ANNEX B

ANNUAL REPORT FROM THE GROUP OF RESPONSABLES "AVIATION SECURITY"

The Group of Responsables on Aviation Security was created during the GARTEUR Council meeting in March 2014.
This new GoR is composed of specialists from Research Establishments and Industry who have identified relevant topics to be studied in the Aviation Security area.
GoR AS pursues to do research in the Aviation Security field dealing with both military and civil R&T.
Future GoR AS projects will initiate activities in research fields regarding:

- Cybersecurity in the aviation sector,
- Chemical, Biological and Explosive (CBE) detection,
- Dazzling,
- Malevolent use of RPAS.

Blank page

TABLE OF CONTENTS

AVIATION SECURITY

OVERVIEW

The Group of Responsables on Aviation Security was created during the GARTEUR Council meeting in March 2014. GoR AS pursues to do research in the Aviation Security field dealing with both military and civil R&T.

Four research themes have been identified inside this GoR:

- **Cybersecurity**: Airspace operators (both commercial and military) wish to make use of new communications capabilities to support their missions, develop new cost efficient operations and maintenance procedures, and offer new revenue producing services. These intentions can only be realised by moving more information on and off the aircraft on a regular basis. The latest aircraft therefore rely on interconnected systems which extend off the aircraft to ground-based systems run by airlines, airports and Aviation Service providers of various types. With the continual and rapid integration of new technologies, the aviation industry keeps expanding, changing, and becoming increasingly connected.
  A forthcoming evolution towards net-centric operations of the Air Transport System will occur in the Air Traffic Management domain. The current Air Traffic Management (ATM) system was designed decades ago and is based on an operational concept and technologies which are currently reaching their limits and which will not be able to cope with the expected increase in traffic demand. The "SESAR" project (Single European Sky Air Traffic Management Research) has been set up as a development program for a new ATM system that should be able to handle a 3-fold increase in capacity, while improving the safety performance by a factor of 10, enabling a 10% reduction in the effect flights have on the environment and reducing the ATM services cost to the airspace users by at least 50%.
  Supporting the SESAR ATM system to reach its goals is a net-centric, System Wide Information Management (SWIM) environment that enables sharing essential information between all the ATM stakeholders. It will support collaborative decision making processes, using efficient end-user applications to exploit the power of shared information and will facilitate greater sharing of ATM system information, such as airport operational status, weather information, flight data, etc. In order to accommodate data sharing, SWIM will require introduction of new communication methods and technologies, including the use of commercial internet based solutions.
  The introduction of new technologies and interconnection of systems also introduce new vulnerabilities. Without the appropriate cyber-security measures in place, the air transport system may be at risk. More attention is therefore due to this complex problem.
- **CBE** (Chemical, Biological and Explosive detection): Both, the criminal and the accidental release of chemical, biological and explosive (CBE) substances represent a threat to civil security, especially at public places like airports. Laser based standoff methods offer promising possibilities for early detection and identification of hazardous CBE substances at a distance. People and luggage can be screened nearly instantaneously in a harmless way without any further disturbance of the passengers and by maintaining their integrity. In case of crisis management discrete and reliable detection methods allow for an immediate initiating of counter measures and thereby reduce the threat for people in general and first responders in particular.
- **Dazzling**: In order to protect pilots from dazzling attack, laser radiation present on an aircraft has to be detected and to be reported to the pilots to make them aware of the threat and to prepare protection measures.
- **Malevolent use of RPAS**: Remotely Piloted Aircraft Systems and/or Unmanned Aerial Systems (RPAS/UAS) are expected to become a reality in the airspace within the coming years thanks to their (imminent) integration into non segregated airspace (thanks, among others, to EU roadmap). This will open the airspace not only to security applications but also to a wide number of particular, private, leisure and commercial ones.

Many small and low cost systems (some hundred Euros) such as autonomous model aircraft or micro/mini RPAS/UAS are currently being flown in cities and/or in open environments and will exponentially thrive within this context.
So more effort in prevention has to be done. Security agencies do not count on required technology or procedures to face such a scenario. Closing the airspace is not a solution, as these devices can be deployed few hundreds of meters away from their possible targets and they fly at very low altitude. Normal radars are not able to detect such small objects. Frequency inhibitors or GPS jamming systems may not be effective enough as RPA navigation systems may be based on ground/face recognition and/or radio silence navigation mode. Only several very costly laser based systems have been developed as countermeasures to cope with similar threats (RPAS/UAS or mortar projectiles). However, these technologies are extremely expensive or their use in the urban environment would be questionable.

GOR ACTIVITIES

The main action in 2015 was to produce a White paper on Aviation Security proposing a research programme in this domain. This white paper was presented to the European commission representatives on October 12 (DG HOME and DG MOVE). The meeting was very interesting and showed that security topics are scattered in several different European initiatives. AS-GoR could be a good place to make links between these different initiatives.
The white paper was also distributed to institutions and industrial companies. It raised a lot of interest and allowed to identify interested industrial partners that are potential IPoC for the GoR.

Two GoR meetings also took place in 2015 in February and October.

Four Exploratory Groups are under consideration inside the GoR:

- AS/EG-1 (Cybersecurity): Towards an Information Security Management System for the aviation sector;
- AS/EG-2 (CBE): Enhancing airport security against CBE threats;
- AS/EG-3 (Dazzling): Detection of threatening laser radiation on aircraft or helicopters for future protection of pilots;
- AS/EG-4 (RPAS): Analysis of new threats posed by malevolent use of Unmanned Aerial Systems (UAS) and/or Remote Piloted Aircraft Systems (RPAS). Threat mapping.

The description of these four Exploratory Groups is given below.

AS/EG-1: TOWARDS AN INFORMATION SECURITY MANAGEMENT SYSTEM FOR THE AVIATION SECTOR

Task 1
The ability to assess, manage, reduce, mitigate and accept risk is paramount for an effective protection of the air transport system against cybersecurity threats and incidents. A “cyber resilient” air transport system will therefore require the establishment, adaption and implementation of a standardized aviation Information Security Management System (ISMS). An ISMS can be defined as a systematic approach to managing sensitive information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. GARTEUR could contribute to the definition of (parts of) such an ISMS for the aviation sector, focusing on understanding risk as first step.

Proposed tasks for GARTEUR include:

- Definition of key assets/systems/services in the Air Transport System to protect;
- Identification of vulnerabilities that can be exploited by cyber threats;
- Definition of aviation specific cyber-threat scenario’s;
- Risk assessment: Specification of tools (such as assessment methodology and metrics) to systematically and dynamically assess the impact of threat scenario’s.

Task 2: Research on aeronautical information systems assurance that would contribute to airworthiness certification
Risks are increased by the increased use of internet technologies and COTS systems both ‘on’ and ‘off’ the aircraft. The rule-making and regulatory bodies are struggling to provide the certification criteria, methods and toolsets which will be required to substantiate the airworthiness assurance, i.e. safety, related to the new cyber security dimension. This applies equally to the manufacture, operation and maintenance of the new aircraft and new ATM systems.

Proposed tasks for GARTEUR include:

- Aviation certification authorities will have to deal with cyber-security in the future. System assurance techniques that usually focus on safety need to be extended/changed in order to deal with cyber-threats.

Expected impact/Justification:

- The introduction of new communication methods and technologies in the air transport system also introduces new cyber security vulnerabilities. These vulnerabilities have the potential to jeopardise civil aviation safety and efficiency and therefore need to be identified and addressed.
- Understanding the (cyber) environment the Air Transport System is operating in, the cyber threat and associated risks is a prerequisite for defining procedures and technological measures to prevent, detect and recover from cyber attacks.

AS/EG-2: ENHANCING AIRPORT SECURITY AGAINST CBE THREATS

Description of the task:

- Fast and safe screening of passengers and luggage at a distance by optical methods;
- Integration in existing security and luggage sections.

Expected impact/Justification:

- Protection of citizens in airports and aircrafts from CBE exposures;
- Filling the gap of B detection;
- No additional time delay for passengers due to the additional inspection;
- Maintenance of the integrity for persons and freight;
- Further application of the system at public events.

AS/EG-3: DETECTION OF THREATENING LASER RADIATION ON AIRCRAFT OR HELICOPTERS FOR FUTURE PROTECTION OF PILOTS

Description:

- Comparison of solutions of detection of the threats: detection from the aircraft or detection from the ground → Assessment → Scenarios and technological impact → Perspectives;
- Localisation of the threat.

Expected impact/Justification:

- Detection is the first step for this topic and is required for protection.
- Civil and military interest.
- Perspectives → Proposals for protection.
- No solution at present.

AS/EG-4: ANALYSIS OF NEW THREATS POSED BY MALEVOLENT USE OF UNMANNED AERIAL SYSTEMS (UAS) AND/OR REMOTE PILOTED AIRCRAFT SYSTEMS (RPAS). THREAT MAPPING.

Description:
The research areas under the scope of this topic will mainly cover the scenario analysis. It is intended to map the different occasions, physical layouts and/or opportunities in which this threat may occur. It is intended to:

a. Identify situations, assets or terrorist objectives vulnerable to this threat:
   - General assets: critical infrastructures, power plants, airports, official buildings, industries;
   - Public mass events;
   - VIP events protection;
   - Mobile targets: airplanes, trains, vessels;

b. Identify the possible innovative means for RPAS/UAS guidance and target tracking: automatic optical reconnaissance systems / GPS / ADS-B / acoustic / Electromagnetic signal recognisers / etc…
c. RPAS high-jacking. Dealing with the very specific topics of GPS jamming and spoofing, D/L security and RPS security. This is related to cybersecurity.

Expected impact/Justification:

- The potential for increasing the authorities' awareness and preparedness to face this new issue, bringing together mutual benefit across industry, academia and end users.
- The value for a future system prototype/ industrial development in terms of product implementation after the project and participation of SMEs.
- The promotion of standardization (hybrid or not) and interoperability features, through the contribution of standardization bodies.
- The capacity to increase social acceptance of the use of RPAS. The proposal will address the Safety of Life of citizens, and will have a positive impact on the perception of threats and the measures taken to address them by authorities.
- The development of solutions at different levels:
    - At technology level, by covering previous technologies for detection and threat assessment and new countermeasures techniques;
    - Operational and procedural level;
    - Potential for policy and standards' recommendations.

Ethical issues arising from the misuse of the developed research should be considered related to its malevolent use with unlawful purposes by criminals and/or for privacy interventions.
End users of the results would be law enforcement authorities and private sector able in prototyping such a pre-commercial systems.

6 years rolling Plan for AS/EGs

No	Theme	Topic	2012	2013	2014	2015	2016	2017
AS/EG-1	Cybersecurity	- Towards an Information Security Management System for the aviation sector						
AS/EG-2	CBE	- Enhancing airport security against CBE threat						
AS/EG-3	Dazzling	- Detection of threatening laser radiation on aircraft or helicopters for future protection of pilots						
AS/EG-4	Malevolent use of RPAS	- Analysis of new threats posed by malevolent use of Unmanned Aerial Systems (UAS) and/or Remote Piloted Aircraft Systems (RPAS) - Threat mapping						

FUTURE PLANS

A first objective in 2016 is to include industrial partners in the GoR. This addition should help the GoR focus on specific research themes and propose consortia for collaborative research projects.

In 2016 the first meeting will take place in January. The second meeting involving industrial partners will take place in April.

Virginie Wiels
Chairman (2014-2016)
Group of Responsables Aviation Security

GOR MEMBERSHIP

Chairman			
Ms. Virginie Wiels	ONERA	France	Virginie.Wiels@onera.fr
Vice-Chairman			
Mr. Ingmar Ehrenpfordt	DLR	Germany	Ingmar.Ehrenpfordt@dlr.de
Members			
Mr. Bernd Eberle	Fraunhofer	Germany	Bernd.Eberle@iosb.fraunhofer.de
Mr. Anders Eriksson	FOI	Sweden	e.Anders.Eriksson@foi.se
Mr. Francisco Munoz Sanz	INTA	Spain	mugnozsf@inta.es
Ms. Angela Vozella	CIRA	Italy	A.Vozella@cira.it
Mr. René Wiegers	NLR	Netherlands	Rene.Wiegers@nlr.nl