOR	RF Sensor, Radar, and Jammer
TYR	Radar
ULLR	RF Sensor and Optical
VALI	Jammer
VIDAR	Jammer

Table 4 Systems participating in the event, and type of system

Appendix 6: Test Results prepared by the Norwegian Police and TEKDIR AS.

6.1 Introduction

The results of all three system tests conducted during the INTERPOL Drone Incursion Exercise in 2021 are described here, as well as screenshots captured from the C-UAS system during each test. These scores were derived from analyzing the data taken from the drone flown during the test, from the C-UAS system data, and from a neutral observer, who was stationed at the C-UAS system during the test. After the drone testing was complete, data collected from the C-UAS system, the observer, and the drone was combined and verified to ensure the drone was detected, tracked, and identified and scored correctly. In addition to consulting with the C-UAS providers, the analysis and verification of the three tests took approximately four months.

6.2 Results of Passive System Tests

The first test was the test of passive sensors. Since passive sensors do not have an external effect or interfere with other sensors, systems, or technologies, all passive sensors were tested simultaneously. The test was conducted on Tuesday, September 28th, at 10:32 CET. Three test scenarios were conducted: RED, BLUE, and CYAN. The drones used to test the capabilities of the passive systems were a DJI Mavic Enterprise 2, a DJI Mini 2, and a DJI Matrice 210 V2. The weather was cloudy, with a temperature of 10C. The test was completed at 11:38 CET. Detailed test results are provided in figures 14 – 21; screen caps of system displays are provided in figures 22 – 27.

PASSIVE SENSOR					
Supplier	1	2	3	Total	Average
BRAGE	405	355	405	1165	388
ODIN	272	324	267	863	288
FROYA	239	249	154	642	214
TOR	152	NA	140	292	146
ULLR	155	152	151	458	153
BALDER	375	347	382	1104	368
LOKE	148	241	142	531	177

Fig. 14 Summary of results from Passive test

BRAGE				
TOTAL SCORE				
1165				
		Test Scores		
		Active	Active	Active
No of Tests	Avg. Points	Flight ID 4	Flight ID 5	Flight ID 6
3	388	405	355	405
Flight length (seconds)		297	670	491
Detection point of time (seconds)		0	0	0
Postition point of time (seconds)		0	0	0
Total Points		0	0	0
Detection Altitude (Meters)		0	0	0
Position Detection Altitude (Meters)		0	0	0
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		50	0	50
Shown Data: Speed (points)		25	25	25
Shown Data: Altitude (points)		25	25	25
Shown Data: Direction (points)		25	25	25
Shown Data: Path map (points)		0	0	0
Shown Data: Producer of drone (points)		10	10	10
Shown Data: Model (points)		10	10	10
Shown Data: Drone ID/Serial (points)		10	10	10
Shown Data: Pilot position located (points)		0	0	0
Total Points		205	155	205
Wrong pilot position (points)		0	0	0
Number of false positives (points)		0	0	0
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	-5
Position lost more than 11+ sec (points)		0	0	0
Total Points		0	0	0
Corrected Values		200	200	200

Fig. 15 Results of the test of passive systems; from BRAGE

ODIN				
TOTAL SCORE				
863				
		Test Scores		
		Passive	Passive	Passive
No of Tests	Avg. Points	Flight ID 1	Flight ID 2	Flight ID 3
3	288	272	324	267
Flight length (seconds)		297	670	491
Detection point of time (seconds)		82	0	39
Postition point of time (seconds)		82	0	39
Total Points		-55	0	-16
Detection Altitude (Meters)		0	0	64
Position Detection Altitude (Meters)		18	0	64
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		50	0	50
Shown Data: Speed (points)		0	0	0
Shown Data: Altitude (points)		25	25	25
Shown Data: Direction (points)		0	0	0
Shown Data: Path map (points)		25	25	25
Shown Data: Producer of drone (points)		10	10	0
Shown Data: Model (points)		10	10	10
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		25	25	25
Total Points		145	145	135
Wrong pilot position (points)		0	0	0
Number of false positives (points)		0	0	0
Position lost more than 3 sec. (points)		-18	-21	-45
Position lost more than 6-10 sec (points)		0	0	-5
Position lost more than 11+ sec (points)		0	0	-7
Total Points		-18	-21	-52
Corrected Values		200	200	200

Fig. 16 Results of the test of passive systems; from ODIN

INTERPOL

FROYA				
TOTAL SCORE				
642				
		Test Scores		
		Passive	Passive	Passive
No of Tests	Avg. Points	Flight ID 1	Flight ID 2	Flight ID 3
3	214	239	249	154
Flight length (seconds)		297	670	517
Detection point of time (seconds)		18	48	109
Postition point of time (seconds)		55	125	139
Total Points		-25	-26	-48
Detection Altitude (Meters)		60	80	64
Position Detection Altitude (Meters)		60	117	64
Total Points		0	0	0
Drone detected (points)		50	50	0
Postition accuracy +-R100m (points)		0	0	0
Shown Data: Speed (points)		0	0	0
Shown Data: Altitude (points)		0	0	0
Shown Data: Direction (points)		0	0	0
Shown Data: Path map (points)		25	25	25
Shown Data: Producer of drone (points)		10	10	10
Shown Data: Model (points)		0	0	0
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		25	25	25
Total Points		85	85	35
Wrong pilot position (points)		0	0	0
Number of false positives (points)		0	-3	-33
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	0
Position lost more than 11+ sec (points)		-21	-7	0
Total Points		-21	-10	-33
Corrected Values		200	200	200

Fig. 17 Results of the test of passive systems; from FROYA

ULLR				
TOTAL SCORE				
458				
		Test Scores		
		Passive	Passive	Passive
No of Tests	Avg. Points	Flight ID 1	Flight ID 2	Flight ID 3
3	153	155	152	151
Flight length (seconds)		297	670	491
Detection point of time (seconds)		45	52	91
Postition point of time (seconds)		ND	ND	ND
Total Points		-115	-108	-119
Detection Altitude (Meters)		24	0	8
Position Detection Altitude (Meters)		0	0	64
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		0	0	0
Shown Data: Speed (points)		0	0	0
Shown Data: Altitude (points)		0	0	0
Shown Data: Direction (points)		0	0	0
Shown Data: Path map (points)		0	0	0
Shown Data: Producer of drone (points)		10	10	10
Shown Data: Model (points)		10	0	10
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		25	25	25
Total Points		70	60	70
Wrong pilot position (points)		0	0	0
Number of false positives (points)		0	0	0
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	0
Position lost more than 11+ sec (points)		0	0	0
Total Points		0	0	0
Corrected Values		200	200	200

Fig. 18 Results of the test of passive systems; from ULLR

LOKE				
TOTAL SCORE				
531				
		Test Scores		
		Passive	Passive	Passive
No of Tests	Avg. Points	Flight ID 1	Flight ID 2	Flight ID 3
3	177	148	241	142
Flight length (seconds)		297	670	491
Detection point of time (seconds)		5	31	37
Postition point of time (seconds)		ND	31	ND
Total Points		-102	-9	-108
Detection Altitude (Meters)		28	0	0
Position Detection Altitude (Meters)		60	0	0
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		0	0	0
Shown Data: Speed (points)		0	0	0
Shown Data: Altitude (points)		0	0	0
Shown Data: Direction (points)		0	0	0
Shown Data: Path map (points)		0	0	0
Shown Data: Producer of drone (points)		0	0	0
Shown Data: Model (points)		0	0	0
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		0	0	0
Total Points		50	50	50
Wrong pilot position (points)		0	0	0
Number of false positives (points)		0	0	0
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	0
Position lost more than 11+ sec (points)		0	0	0
Total Points		0	0	0
Corrected Values		200	200	200

Fig. 19 Results of the test of passive systems; from LOKE

TOR				
TOTAL SCORE				
292				
		Test Scores		
		Passive	Passive	Passive
No of Tests	Avg. Points	Flight ID 1	Flight ID 2	Flight ID 3
2	146	152	NA	140
Flight length (seconds)		297	NA	491
Detection point of time (seconds)		25	NA	96
Postition point of time (seconds)		ND	NA	ND
Total Points		-108	NA	-120
Detection Altitude (Meters)		60	NA	64
Position Detection Altitude (Meters)		0	NA	0
Total Points		0	NA	0
Drone detected (points)		50	NA	50
Postition accuracy +-R100m (points)		0	NA	0
Shown Data: Speed (points)		0	NA	0
Shown Data: Altitude (points)		0	NA	0
Shown Data: Direction (points)		0	NA	0
Shown Data: Path map (points)		0	NA	0
Shown Data: Producer of drone (points)		10	NA	10
Shown Data: Model (points)		0	NA	0
Shown Data: Drone ID/Serial (points)		0	NA	0
Shown Data: Pilot position located (points)		0	NA	0
Total Points		60	NA	60
Wrong pilot position (points)		0	NA	0
Number of false positives (points)		0	NA	0
Position lost more than 3 sec. (points)		0	NA	0
Position lost more than 6-10 sec (points)		0	NA	0
Position lost more than 11+ sec (points)		0	NA	0
Total Points		0	NA	0
Corrected Values		200	NA	200

Fig. 20 Results of the test of passive systems; from TOR

BALDER				
TOTAL SCORE				
1104				
		Test Scores		
		Passive	Passive	Passive
No of Tests	Avg. Points	Flight ID 1	Flight ID 2	Flight ID 3
3	368	375	347	382
Flight length (seconds)		297	670	491
Detection point of time (seconds)		26	49	31
Postition point of time (seconds)		26	54	31
Total Points		-18	-15	-13
Detection Altitude (Meters)		20	104	46
Position Detection Altitude (Meters)		20	104	46
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		0	0	0
Shown Data: Speed (points)		25	25	25
Shown Data: Altitude (points)		25	25	25
Shown Data: Direction (points)		25	25	25
Shown Data: Path map (points)		25	25	25
Shown Data: Producer of drone (points)		10	10	10
Shown Data: Model (points)		10	10	10
Shown Data: Drone ID/Serial (points)		10	10	10
Shown Data: Pilot position located (points)		25	25	25
Total Points		205	205	205
Wrong pilot position (points)		0	-25	0
Number of false positives (points)		-12	-6	-3
Position lost more than 3 sec. (points)		0	-12	0
Position lost more than 6-10 sec (points)		0	0	0
Position lost more than 11+ sec (points)		0	0	-7
Total Points		-12	-43	-10
Corrected Values		200	200	200

Fig. 21 Results of the test of passive systems; from BALDER

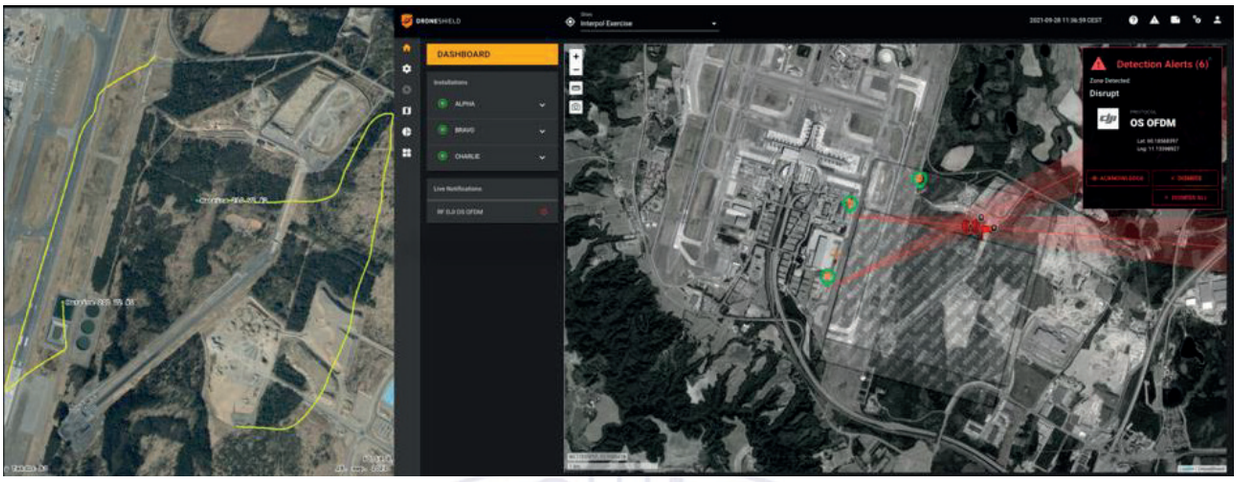

Fig. 22 Screenshot of a system display taken during testing of passive systems; from Droneshield

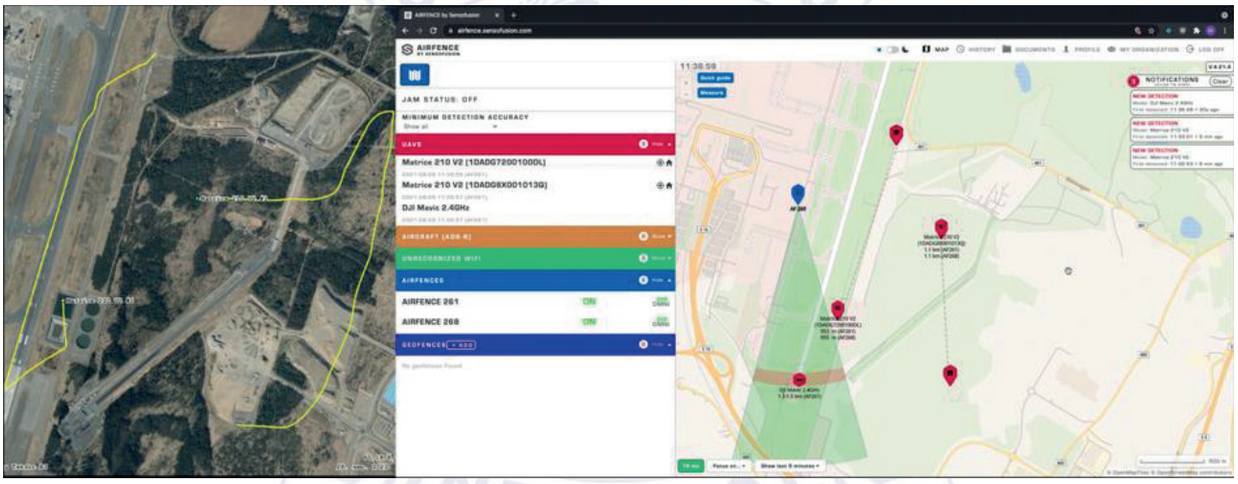

Fig. 23 Screenshot of a system display taken during testing of passive systems; from Sensofusion

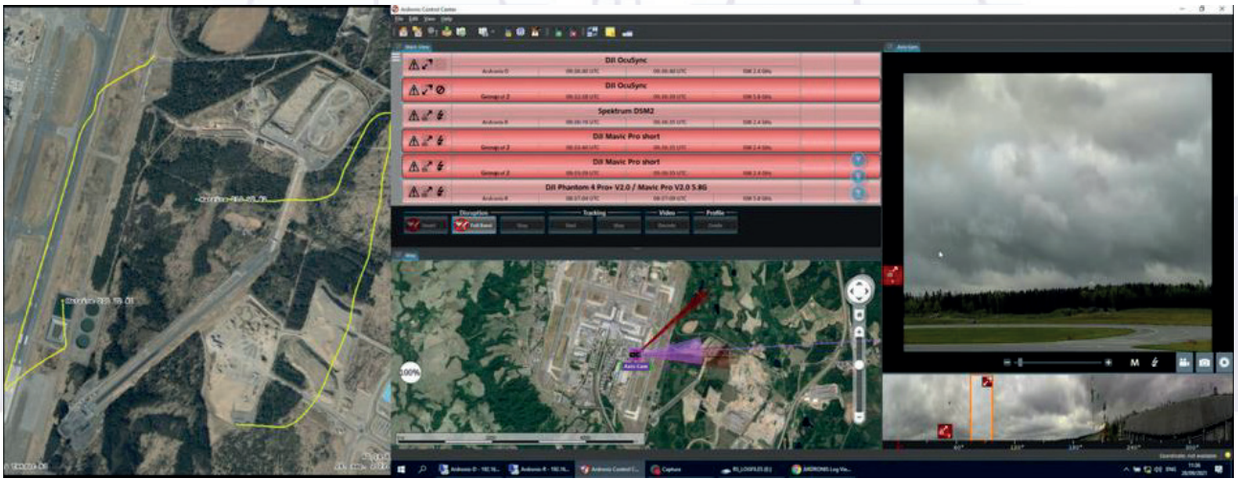

Fig. 24 Screenshot of a system display taken during testing of passive systems; from Rohde & Schwarz

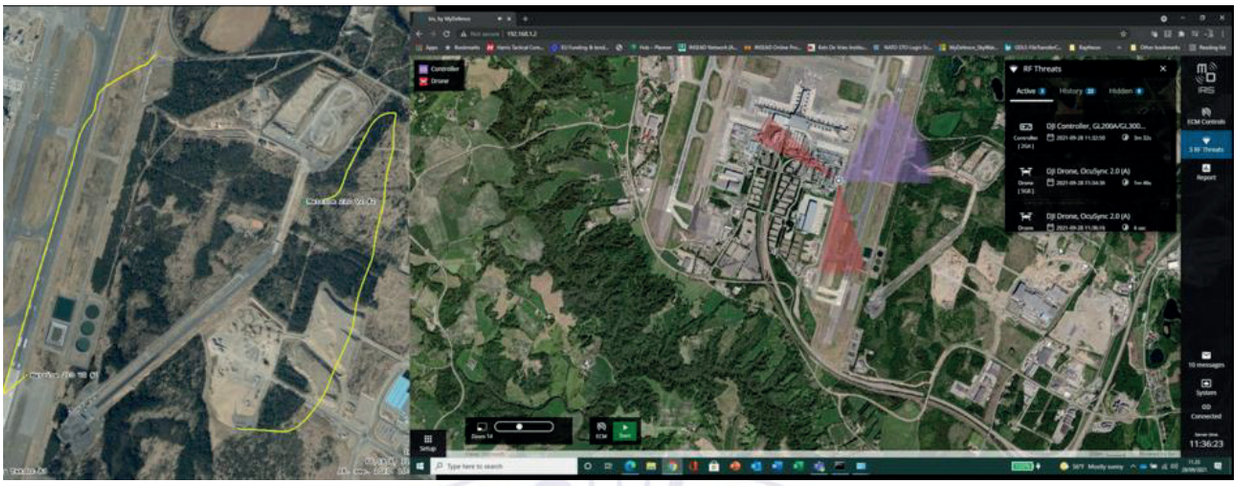

Fig. 25 Screenshot of a system display taken during testing of passive systems; from Mydefence

Fig. 26 Screenshot of a system display taken during testing of passive systems; from D-Fend

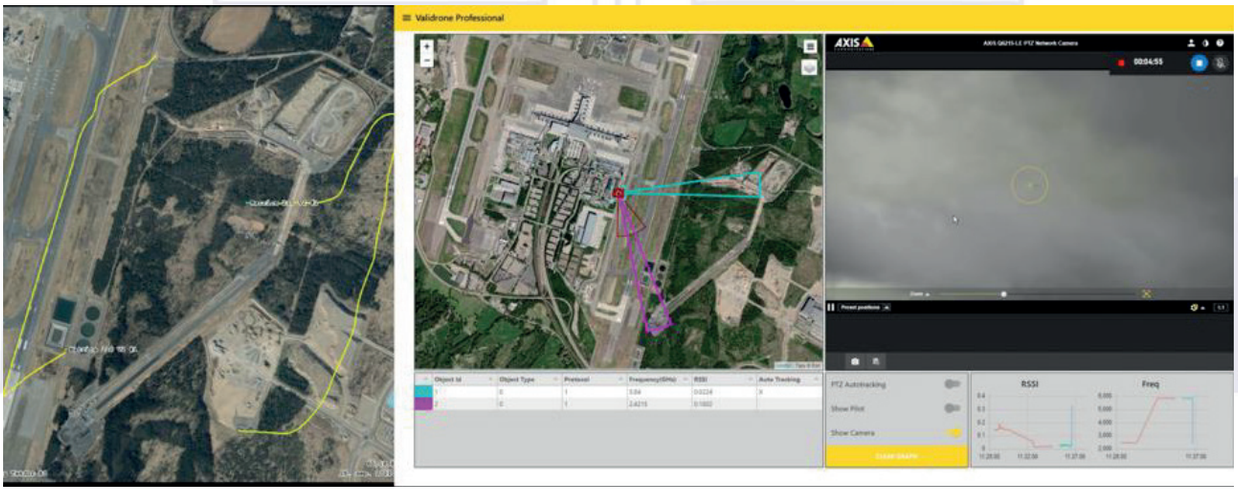

Fig. 27 Screenshot of a system display taken during testing of passive systems; from Stanley

6.3 Tests of Active Systems

The second test conducted during this event was the test of only active sensors. Since active sensors do disturb or interfere with each other, each participating C-UAS system was tested individually. The test was conducted on Tuesday, September 28th starting at 12:42 CET. Three test scenarios were conducted: YELLOW, BLUE, and CYAN. As it was raining during testing, the drone used for testing was a DJI Matrice 210 V2. The temperature was 8C. Testing was completed at 15:34 CET. A summary of the results of the test of active systems is provided in figure 28. Detailed test results are provided in figures 29 – 32. A screen cap of each system taken during testing is provided in figures 33 – 36.

ACTIVE SENSOR					
Supplier	Flight ID				
	4	**5**	**6**	**Total**	**Average**
FRIGG	272	240	277	789	263
LODUR	281	312	296	889	296
HEMIDALLR	310	310	315	935	312
TYR	373	362	NA	735	368

Fig. 28 Summary of results from the testing of active systems

INTERPOL

FRIGG				
TOTAL SCORE				
789				
		Test Scores		
		Active	Active	Active
No of Tests	Avg. Points	Flight ID 4	Flight ID 5	Flight ID 6
3	263	272	240	277
Flight length (seconds)		460	475	457
Detection point of time (seconds)		87	49	31
Postition point of time (seconds)		98	247	31
Total Points		-40	-62	-14
Detection Altitude (Meters)		119	119	65
Position Detection Altitude (Meters)		119	119	65
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		50	50	50
Shown Data: Speed (points)		0	0	0
Shown Data: Altitude (points)		0	0	0
Shown Data: Direction (points)		0	0	0
Shown Data: Path map (points)		25	25	25
Shown Data: Producer of drone (points)		0	0	0
Shown Data: Model (points)		0	0	0
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		0	0	0
Total Points		125	125	125
Wrong pilot position (points)		0	0	0
Number of false positives (points)		-6	-9	-15
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	-5
Position lost more than 11+ sec (points)		-7	-14	-14
Total Points		-13	-23	-34
Corrected Values		200	200	200

Fig. 29 Results of the test of active systems; from FRIGG

HEMIDALLR				
TOTAL SCORE				
935				
		Test Scores		
		Active	Active	Active
No of Tests	Avg. Points	Flight ID 4	Flight ID 5	Flight ID 6
3	312	310	310	315
Flight length (seconds)		523	498	475
Detection point of time (seconds)		72	59	17
Postition point of time (seconds)		72	59	17
Total Points		-28	-24	-7
Detection Altitude (Meters)		109	115	66
Position Detection Altitude (Meters)		109	123	66
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		0	0	0
Shown Data: Speed (points)		25	25	25
Shown Data: Altitude (points)		0	0	0
Shown Data: Direction (points)		0	0	0
Shown Data: Path map (points)		25	25	25
Shown Data: Producer of drone (points)		0	0	0
Shown Data: Model (points)		0	0	0
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		0	0	0
Total Points		125	125	125
Wrong pilot position (points)		0	0	0
Number of false positives (points)		-6	-9	-15
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	-5
Position lost more than 11+ sec (points)		-7	-14	-14
Total Points		-13	-23	-34
Corrected Values		200	200	200

Fig. 30 Results of the test of active systems; from HEIMDALLR

TYR				
TOTAL SCORE				
735				
		Test Scores		
		Active	Active	Active
No of Tests	Avg. Points	Flight ID 4	Flight ID 5	Flight ID 6
2	368	373	362	NA
Flight length (seconds)		423	441	NA
Detection point of time (seconds)		19	65	NA
Postition point of time (seconds)		19	65	NA
Total Points		-9	-29	NA
Detection Altitude (Meters)		35	51	NA
Position Detection Altitude (Meters)		35	97	NA
Total Points		0	0	0
Drone detected (points)		50	50	NA
Postition accuracy +-R100m (points)		50	50	NA
Shown Data: Speed (points)		25	25	NA
Shown Data: Altitude (points)		25	25	NA
Shown Data: Direction (points)		25	25	NA
Shown Data: Path map (points)		25	25	NA
Shown Data: Producer of drone (points)		0	0	NA
Shown Data: Model (points)		0	0	NA
Shown Data: Drone ID/Serial (points)		0	0	NA
Shown Data: Pilot position located (points)		0	0	NA
Total Points		200	200	NA
Wrong pilot position (points)		0	0	NA
Number of false positives (points)		-18	-9	NA
Position lost more than 3 sec. (points)		0	0	NA
Position lost more than 6-10 sec (points)		0	0	NA
Position lost more than 11+ sec (points)		0	0	NA
Total Points		-18	-9	NA
Corrected Values		200	200	NA

Fig. 31 Results of the test of active systems; from TYR

LODUR				
TOTAL SCORE				
889				
		Test Scores		
		Active	Active	Active
No of Tests	Avg. Points	Flight ID 4	Flight ID 5	Flight ID 6
3	296	281	312	296
Flight length (seconds)		449	397	348
Detection point of time (seconds)		106	69	69
Postition point of time (seconds)		106	69	69
Total Points		-47	-35	-40
Detection Altitude (Meters)		120	113	71
Position Detection Altitude (Meters)		120	113	71
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		0	0	0
Shown Data: Speed (points)		25	25	25
Shown Data: Altitude (points)		25	25	25
Shown Data: Direction (points)		25	25	25
Shown Data: Path map (points)		25	25	25
Shown Data: Producer of drone (points)		0	0	0
Shown Data: Model (points)		0	0	0
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		0	0	0
Total Points		150	150	150
Wrong pilot position (points)		0	0	0
Number of false positives (points)		-15	-3	0
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	0
Position lost more than 11+ sec (points)		-7	0	-14
Total Points		-22	-3	-14
Corrected Values		200	200	200

Fig. 32 Results of the test of active systems; from LODUR

Fig. 33 Screenshot of a system display taken during testing of active systems; from FLIR

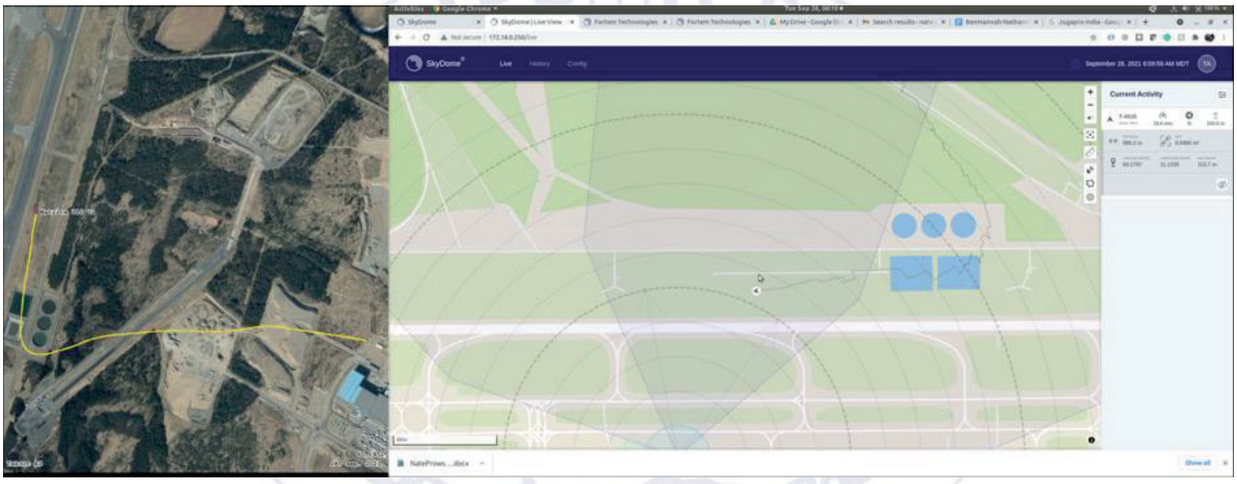

Fig. 34 Screenshot of a system display taken during testing of active systems; from Fortem

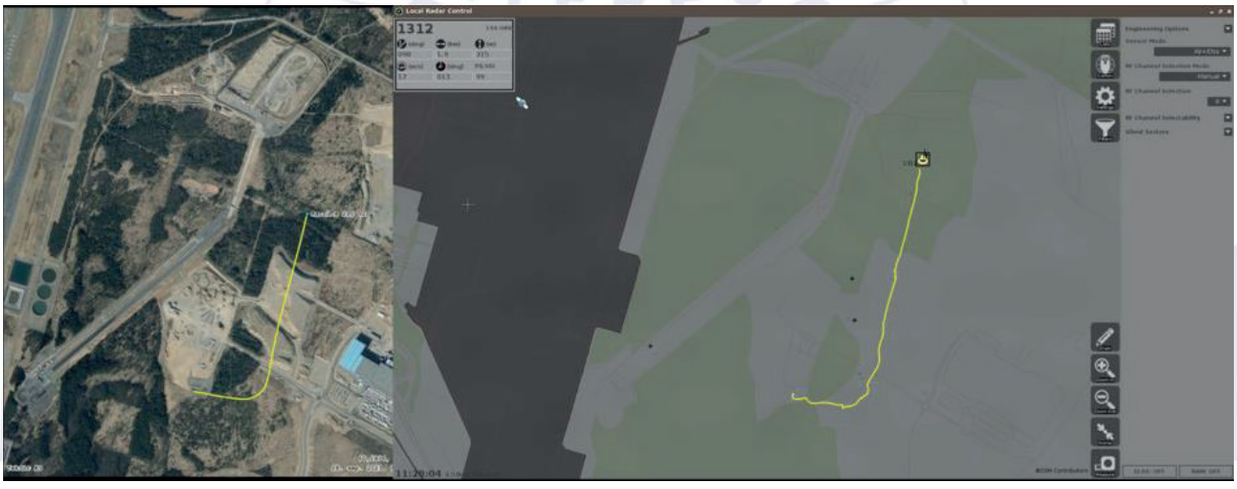

Fig. 35 Screenshot of a system display taken during testing of active systems; from Saab

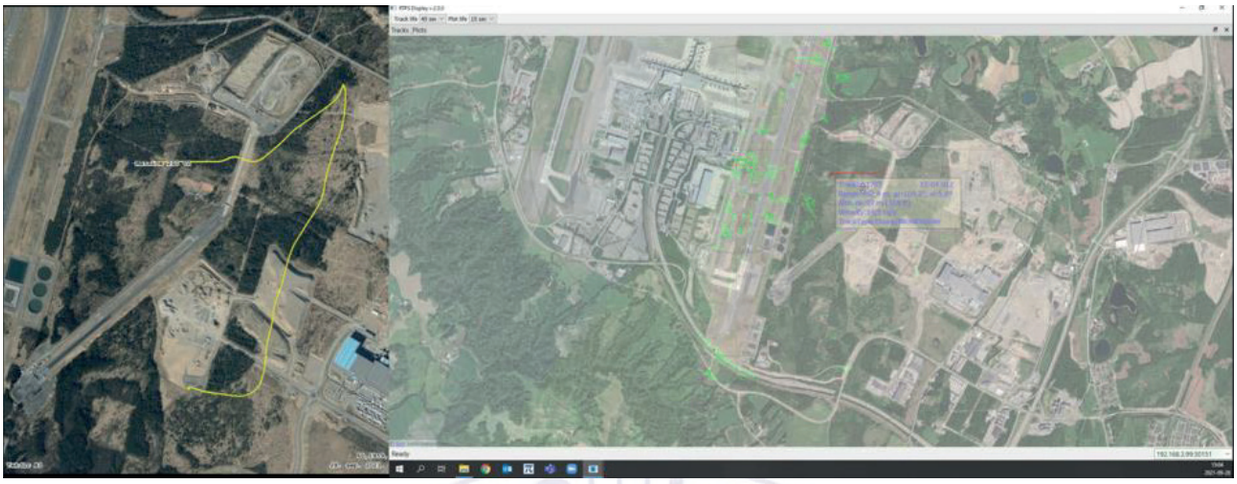

Fig. 36 Screenshot of a system display taken during testing of active systems; from Weibel

6.4 Tests of Multisensor Systems

The third test was the test of multi-sensor C-UAS systems. As these sensors can disturb or interfere with each other, each system was tested individually. The test was conducted on Wednesday, September 29th starting at 11:28 CET. Three test scenarios were conducted: YELLOW, RED, and CYAN. As it was raining, the drone used for testing was a DJI Matrice 210 V2. The temperature was 8C. Testing was completed at 14:54 CET. A summary of the results of the multisensor test is provided in figure 37. Detailed results of each system are provided in figures 38 – 44. Screen caps of the display of each system taken during testing are provided in figures 45 – 51.

MULTIPLE SENSOR					
Supplier	**7**	**8**	**9**	**Total**	**Average**
BRAGE	397	400	0	797	399
FROYA	222	243	249	714	238
FRIGG	212	214	245	671	224
NJORD	227	329	330	886	295
TOR	145	173	234	552	184
BALDER	324	316	338	978	326
LOKE	135	110	135	380	127

Fig. 37 Summary of results from testing of multisensor systems

INTERPOL

BRAGE				
TOTAL SCORE				
797				
		Test Scores		
		Multiple	Multiple	Multiple
No of Tests	Avg. Points	Flight ID 7	Flight ID 8	Flight ID 9
2	399	397	400	0
Flight length (seconds)		411	383	472
Detection point of time (seconds)		10	9	ND
Postition point of time (seconds)		10	9	ND
Total Points		-5	-5	-200
Detection Altitude (Meters)		21	54	26
Position Detection Altitude (Meters)		21	54	26
Total Points		0	0	0
Drone detected (points)		50	50	0
Postition accuracy +-R100m (points)		50	50	0
Shown Data: Speed (points)		25	25	0
Shown Data: Altitude (points)		25	25	0
Shown Data: Direction (points)		25	25	0
Shown Data: Path map (points)		0	0	0
Shown Data: Producer of drone (points)		10	10	0
Shown Data: Model (points)		10	10	0
Shown Data: Drone ID/Serial (points)		10	10	0
Shown Data: Pilot position located (points)		0	0	0
Total Points		205	205	0
Wrong pilot position (points)		0	0	0
Number of false positives (points)		-3	0	0
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	0
Position lost more than 11+ sec (points)		0	0	0
Total Points		-3	0	0
Corrected Values		200	200	200

Fig. 38 Results the test of multisensor systems; from BRAGE

FROYA				
TOTAL SCORE				
714				
		Test Scores		
		Multiple	Multiple	Multiple
No of Tests	Avg. Points	Flight ID 7	Flight ID 8	Flight ID 9
3	238	222	243	249
Flight length (seconds)		366	390	268
Detection point of time (seconds)		93	40	56
Postition point of time (seconds)		93	43	65
Total Points		-51	-21	-33
Detection Altitude (Meters)		76	75	76
Position Detection Altitude (Meters)		76	76	91
Total Points		0	0	0
Drone detected (points)		50	50	0
Postition accuracy +-R100m (points)		50	50	0
Shown Data: Speed (points)		25	25	0
Shown Data: Altitude (points)		25	25	0
Shown Data: Direction (points)		25	25	0
Shown Data: Path map (points)		0	0	0
Shown Data: Producer of drone (points)		10	10	0
Shown Data: Model (points)		10	10	0
Shown Data: Drone ID/Serial (points)		10	10	0
Shown Data: Pilot position located (points)		0	0	0
Total Points		205	205	0
Wrong pilot position (points)		0	0	0
Number of false positives (points)		-3	0	0
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	0
Position lost more than 11+ sec (points)		0	0	0
Total Points		-3	0	0
Corrected Values		200	200	200

Fig. 39 Detailed results of the test of multisensory systems; from FROYA

FRIGG				
TOTAL SCORE				
789				
		Test Scores		
		Active	Active	Active
No of Tests	Avg. Points	Flight ID 4	Flight ID 5	Flight ID 6
3	263	272	240	277
Flight length (seconds)		460	475	457
Detection point of time (seconds)		87	49	31
Postition point of time (seconds)		98	247	31
Total Points		-40	-62	-14
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		50	50	50
Shown Data: Speed (points)		0	0	0
Shown Data: Altitude (points)		0	0	0
Shown Data: Direction (points)		0	0	0
Shown Data: Path map (points)		25	25	25
Shown Data: Producer of drone (points)		0	0	0
Shown Data: Model (points)		0	0	0
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		0	0	0
Total Points		125	125	125
Wrong pilot position (points)		0	0	0
Number of false positives (points)		-6	-9	-15
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	-5
Position lost more than 11+ sec (points)		-7	-14	-14
Total Points		-13	-23	-34
Corrected Values		200	200	200

Fig. 40 Detailed results of the test of multisensory systems; from FRIGG

INTERPOL

BALDER				
TOTAL SCORE				
978				
		Test Scores		
		Multiple	Multiple	Multiple
No of Tests	Avg. Points	Flight ID 7	Flight ID 8	Flight ID 9
3	326	324	316	338
Flight length (seconds)		415	415	397
Detection point of time (seconds)		45	128	34
Postition point of time (seconds)		45	138	34
Total Points		-22	-64	-17
Detection Altitude (Meters)		75	73	24
Position Detection Altitude (Meters)		75	73	24
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		0	0	0
Shown Data: Speed (points)		25	25	25
Shown Data: Altitude (points)		25	25	25
Shown Data: Direction (points)		25	25	25
Shown Data: Path map (points)		25	25	25
Shown Data: Producer of drone (points)		10	10	10
Shown Data: Model (points)		10	10	10
Shown Data: Drone ID/Serial (points)		10	10	10
Shown Data: Pilot position located (points)		25	25	25
Total Points		205	205	205
Wrong pilot position (points)		0	0	0
Number of false positives (points)		0	0	-9
Position lost more than 3 sec. (points)		0	-6	-3
Position lost more than 6-10 sec (points)		-10	-5	-10
Position lost more than 11+ sec (points)		-49	-14	-28
Total Points		-59	-25	-50
Corrected Values		200	200	200

Fig. 41 Detailed results of the test of multisensory systems; from BALDER

NJORD				
TOTAL SCORE				
886				
		Test Scores		
		Multiple	Multiple	Multiple
No of Tests	Avg. Points	Flight ID 7	Flight ID 8	Flight ID 9
3	295	227	329	330
Flight length (seconds)		531	378	610
Detection point of time (seconds)		273	45	39
Postition point of time (seconds)		273	45	39
Total Points		-103	-24	-13
Detection Altitude (Meters)		88	81	50
Position Detection Altitude (Meters)		88	81	50
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		0	0	0
Shown Data: Speed (points)		25	25	25
Shown Data: Altitude (points)		25	25	25
Shown Data: Direction (points)		25	25	25
Shown Data: Path map (points)		25	25	25
Shown Data: Producer of drone (points)		0	10	10
Shown Data: Model (points)		0	0	0
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		0	0	0
Total Points		150	160	160
Wrong pilot position (points)		0	0	0
Number of false positives (points)		-3	0	0
Position lost more than 3 sec. (points)		-3	0	-3
Position lost more than 6-10 sec (points)		0	0	0
Position lost more than 11+ sec (points)		-14	-7	-14
Total Points		-20	-7	-17
Corrected Values		200	200	200

Fig. 42 Detailed results of the test of multisensory systems; from NJORD

TOR				
TOTAL SCORE				
552				
		Test Scores		
		Multiple	Multiple	Multiple
No of Tests	Avg. Points	Flight ID 7	Flight ID 8	Flight ID 9
3	184	145	173	234
Flight length (seconds)		388	377	754
Detection point of time (seconds)		60	121	30
Postition point of time (seconds)		ND	184	100
Total Points		-115	-81	-17
Detection Altitude (Meters)		81	82	50
Position Detection Altitude (Meters)		0	82	50
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		0	0	0
Shown Data: Speed (points)		0	0	0
Shown Data: Altitude (points)		0	0	0
Shown Data: Direction (points)		0	0	0
Shown Data: Path map (points)		0	0	0
Shown Data: Producer of drone (points)		10	10	10
Shown Data: Model (points)		0	0	0
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		0	0	0
Total Points		60	60	60
Wrong pilot position (points)		0	0	0
Number of false positives (points)		0	-3	-6
Position lost more than 3 sec. (points)		0	-3	-3
Position lost more than 6-10 sec (points)		0	0	0
Position lost more than 11+ sec (points)		0	0	0
Total Points		0	-6	-9
Corrected Values		200	200	200

Fig. 43 Detailed results of the test of multisensory systems; from TOR

LOKE				
TOTAL SCORE				
380				
		Test Scores		
		Multiple	Multiple	Multiple
No of Tests	Avg. Points	Flight ID 7	Flight ID 8	Flight ID 9
3	127	135	110	135
Flight length (seconds)		414	480	381
Detection point of time (seconds)		51	145	44
Postition point of time (seconds)		ND	ND	ND
Total Points		-112	-130	-112
Detection Altitude (Meters)		73	73	73
Position Detection Altitude (Meters)		73	70	70
Total Points		0	0	0
Drone detected (points)		50	50	50
Postition accuracy +-R100m (points)		0	0	0
Shown Data: Speed (points)		0	0	0
Shown Data: Altitude (points)		0	0	0
Shown Data: Direction (points)		0	0	0
Shown Data: Path map (points)		0	0	0
Shown Data: Producer of drone (points)		0	0	0
Shown Data: Model (points)		0	0	0
Shown Data: Drone ID/Serial (points)		0	0	0
Shown Data: Pilot position located (points)		0	0	0
Total Points		50	50	50
Wrong pilot position (points)		0	0	0
Number of false positives (points)		-3	-3	-3
Position lost more than 3 sec. (points)		0	0	0
Position lost more than 6-10 sec (points)		0	0	0
Position lost more than 11+ sec (points)		0	-7	0
Total Points		-3	-10	-3
Corrected Values		200	200	200

Fig. 44 Detailed results of the test of multisensory systems; from LOKE

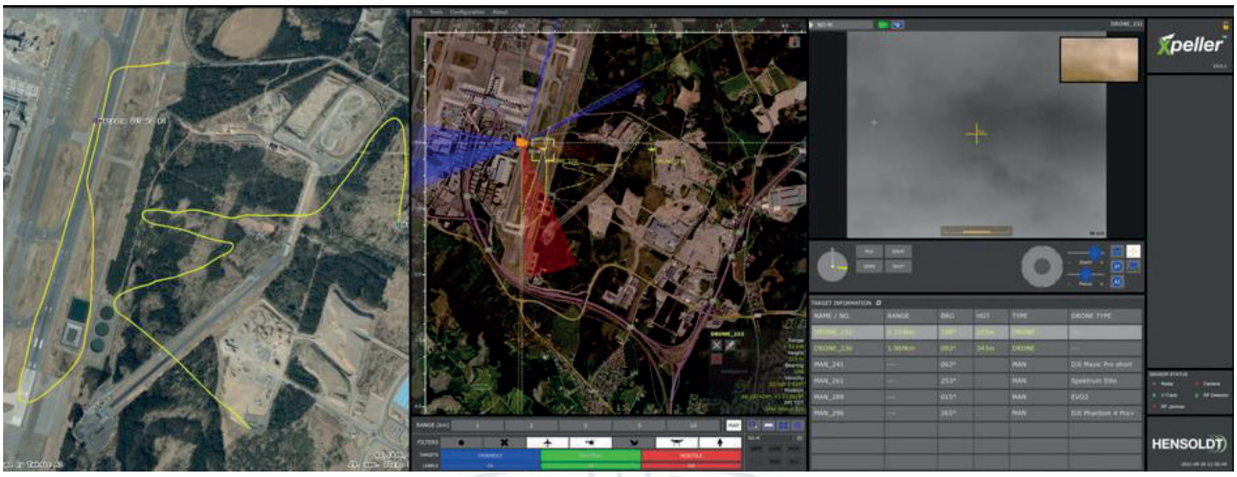

Fig. 45 Screenshot of a system display taken during testing of multisensor systems; from Frequentis

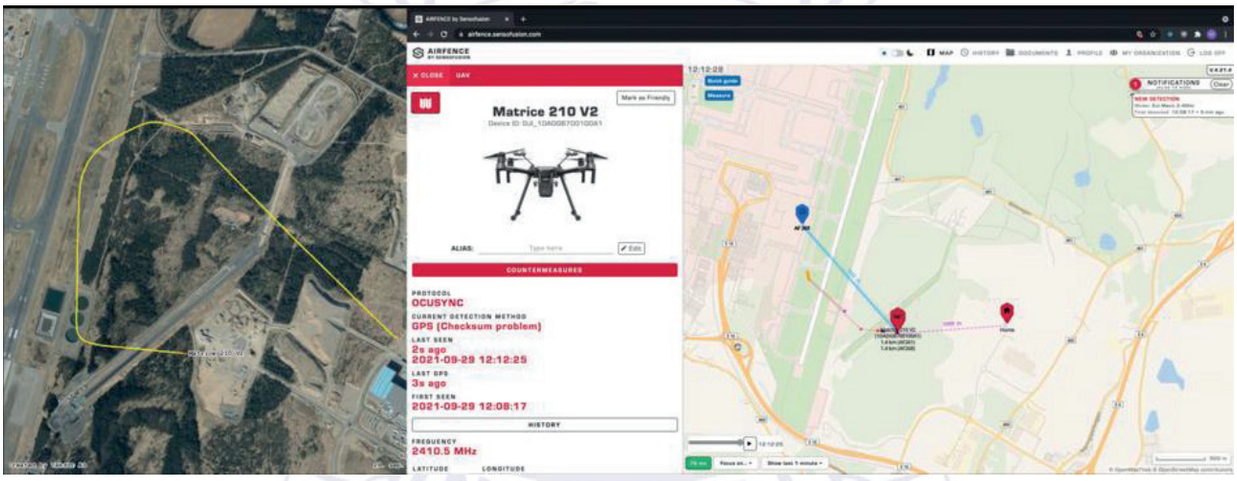

Fig. 46 Screenshot of a system display taken during testing of multisensor systems; from Sensofusion

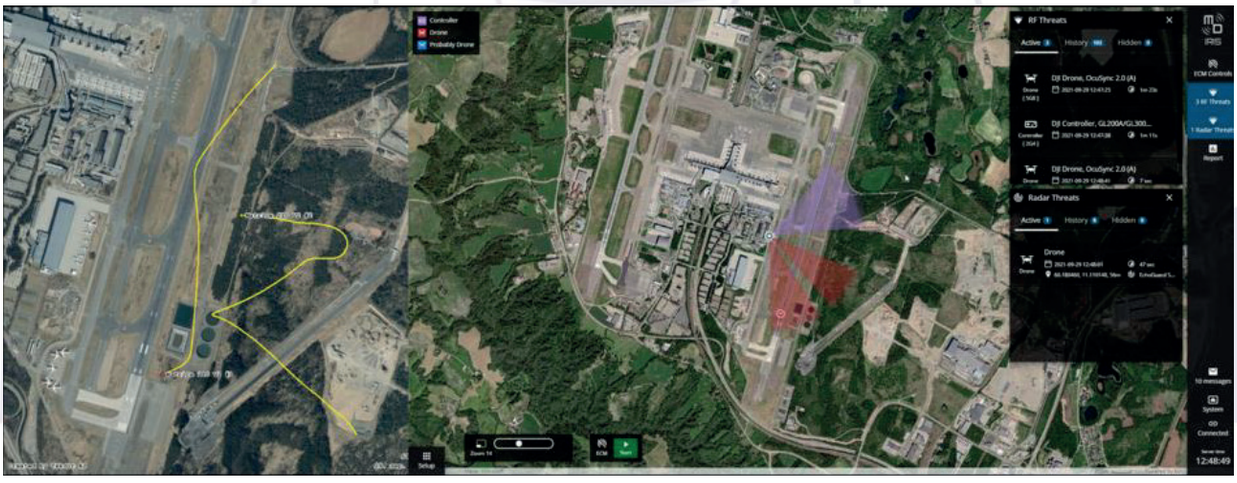

Fig. 47 Screenshot of a system display taken during testing of multisensor systems; from Mydefence

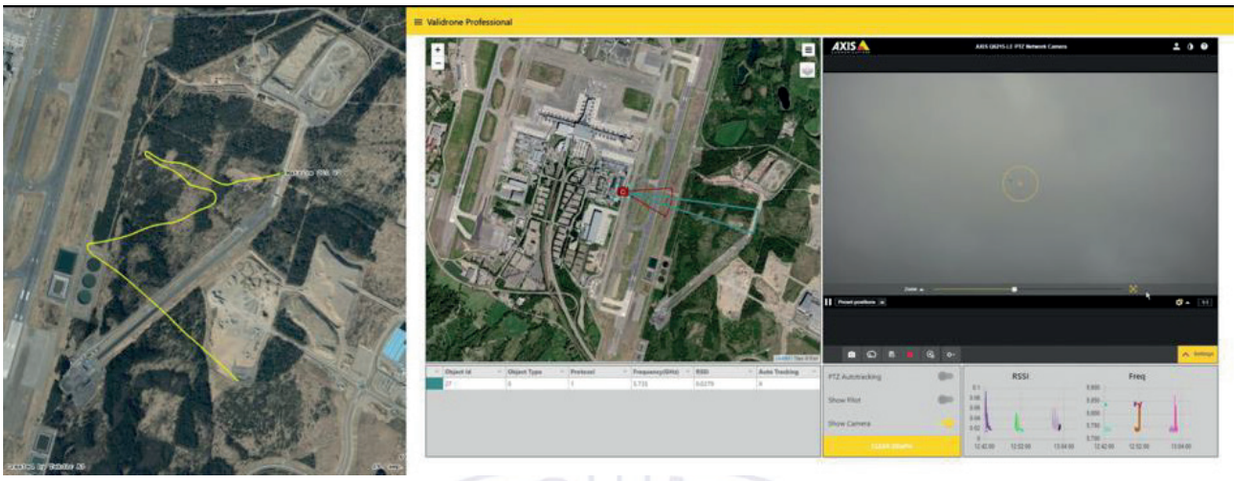

Fig. 48 Screenshot of a system display taken during testing of multisensor systems; from Stanley

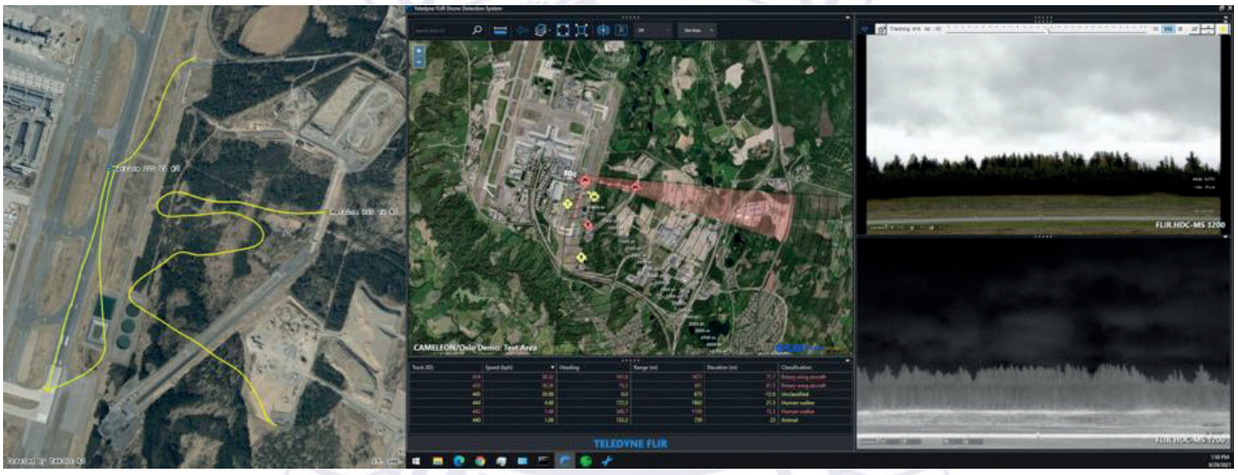

Fig. 49 Screenshot of a system display taken during testing of multisensor systems; from Flir

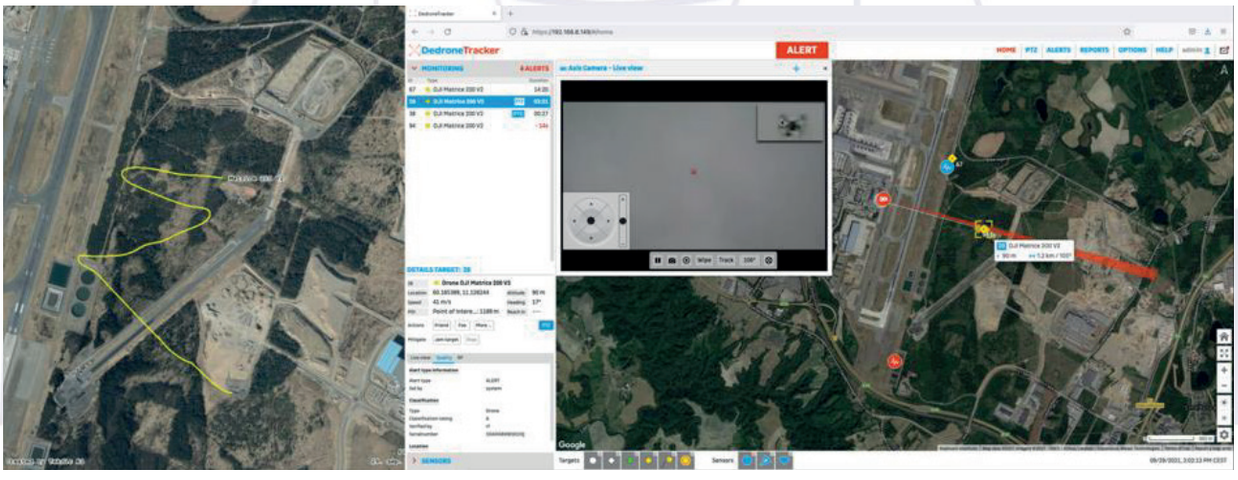

Fig. 50 Screenshot of a system display taken during testing of multisensor systems; from Dedrone

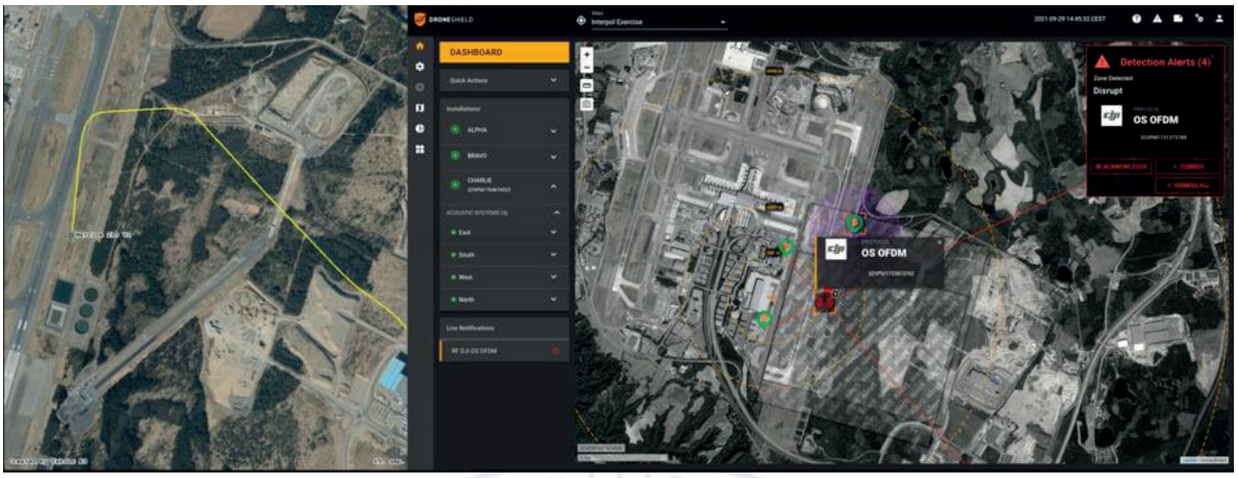

Fig. 51 Screenshot of a system display taken during testing of multisensor systems; from DroneShield

6.5 Jamming Test

The fourth test was the test of mitigation of drones with jamming systems. Each supplier tested their system individually. Each supplier was asked at what distance (between the drone and the system) they would like to start the test. The drone was flown to the specified position, and the supplier jammed for 10 seconds. If the drone was still operational, the drone was moved 100 meters towards the supplier, and the test was restarted. This test protocol continued until the pilot lost control of the drone and the drone activated its emergency return to base programming. The test was conducted on Thursday, September 30th starting at 12:09 CET. Given the fact that a jammer can destroy a drone, a new-out-of-the-box DJI Mini 2 was used for each supplier. The weather was cloudy during testing, and the temperature was 8C. The test was finished at 14:28 CET. A summary of the results of the test of jamming systems is provided in figure 52.

Test	Supplier	Type	Start Distance Test	Distance Loss of Control	Notes
J1	TOR	Stationary Jammer	1000 m	300 m	
J2	ULLR	Stationary Jammer	1000 m	N/A	Device was not successful in jamming drone
J3	VIDAR	Handheld Jammer	1000 m	600 m	
J4	VALI	Handheld Jammer	1000 m	800 m	
J5	FROYA	Handheld Jammer	1200 m	700 m	
J6	BALDER	Stationary Jammer	1500 m	N/A	Disqualified since device was jamming GPS
J7	BRAGE	Handheld Jammer	1500 m	550 m	
J8	BRAGE	Stationary Jammer	1500 m	1000 m	
J9	FROYA	Stationary Jammer	1500 m	500 m	

Fig. 52 Overview of the performance of jamming C-UAS systems

6.6 Technology Round-Up

SENSOR TECHNOLOGY			
TYPE	**Flights ID**		
	Qty of tests	**Total Score**	**Average**
PASSIVE SENSORS	20	5055	253
ACTIVE SENSORS	15	3348	223
MULTIPLE SENSORS	20	4978	249

Fig. 53 Overview of performance of the three types of detection/tracking C-UAS systems that participated in this event

As could be expected, the likelihood of detecting drones manufactured by the world's biggest drone producer was higher than that of detecting drones manufactured by other companies. The primary reason is that all UAV systems using RF-based detection contain the most common drone signatures. Had less popular, custom built, or modified COTS drones been used, the results might have been different.

INTERPOL

Appendix 7: Challenges of the INTERPOL Drone Incursion Exercise 2021 prepared by INTERPOL and the Norwegian Police

7.1 Introduction

This section provides an overview of the challenges identified throughout the INTERPOL Drone Incursion Exercise. This part is specifically relevant for entities seeking to recreate or execute their own C-UAS exercises.

7.2 Challenges

This exercise demonstrated many challenges from the initial planning phase and highlighted several complex situations and elements that emerged during the pre-test evaluation and analysis phase. The following provides a summarized list of scenarios of challenging contexts and issues that should be taken into account for future C-UAS to prevent the alteration of testing results.

7.2.1 Identification of Stakeholders

When preparing for the tests, INTERPOL IC did not anticipate the number of stakeholders that would have to contribute to the exercise to ensure its success. Due to the diverse operating system of an airport environment and the complexity of the exercise, there was a need to include a multitude of stakeholders in the phases of preparation, operation and evaluation of the test. Consequently, after an initially limited number of partners, the number of stakeholders involved in the drone exercise increased significantly. This element created a number of issues in terms of identifying responsibilities that ensured the standard operational functionality of the airport.

These stakeholders ranged from the airport owner – Avinor, to the frequency regulator, the ground handling company, the Ministry of the Interior of Norway, the civil aviation agency, the airline managers, local and national police agencies, military services, and the air traffic controllers. To ensure the safe operation of C-UAS within the airport during the test, these agencies had to be further briefed and engaged in the operational aspects.

7.2.2 Pre-Event Testing of Equipment

Before starting the operational test, it was necessary to gather information on the substantial drone threat potentially faced by Oslo Gardermoen Airport. In order to do so, drone detection equipment apt to monitor the surrounding airspace and detect and register any drone entering the prohibited airspace was installed by the Norwegian Police and airport owner Avinor. This monitoring effort was conducted over the course of three months before the actual drone test. Thanks to this pre-event testing, INTERPOL IC ensured that the threat scenarios used during the evaluations were relevant and applicable to the environment and capability being tested.

7.2.3 Establishing Standardized Testing Criteria

During the initiation phase of these monitoring tests, INTERPOL IC and the Norwegian Police engaged with member countries and regional programmes testing C-UAS to understand better the main criteria implemented, the scope of the objective tested, and any fundamental outcomes that emerged during previous assessments of C-UAS.

Moreover, INTERPOL IC cooperated with numerous agencies and organizations on the phases and analysis of C-UAS testing. In this regard, INTERPOL IC cooperated with the solution providers to fully understand the previous tests. They also collected information on locations, systems, and models of drone devices used during the test analysis. From these numerous exchanges, a significant number of operational drone tests followed similar methodologies and testing criteria. However, these correlation elements were rarely shared or discussed between member countries and related agencies. Hence, introducing a standardized testing methodology and assessment framework would make it possible to reduce the number of tests conducted. This would improve the shared benefits of previous drone assessments among INTERPOL member countries.

7.2.4 Disruption of Airport Activity

The dynamics and disruption of the environment are critical factors to consider when conducting CUAS tests. During the pre-test arrangements, a fundamental element to be taken into account was the extensive amount of disruption to the day-to-day activities within the airport environment. The following interference factors were considered at Oslo Gardermoen Airport: closure of one of the runways, limitation of the airport's capacity, and landing and take-off patterns for airlines.

7.2.5 Operating Restrictions for C-UAS

During the initial phase of testing, it was identified that specific capabilities of the C-UAS systems might have to be inhibited to minimize disruption to airport operations and guarantee systems' functionality within the area. For instance, many systems within the airport rely on GPS time signals; therefore, the use of GPS technology was intentionally avoided during C-UAS testing to prevent disruption being caused to the airport environment.

7.2.6 Certification and Licensing of C-UAS

As in many countries, the use of C-UAS is still a relatively new field, and the current rules, regulations and licensing may not be sufficient for the use of operational test systems. For this reason, INTERPOL IC worked closely with regulators and licensing agencies to ensure strict selection criteria for the C-UAS suppliers, thus minimizing the risk of unknown issues arising during their deployment in the test phases in a very frequency-rich environment.

7.2.7 Drones Required for Testing C-UAS

During the initial planning phase of the test, the goal was to examine several drone devices and models against different systems. However, testing multiple drone devices later proved to be a challenging task. This was mainly because each drone had to be purchased and operated by a certified pilot specifically licensed to operate that specific drone.

During the different test steps at the Oslo Gardermoen Airport, drone pilots from the Norwegian Police were informed of the flight paths that the drones had to conduct and the required attitude and behaviours that the drone should exhibit during the tests. Although a large number of drone scenarios were planned with the intention of testing, only a limited number of flight paths were executed during the actual tests. This was identified as the most efficient way to test each system and ensure they had a reasonable probability of detecting, tracking and identifying the drone being flown.

7.2.8 Testing Frequency Scanning and Monitoring

During the tests, the frequency regulator used numerous frequency scanning and monitoring solutions to verify that the systems stayed within the parameters set in the initial event proposal shared with the C-UAS companies. These monitoring solutions ensured that the C-UAS systems stayed within the operating frequency range. In addition, this ensured that when testing was conducted, the chosen system would remain unaffected by other C-UAS systems or measures.

C-UAS tests generate a considerable amount of data that can vary from drone data to C-UAS system data. Hence, in order to ensure transparency of the results, these data need to undergo an in-depth examination and analysis phase. Because of this, each system was tested using specific criteria that, in some cases, required an ad hoc adaptation to respond accurately to unexpected system responses during the tests.

The drone threat to airports and other areas under law enforcement control will be a target for criminals and terrorists, and by evaluating and assessing C-UAS, LEAs can better prepare themselves for this emerging asymmetrical threat. These tests can be shared through INTERPOL IC to develop a coherent and cohesive global expertise in this area and to ensure that the new and emerging applications where drones are being used for nefarious purposes can be combated and the safety of the public, infrastructure and law enforcement ensured.

Appendix 8: Glossary of Terms, Abbreviations and Acronyms

AGL – Above Ground Level
AGL – Above Ground Level
ANSP – Air Navigation Service Providers
APOC – Airport Operations Center
ATC – Air Traffic Control
ATIS – Automatic Terminal Information
ATM – Air Traffic Management
ATS – Air Traffic Services
BVLOS – Beyond Visual Line of Sight
C-UAS – Counter Unmanned Aircraft Systems
CET – Central European Time
CONOPS – Concept of Operations
COTS – Commercial-off-the-shelf
DG Home – Directorate General for Migration and Home Affairs
DG MOVE – Directorate General for Mobility and Transport
DIMC – Drone Incident Management Cell
DJI – Da-Jiang Innovations
DTI – Detect, Track and Identify
EASA – European Union Aviation Safety Agency
EC – European Community
EMC – Electromagnetic Compatibility
EMI – Electromagnetic Interference
EMS – Electromagnetic System
ENLETS – European Network for Law Enforcement Services
EU MS – European Union Member States
EU – European Union
EUROCONTROL – the European Organization for the Safety Navigation
EUROPOL – European Union Agency for Law
GDPR – General Data Protection Regulation
GLONASS – Space-based Global Navigation Satellite System
GNSS – Global Navigation Satellite System
GPS – Global Positioning Systems
IDIEX21 – INTERPOL Drone Incursion Exercise 2021
INTERPOL IC – Innovation Center
INTERPOL – The International Criminal Police Organization
IoT – Internet of Things
LE – Law Enforcement
LEA(s) – Law Enforcement Agencies
NCASP – National Civil Aviation Security Program
NEG – Negative
NKOM – the Norwegian Communications Authority
NOTAMs – Notices to Airmen
OSL – Oslo Norway
POS – Positive
R&D – Research & Development
RF – Radio Frequency
RVR – Runway Visual Range
SOP – Standard Operating Procedure
SRO – Single Runway Operation
TB – Terabytes
TIG – (Drone Forensic) Technology Interest Group
TRL – Technology Readiness Level
TWR – Air Traffic Control Tower
UAS – Unmanned Aerial Vehicles
UAV(s) – Unmanned Aerial Vehicles
USA – United States of America
VLOS – Visual Line of Sight
Wi-Fi – Wireless Fidelity

INTERPOL

Foto: UAS Norway, Anders Martinsen

INTERPOL

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Our role is to assist law enforcement agencies in our 195 member countries to combat all forms of transnational crime. We work to help police across the world meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. Our services include targeted training, expert investigative support, specialized databases and secure police communications channels.

UAS NORWAY

POLITIET POLITIDIREKTORATET

AVINOR

www.interpol.int

INTERPOL_HQ

INTERPOL_HQ@

INTERPOL HQ

INTERPOL