TNO innovation for life

TNO report

TNO 2015 R11721 | Final report

Technical Aspects Concerning the Safe and Secure Use of Drones

Date	March 2016
Author(s)	P.J.M. Elands, J.K. de Kraker, J. Laarakkers, J.G.E. Olk, J.J. Schonagen
Copy no	
No. of copies	
Number of pages	101 (incl. appendices)
Number of appendices	
Sponsor	
Project name	Verkenning technische maatregelen drones
Project number	060.18762

Summary

On request of the Dutch National Coordinator for Security and Counterterrorism (NCTV) of the Ministry of Security and Justice, TNO has investigated the issues and corresponding risks which arise from the introduction and use of drones in the national airspace.

The issues identified are primarily related to safety and security and to the corresponding regulatory framework and law enforcement. A number of interviews was held with relevant stakeholders, addressing their specific issues. The issues were translated to specific risks, which have been listed and categorized in the table below.

#	Description of risks	Type of risk
1	Damage to other aircraft or other colliding objects	Safety
2	Damage to people and property on the ground	Safety
3	Damage to (critical infrastructure)	Safety
4	Consequential and/or reputation damage	Economic
5	Prevent other aircraft from flying	Safety
6	Loss of drone	Economic
7	Loss of information stored in the drone	Security
8	Privacy infringement	Privacy
9	Economic damage	Economic
10	Security breach	Security
11	Terrorist attack	Security
12	Panic/disturbance of people on the ground	Security
13	Crime	Security
14	Annoyance (noise)	Environment
15	Environmental pollution and global warming	Environment
16	EM spectrum congestion	Environment

Risks identified with respect to the safe and secure use of drones in the national airspace.

For most of these risks, a quantitative assessment is not available, neither on the probability of occurrence nor on the impact. This makes a discussion about risks and risk assessment only possible in a qualitative way. To allow a proper evaluation of risks, risk acceptance levels should be defined by the government.

The approach of Networked Risk Management (NRM) is suggested for an issue as complex as the safe and secure use of drones in the national airspace, because traditional risk management techniques often become too complex and do not take into account all relevant relations.

Based on these issues and risks, we have identified a number of measures, most of them of a technical nature, which can be applied to decrease the risks associated and hence to take care of some of the issues identified. We have made a shortlist of technical measures which can be taken quickly and easily. Three very relevant technical measures we have discussed in more detail. Many of the measures

described, are presently being studied or installed, somewhere in the world. The introduction of drones into the airspace is worked at simultaneously in many places around the world.

In the table below, the technical measures proposed have been listed, sorted in order of feasibility; the 'quick and easy' measures form the top of the list. The assessment of feasibility is of a qualitative nature and comprises cost, technological complexity, time to implement and expected resistance.

Technical Measure	Cost of Technical Measure	Technological complexity	Time to implement	Expected Resistance
Observability	1	1	1	1
Airspace division	1	1	1	1
Establishing No-fly zones	1	1	1	1
Propellors	1	1	1	1
Pricing of safety measures	2	1	1	1
Limiting technical capabilities of drones	1	1	1	3
Apps for sharing flight information and practice	2	1	2	1
Enforcing No-fly zones	1	2	2	1
Communications link	2	2	1	1
Information downlink	2	2	1	1
Pilot's licence	2	1	1	2
Education and PR	2	1	2	1
Reporting incidents	1	1	1	3
Rewarding good behavior/perks	1	1	2	2
Collision avoidance	2	2	2	1
Transponders	2	2	2	1
Flight planning & approval	2	1	1	3
Noise reduction	2	2	2	1
Registration & Identification	2	2	2	2
Beacons to establish no-fly zones	2	2	2	2
Impact limiting devices	2	2	2	2
Drone circuits	2	1	3	2
Telecom networks to track drones	2	2	3	2
Safety requirements	1	2	2	2
Detection/tracking/logging	3	3	3	1
Air traffic management systems	3	3	3	1
Pollution reduction	2	3	3	2
Kill switch	3	2	3	3

Longlist of technical measures to enhance the safe and secure use of drones ranked according to a qualitative assessment of feasibility.

Law enforcement with respect to drones is a challenge, also with respect to avoiding collateral damage. In the report we address the various technical measures which may contribute to law enforcement.

The cybersecurity of drones being used as a CCTV camera has been looked at in some more detail. Vulnerabilities and technical measures to overcome these vulnerabilities have been identified.

We have the following recommendations:
- the execution of proper risk assessments, for all relevant risks identified;
- the definition of quantitative risk acceptance levels by the authorities;
- assessment and implementation of the technical measures identified, preferably in a European context;
- an initiating and guiding role by the national and international authorities to stimulate industry and standardization bodies to define standards for the safe and secure use of drones;
- a stimulating and guiding role by the national and regional authorities to conceive one or more test and experimenting facilities, where drones can be developed and tested in a secure and controlled part of airspace, without the need to comply to rules and legislation;
- continuation of the approach taken by the government to develop legislation and to stimulate standardization in a European context.

Developments in technology and application in the area of drones are evolving very rapidly. For this reason, the results of this study should be reviewed critically and updated at least within one year.

Contents

Appendices
A Interviews
B Slides per Issue
C Slides per Technical Measure

D Slides per Risk

1   Abbreviations

ADS-B	Automatic Dependent Surveillance-Broadcast
AT	Agentschap Telecom
BLOS	Beyond Line of Sight
BVLOS	Beyond Visual Line of Sight
CCTV	Closed Circuit Television
CNPC	Command and Non Payload Communication
CNS	Communication, Navigation, Surveillance
CRC	Cyclic Redundancy Check
DARPAS	Dutch Association of Remotely Piloted Aerial Systems
DSSS	Direct-Sequence Spread Spectrum
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HEMS	Helicopter Emergency Medical Services
ICS	Industrial Control Systems
IP	Internet Protocol
ISM	Industrial, Scientific, Medical
LATAS	Low Altitude Traffic and Airspace Safety
LED	Light Emitting Diode
LOS	Line of Sight
MIT	Massachusetts Institute of Technology
MLA	Military Aviation Authority ('Militaire Luchtvaartautoriteit')
MOD	Ministry of Defence
NAA	National Aviation Authority
NASA	National Aeronautics and Space Administration
NCAP	New Car Assessment Programme
NCSC	National Cyber Security Center
NCTV	National Coordinator for Security and Counterterrorism
NFI	Netherlands Forensics Institute
NFP	National Frequency Plan
NGO	Non-Governmental Organization
NLR	National Aerospace Laboratory
NOTAM	Notice to Airmen
NRM	Networked Risk Management
QE	Qualified Entity
RAVT	RPAS Autopilot Validation Tool
R&D	Research and Development
RFID	Radio Frequency Identification
RPAS	Remotely Piloted Aerial System
SAA	Sense and Avoid
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SME	Small and Medium Enterprise
SORA	Specific Operation Risk Assessment
TNO	Organization for Applied Scientific Research
TRL	Technology Readiness Level
UAS	Unmanned Aerial System

UAV	Unmanned Aerial Vehicle
UTM	UAS Traffic Management System
UVS	Unmanned Vehicle Systems
VLOS	Visual Line of Sight
VIN	Vehicle Identification Number
VNV	Vereniging van Nederlandse Verkeersvliegers
VSS	Video Surveillance System
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

2 Introduction

2.1 Request

The Dutch National Coordinator for Security and Counterterrorism (NCTV) of the Ministry of Security and Justice has issued a request for innovation within the framework of the Research Program on Public Safety and Societal Security carried out at TNO. The request concerns exploratory research into technical standards, fail-safes, and cybersecurity aspects related to drones.

This request originates from the intention of the Dutch government [1], expressed in writing to parliament (March 2, 2015), to stimulate the professional use of drones for economic benefit, to enable the use of drones by police and fire brigades and to also allow for the use of drones for recreation purposes. Specific attention is given to the risks in the area of security and safety.

The safety and security of the use of drones is influenced by the quality of the system: the drone, the control station, the required frequencies and the quality of the connection. It concerns the quality of hard- and software, the ability to land safely in case of emergency ('fail-safes'), the dependency on positioning systems and the security of the link between operator and drone. An explicit item of attention is cybersecurity[1], such as possibilities to intercept information or to manipulate or disrupt the control of the drone. An assessment of future risks and possibilities for cybersecurity by design shall be taken into account.

2.2 Implementation of the Innovation Request

The innovation request clearly has a match with the goals of the Research Program on Public Safety and Societal Security. The program manager has requested a two-way approach:

- assessment of the issues concerning the use of drones, both with respect to the airspace as to the situation on the ground;
- assessment of the vulnerability of drones with respect to jamming/hacking/spoofing of the control link as well as the data link for surveillance activities of public safety and security organizations. Cybersecurity of surveillance cameras in general (such as CCTVs), is included in the work, because there are no fundamental differences.

After a discussion with the NCTV it was decided to not only carry out an inventory of safety and security aspects (issues) concerning drones, but to also conceive/propose a number of technical measures which directly contribute to enhance the safety and security of the use of drones. In addition, the NCTV has asked TNO to interview a number of relevant stakeholders, to collect relevant safety and security issues and to discuss the relevance of possible measures.

---

[1] A distinction can be made between interfering with the electromagnetic spectrum (electronic warfare) and interfering with the digital information in the drone.

Policy measures and legal measures are out of scope of this study; our focus lies on the technical measures. If specific non-technical measures require support through some form of technology, this will be addressed too.

2.3 Developments

The use of (small) drones has increased tremendously. The ample availability of affordable small drones, equipped with a camera and very easy to use, has led to large amounts of drones being sold. Late 2015, at the holiday season, drone sales peaked. Companies like DJI, Parrot and 3D Robotics, the major sellers on the consumer market, innovate their products very rapidly, making them increasingly easy to use.

The availability of these drones has been made possible by a number of technology developments, having taken place the last years, in the area of materials, propulsion, sensors, computers, et cetera. Like in smartphones, the combination of these technologies allows for completely new functionalities.

In [2] an overview picture was given of a number of technology developments and their interaction, allowing for the quick developments in the capabilities of small drones, see Figure *2.1*.
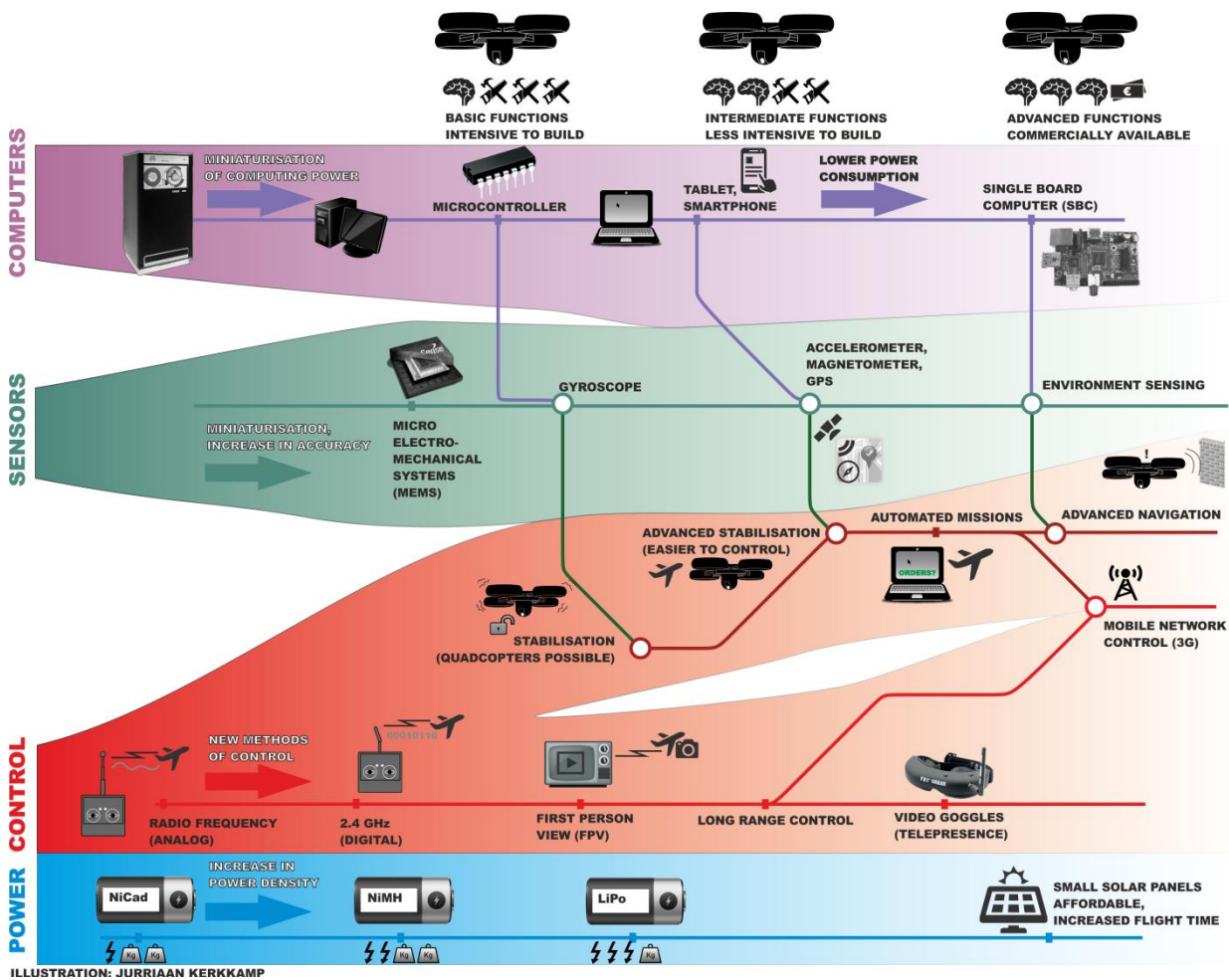

Figure 2.1   Synergy among technology developments related to drones.

This rapid increase of the number of drones entering the national airspace has led to sincere concerns about safety and security; more and more incidents occur and it seems only a matter of time before a serious accident takes place.
Not only the government is concerned about safety and security, but also the traditional users of the national airspace, who experience many new aircraft and other flying objects entering the airspace, without the traditional safety measures and procedures being followed.

This concern has led to many different initiatives and studies to enhance the safe and secure use of drones. Almost on a daily basis new reports and findings are published and measures are proposed to be implemented.

2.4   Government Position

In the Netherlands, the government wants to stimulate the economic benefits made possible by the professional use of drones. Nowadays, many different kinds of new services are being developed using drones, for instance services allowing for faster and more precise inspections of buildings and infrastructure. These developments are encouraged by the government, as long as the safety and security of drone flights is taken care of.

With respect to the recreational use of drones, the government does not want to take measures which make the use of drones completely impossible, but it is imperative that safety and security are well taken care of (safety first!).

With respect to the use of drones, different government entities are involved. The use of airspace is governed by the Ministry of Infrastructure and Environment, the use of radio frequencies is controlled by the Agentschap Telecom, part of the Ministry of Economic Affairs, the concern for safety and security in general is governed by the Ministry of Security and Justice and the stimulation of economic development is the job of the Ministry of Economic Affairs. In addition, the Ministry of Defence is an important user of the national airspace, both with manned aircraft and unmanned aircraft (drones). Between these different government entities frequent discussion is taking place; coordination is in the hands of the Ministry of Security and Justice. For (commercial) users of drones however, it is sometimes difficult to know which government entity to go to.

Requested by parliament, the Minister of Security and Justice has asked end 2014 the Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) of his own ministry, to carry out a study [4] into the use of drones. The report primarily addresses the legal framework and the privacy issues concerned with the use of drones and provides excellent guidance for policy measures and regulation in these matters. Other safety and security aspects were not addressed in great detail.

In 2015 the government has issued some new rules and legislation [3] [26] [27] [28] [29] [30] to deal with the situation in the Netherlands in the area of drones. For the future, the government has chosen to follow European developments in legislation. In the first half year of 2016, the Netherlands will act as chairman of the EU, and is willing to make significant progress on this topic. We support this international

approach, because it will create clarity and equality in the rules all over Europe and it will facilitate international standardization.

All the measures, regulations and legislation which have been and will be put in place, need to be enforced by the authorities. A necessary aspect of conceiving new measures and regulations is law enforcement; this has to be taken into account in an early stage of the development of new approaches, in order to avoid the conception of measures and regulations which cannot be enforced.

2.5 National Setting

In the Netherlands, various entities are involved in the design, development, conception and use of drones.

A number of SME's (such as Aerialtronics and Delft Dynamics) is involved in the design, development, construction and sales of drones, both for the recreational market as well as for the professional market.

Many SME's offer services using drones, for inspections and aerial photography of buildings, infrastructure and crops, for aerial surveillance et cetera. The number of services offered making use of drones increases rapidly.

Professional users of drones and drone manufactures have joined forces in the Dutch Association of Remotely Piloted Aerial Systems (DARPAS).

From a government point of view, primarily the Ministry of Defence is using drones in the national airspace. At present the Raven Mini-UAS and the ScanEagle Tactical UAS are in service. The use of these aircraft in the national airspace is carried out only on specific request of for instance the National Police. Both the National Police and the Fire Brigade are working on a capability to fly drones for their own purposes. The National Police is training and educating operators to fly drones for a number of specific tasks. The Fire Brigades of regions Twente and Midden-West Brabant are actively pursuing a capability to fly drones on behalf of all other regions. The Fire Brigade in general has received permission to fly drones for special purposes (incidents) under strict conditions.

At Delft University of Technology and University of Twente research is being carried on drones. The Faculty of Aerospace Engineering of Delft University of Technology has created a Micro Air Vehicle Laboratory, where very small drones are being studied. Both the National Aerospace Laboratory (NLR) and TNO are involved in studies concerning the use of drones. NLR focuses on the safe introduction of drones in the national airspace, TNO focuses on safety for the environment on the ground, on security issues and on techniques to counter unwanted drones. In addition, TNO leads a four-year research programme for the Ministry of Defence to assess the impact of the introduction of unmanned systems in the NLMOD, taking care of many different aspects. In this programme for instance, new developments like increased levels of autonomy and swarms of drones are being studied and developed.

A number of initiatives has been taken, to establish a national or regional test and evaluation facility for drones. It seems logical to have a facility and a specific part of airspace, where it is possible to test and experiment with drones, outside the boundary conditions of present rules and legislation, for instance to investigate specific risks and to develop new technologies, but also for law enforcement authorities to practice flying drones and to practice counter-UAV operations.

2.6 International Setting

As mentioned earlier, the Dutch government wants to contribute to and adhere to the European developments with respects to the conception of rules and legislation for drones. An important initiative is the action taken by the EASA to conceive European guidelines and rules for drones.

Very recently, the EASA has issued a so-called Technical Opinion [31], in which updated technical proposals for a regulatory framework and for low-risk operations of all unmanned aircraft are presented. This regulatory framework is operation centric, proportionate, risk- and performance-based, and established three different categories for unmanned systems.

The Technical Opinion does not introduce new regulations, but shows the way the earlier proposed regulations could be implemented. A roadmap for future implementation is added.

Another important player in the international setting is UVS International, the international association of different national associations of unmanned systems, representing the users of unmanned systems.

The issues, risks and technical measures addressed in this report, have been assessed against the international developments in this area.

3 Issues and Associated Risks

3.1 Introduction

For this study, we define issues as those topics, people discuss about and consider as a possible threat, et cetera, when it comes to the safe and secure use of drones in the national airspace. From the interviews in the previous chapter, from contacts with other players in the area of drones and from the literature, we have identified the most relevant issues. In this chapter, we will derive the associated risks for each of the issues identified.

Again it is emphasized that some issues may represent a significant risk, whereas other issues may only represent a minor risk or no risk whatsoever. As long as no quantitative risk analysis has been carried out, this remains an unsolved topic.

It is not the intention to have a thorough and complete description of each issue, we will provide a general description providing the reader a good understanding of what the issue is about and which risks are involved.

In Paragraph 3.2 an overview of all issues found is given, while in Paragraph 3.3 a summary of all relevant risks is given. In Chapter 4 risks and risk management are discussed in more detail.

Part of the inventory of issues consisted of having interviews with relevant stakeholders. In Appendix A the results of these interviews are given, together with an appreciation.

In Appendix B for each of the issues identified, a specific slide is presented, summarizing the issue, providing the associated risks and mentioning the stakeholders involved.

3.2 Overview of Issues

3.2.1 List of issues

In the table below the complete list of issues is given. In the subsequent sections, each issue is explained in some detail and the associated risks are added. The issues have not been categorized.

#	Description of issue
1	Airspace safety
2	Safety on the ground
3	Airworthiness
4	Evolving capabilities
5	Unpredictable behavior
6	Privacy infringement
7	Espionage using drones
8	Vulnerability to jamming, spoofing, hacking, eavesdropping

9	Frequency spectrum
10	Loss of link
11	Legislation
12	Communication
13	Unlawful use
14	Law enforcement
15	Annoyance
16	Environment
17	Liability/insurance
18	Airspace and practice areas
19	Dynamics in developments

Table 3.1   List of issues

3.2.2 *Airspace safety*

The safety of the airspace is a serious concern. Traditionally, the airspace is a very well regulated and relatively safe area. The availability of drones makes it possible for every person without any knowledge of safe flying to enter the airspace and create a hazardous situation.

A drone may collide with static objects and with other flying objects. Examples of static objects include buildings and powerlines, examples of flying objects include other drones and manned aircraft.

Especially when drone pilots fly in areas where it is not allowed, such as the vicinity of airports, significant risk of collision may occur. The community of professional aviators is very concerned about the threat of collisions between drones and manned aircraft [9] [10] and [14]; many incidents have already occurred. Particular worries concern the impact of a drone on the windshield of a rotorcraft or an aircraft, the impact of a drone on the main- or tail rotor of a rotorcraft and the ingestion of a drone in the engine of a turbojet aircraft.

It is noted that no good data are available nor about the probability of an accident neither about the impact of an accident. Some qualitative, merely theoretical studies have been published [8], [11], [12] and [13], mostly comparing the possible consequences of drone impact to the well-known consequences of bird impact. The conclusions of those studies differ considerably, however, both on assessment of probability and of impact.

In a recent publication [22], a large number (241) of incidents (close encounters) has been studied. It shows that most incidents occurred near airports and involve multi-rotor drones. Almost all incidents occurred above 400 feet (133 m).

The presence of illegal drones in the airspace has the additional consequence that regular users of the airspace, such as Helicopter Emergency Medical Services (HEMS) or fire extinguishing aircraft are not able to fly.

The effect of weather conditions on airspace safety is considerable. Drones have a limited ability to deal with adverse weather conditions like heavy winds, rain and other forms of precipitation. Professional drone pilots have been taught to take weather conditions into account and refrain from flying if it is considered unsafe.

Recreational flyers might not fully be aware of the possible consequences of flying in bad weather or with strong winds.

There is considerable effort going on to conceive methods, technology and regulations to increase airspace safety. These, however, are not addressed in this paragraph.

The risks associated with this issue are:
- damage to other aircraft or other colliding objects;
- damage to people and property on the ground;
- damage to (critical) infrastructure;
- consequential and/or reputation damage;
- prevent other aircraft from flying.

3.2.3   *Safety on the ground*

Drones and especially multi-rotor drones (quad-, hexa- or octocopters) crash easily; their current track record in reliability is still relatively poor. Crashes may be due to pilot error or to technical malfunction, such as a poor battery. In addition to crashes, drones used in close proximity to people may also cause accidents and injuries, or the presence of drones may distract people, resulting in an accident (without being hit by the drone). Recently, some cases of injuries to persons were reported, caused by drones hitting persons.

The effect of weather on drones, as mentioned in the previous section, is applicable to safety on the ground as well.

A drone that crashes or hits people or objects in flight may cause physical damage to persons and to property (buildings, cars, infrastructure). The impact of the drone may cause damage due to its kinetic energy and momentum, but also the propellers may cause significant damage, especially to persons. There is an additional risk of causing fire, due to a crashing drone. Furthermore, secondary damage may occur, such as consequential damage (such as stagnation of production processes) and reputational damage.

In principle, the damage caused by a drone that crashes or hits a person or object is covered by insurance, if the user is properly insured.

TNO has conceived a method for risk assessment [7] for crashing drones for the Military Aviation Authority, which can be used to quantify the risks.

The risks associated with this issue are:
- damage to people and property on the ground;
- damage to (critical) infrastructure;
- consequential and/or reputation damage;
- prevent other aircraft from flying;
- loss of drone;
- loss of information stored in the drone;
- panic/disturbance of people on the ground.

3.2.4   *Airworthiness*

In aviation the airworthiness of aircraft is defined by law and regulations. Aircraft to be allowed in the national airspace should adhere to airworthiness requirements. If they do so, they receive an airworthiness certification. In addition, in case of professional use, drone pilots need to get certified, in order to be allowed to fly drones.

The issue concerning airworthiness is that the rules applying to larger manned aircraft often are not very suitable for small unmanned aircraft. In addition, in some cases, quantitative requirements do not exist yet. This makes it difficult for manufacturers to get their drones certified. In the EASA Technical Opinion [31], it is proposed that the rules are adapted to accommodate the specifics of unmanned aircraft.

The risks associated with this issue are:
- damage to other aircraft or other colliding objects;
- damage to people and property on the ground;
- damage to (critical) infrastructure;
- consequential and/or reputation damage;
- prevent other aircraft from flying;
- loss of drone;
- loss of information stored in the drone;
- panic/disturbance of people on the ground.

3.2.5   *Evolving capabilities of drones*

The capabilities of drones are evolving very rapidly, not only in terms of performance (velocity, acceleration, endurance), but also in terms of size, weight and power requirements of their payloads. This rapid development in technology might overtake measures and regulations taken for reasons of safety and security. Regulations could become outdated.

Due to the generic character of this issue, all possible risks may be associated with this issue.

3.2.6   *Unpredictable behavior*

Currently, drones are flown using a remote control. It is expected that in the future, drones more and more will fly by themselves, autonomously. Some types of drones already automatically follow their pilot, following a WiFi or Bluetooth signal, or using their camera to track him. Other current examples of autonomous flight are flying from waypoint to waypoint and failsafes in case of loss of link.

The risk concerned with autonomous flight concerns possible unpredictable behavior, in a situation they have not been programmed for. Such unpredictable behavior could lead to potentially dangerous situations, both in the air and on the ground. This risk may increase if drones operate as a swarm, due to cascading effects.

The risks associated with this issue are comparable to those for airworthiness:
- damage to other aircraft or other colliding objects;

- damage to people and property on the ground;
- damage to (critical) infrastructure;
- consequential and/or reputation damage;
- prevent other aircraft from flying;
- loss of drone;
- loss of information stored in the drone;
- panic/disturbance of people on the ground.

3.2.7 Privacy infringement

The issue of privacy is generally considered to be quite important. Most drones are equipped with a camera and hence are able to make video recordings of persons, also in private settings. In addition, people often will not be aware that they are being filmed, which makes the privacy infringement worse. In case people do notice that they are being filmed, they often do not have an idea who is flying the drone and they do not have any means to stop the drone from filming.

In the WODC report [4] the issue of privacy has been discussed extensively. It is concluded that privacy is addressed sufficiently in present legislation. However, it was also concluded that a privacy impact assessment is required if new policy on the government use of drones is to be conceived.

Privacy issues related to the use of drones by professional users or by recreational users are in principle covered by existing privacy laws. It is expected that professional users will be quite careful in complying with the rules, while recreational users will not, not in the least because they do not known the rules.

Privacy infringement may be the explicit and lawful purpose of specific types of users, such as law enforcement agencies, to identify persons by means of drones equipped with a camera.

Recently, the Ministry of Security and Justice has issued a Letter to Parliament [5] together with a manual [6] how to use drones in relation to privacy. This manual provides a specific interpretation of the possible infringements of privacy laws and regulations when using drones. The interpretation that the possibility of identification of persons being filmed[2] is considered as an infringement of privacy laws is important. This means that drone users have to take explicit measures to prevent such an infringement.

The risk associated with this issue is:
- privacy infringement.

3.2.8 Espionage using drones

Drones may be criminally used to collect proprietary or secret information from companies or government entities (espionage). It is relatively easy to gather information by flying over the fences and enter the premises of companies or government agencies and steal valuable information, while the risk of detection is relatively low, if no specific measures to do so are taken. Should the drone be

---

[2] Except of course lawful privacy infringement

detected and possibly intercepted, the drone pilot may still be a safe distance and may get away undiscovered. The criminal (unlawful) use of drones as such is addressed in Section 3.2.14, but the vulnerability of companies and government agencies to theft of information due to forbidden observation from the air, is considered by us as a separate issue.

The risks associated with this issue are:
-    economic damage;
-    security breach.

3.2.9   *Vulnerability to jamming, spoofing, hacking and eavesdropping*
Sometimes this issue is referred to as cybersecurity; it must be noted however, that a distinction needs te be made between use of the electromagnetic spectrum, also referred to as Electronic Warfare, and changing the information in a system by changing the bits and bytes. The distinction however, is not a very sharp one.

The drone is controlled through a radio signal from the ground control system. This signal could be jammed, leading to the loss of control. In that case, the drone can be programmed to proceed according to a loss of link procedure (failsafe mode), see Section 3.2.11.

Jamming
A drone which use GPS, or another global positioning system, could be attacked by jamming the GPS signal, making it unable for the drone to fix its position. The action the drone will take (supposed it notices it is being jammed), depends on the specific type of drone.

Spoofing
The GPS signal can also be spoofed, which means that another GPS-like signal is sent to the drone, which is more powerful than the original GPS signal coming from the satellite, providing a different location to the drone, in order to mislead it.

The command signal may also be spoofed, for instance by a replay attack. This means that the original signal from the pilot to the drone is recorded by the attacker and then sent again to the drone by the attacker to mislead it.

Hacking
Hacking means that the attacker is able to enter the system (drone and/or ground control system) and give direct commands to the drone. This is also referred to as cybersecurity.

Eavesdropping
Eavesdropping merely relates to the signals coming from the sensor(s) of the drone, such as the video signal coming from the camera of the drone. People who are interested in this signal could intercept it and watch what the drone is filming.

The vulnerabilities mentioned here may lead to the loss or theft of the drone, to unsafe or worse events in the airspace and on the ground due to loss of control by the pilot and to theft of information.

These vulnerabilities can be mitigated by hardware and software protection measures, such as encryption and advanced forms of transmission of radio signals.

For the NL MOD TNO has investigated the vulnerability of various unmanned platforms to jamming and spoofing.

The risks associated with this issue are:
- damage to other aircraft or other colliding objects;
- damage to people and property on the ground;
- damage to (critical) infrastructure;
- consequential and/or reputation damage;
- prevent other aircraft from flying;
- loss of drone;
- loss of information stored in the drone;
- privacy infringement;
- economic damage;
- security breach;
- panic/disturbance of people on the ground.

3.2.10   *Frequency spectrum*
The foreseen increase of drones in the national airspace may lead to congestion in the frequency bands used for command and control to and from drones and for data transport of the sensor data, generated by drones. Should drones be equipped with a transponder (such as ADS-B), this also increases the risk of frequency bandwidth saturation. Such effects may lead to loss of link and hence loss of control or to mid-air collisions because the transponder signals were not picked up. Congestion in the frequency of the downlink of data may lead to the loss of the mission, because the drone is not able to provide the necessary information to its user.

Agentschap Telecom, Appendix A, explicitly warned for possible congestion of the frequency spectrum. The agency recently has designated a specific part of the spectrum for certain types of drones and is studying future use.

The risks associated with this issue are:
- damage to other aircraft or other colliding objects;
- damage to people and property on the ground;
- damage to (critical) infrastructure;
- consequential and/or reputation damage;
- prevent other aircraft from flying;
- EM spectrum congestion.

3.2.11   *Loss of link*
If the control link between the drone and the ground control station fails, the drone becomes uncontrolled. The drone may enter a failsafe mode, e.g. it may enter the return to home failsafe mode and automatically return to its starting point. Other failsafe modes are to land immediately or to go to a specific altitude and stay there and hover, waiting for reconnection of the link.

Loss of link may be induced by a technical failure, by obstacles between the drone and the operator or by attack in the form of jamming, spoofing or hacking. In case of non-visual-line-of-sight (N-VLOS) operations, some form of relay of the signal is used, which again may cause in loss of links if it fails.

The risk of loss of link is that the aircraft in a failsafe mode, collides with other aircraft or objects. If the home location is not well defined, a fly away is likely, resulting in the loss of the aircraft.

The risks associated with this issue are:
- damage to other aircraft or other colliding objects;
- damage to people and property on the ground;
- damage to (critical) infrastructure;
- consequential and/or reputation damage;
- prevent other aircraft from flying;
- loss of drone;
- loss of information stored in the drone;
- panic/disturbance of people on the ground.

3.2.12 *Legislation*
Drone technology is emerging and developing at a very rapid pace. Legislation almost by definition is lagging behind and has difficulties to catch up.

In addition, legislation is experienced as complex and bureaucratic. Professional users complain that getting permission to fly drones is quite cumbersome and time consuming. This could lead to flying without permission, which is a risk of course.

In the Netherlands new regulations have been issued as of July 1st 2015 [3]. These measures are considered to be temporary measures. Much effort is going on in Europe to harmonize the various national laws and regulations into a single European system of rules and regulations [16], [17], [18], [31] and [32].

A specific issue is that although the government is making good progress in conceiving national and international legislation and regulation concerning drones, these efforts are merely based on qualitative risk perceptions instead of quantitative risk assessments. This could lead to risks being underestimated and risks being overestimated. In more mature areas, such as the automotive area, specific measures and corresponding certifications are based on quantitative facts. An additional benefit of quantitative risk assessment is the fact that the government must set an acceptable level of risk, which then again serves as input for drone manufacturers in terms of reliability and crashworthiness of their drones.

An actual issue in the legislation is the registration of drones, to enable the tracking and tracing of their owner. If such a measure be issued, retrofitting to legacy systems will certainly be an issue, and mutatis mutandis also for other technical measures to be taken.

It is not possible to explicitly couple risks to this issue; risks appear only in an indirect manner from this issue.

3.2.13   Communication

Closely linked to legislation is the subject of communication. Not many people are aware of current regulations and legislation, leading to ample unintentional unlawful use and other mishaps (fly aways) with drones. Most people want to obey the law, but if they do not know it, they might easily break it.

For this reason, it is deemed necessary to inform the public through campaigns, websites, commercials and flyers added to the drone about the dos and don'ts of flying drones. Recently, the government has launched a campaign (illustration to the right) (www.rijksoverheid.nl/drones) to communicate the rules concerning drones to the public, equivalent to the 'Know Before You Fly' (www.knowbeforeyoufly.org) campaign in the US.

It is not possible to explicitly couple risks to this issue; risks appear only in an indirect manner from this issue.

3.2.14   Unlawful use

The unlawful use of drones can be split into four different categories:
- unintended violation of no-fly zones or other illegal (reckless) actions by recreational drone pilots not aware of the rules or not in control of their drones;
- recreational or professional drone users, knowingly breaking the rules for the thrill, for the professional benefit ('paparazzi') or the attention (NGO's protesting, disturbance of public events);
- criminal use of drones, such as delivery of packages into jails, smuggling or using drones for reconnaissance or theft of information (espionage);
- use by terrorists to cause panic or inflict damage.

The latter case is the most serious one, since at this point in time it is quite difficult to detect, classify and identify a drone let alone determine its intention. Drones could be used to deliver an (improvised) weapon to target a large audience or a VIP, or just be used to cause panic.

Recently, a number of incidents has occurred related to unlawful use of drones. Many authorities in many countries consider this as a high-priority topic. Industry has conceived a number of solutions to counter unlawful UAV's, although it is commonly believed there exists no one single solution, no silver bullet. Traditional security measures, like checkpoints and body searches, of course have no effect, so new measures must be thought of. Recently, the Ministry of Security and Justice
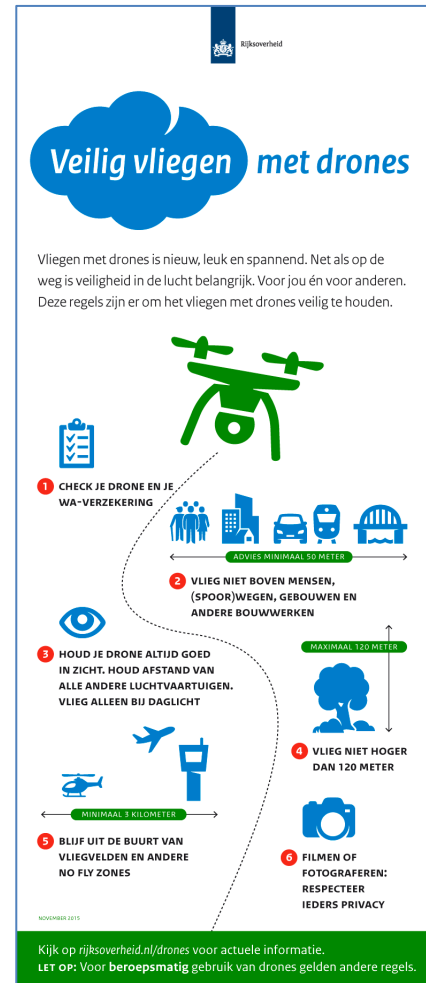
has informed the Parliament on its course of action against unlawful use of drones [5].

The risks associated with this issue are:
- damage to other aircraft or other colliding objects;
- damage to people and property on the ground;
- damage to (critical) infrastructure;
- consequential and/or reputation damage;
- prevent other aircraft from flying;
- privacy infringement;
- economic damage;
- security breach;
- terrorist attack;
- panic/disturbance of people on the ground;
- crime.

3.2.15   *Law enforcement*
This issue strongly relates to the previous issues. Law enforcement authorities should be able to enforce the law. They should check regularly whether drones are certified, whether drone pilots have their licenses et cetera.

In case of intentional or unintentional unlawful flight of drones, law enforcement authorities need to be able to take action, if necessary. They face some significant challenges, however. First, it is quite difficult to detect a drone, to know that a drone is flying in an area where it should not. The second challenge is to classify and identify the drone (and its pilot) and to find out what it is about, what its/his intentions are. In case it is necessary to take action, it is important to get control of the drone, without causing relevant collateral damage and/or risks. Using hard-kill methods like shooting or firing a laser, could cause the drone to crash in an undesirable area, for instance in a crowd of people. Soft-kill methods to gain control over the drone are preferable, if applicable, otherwise it is preferred to highjack the drone, for instance by using a net. In practice however, there might not be enough time to apply such methods and direct strike remains as the only option. In general, the countering of drones requires a flexible approach, in which the reaction is based on the type of threat, the specific situation in which it is used and the imminence of the threat.

In case a drone has been seized, it is important for law enforcement authorities to be able to track the owner, for instance through a registration number or through the flight history, registered by an airspace management system.

The risks associated with this issue are:
- damage to other aircraft or other colliding objects;
- damage to people and property on the ground;
- damage to (critical) infrastructure;
- consequential and/or reputation damage;
- prevent other aircraft from flying;
- loss of drone;
- loss of information stored in the drone;
- panic/disturbance of people on the ground.

3.2.16 *Annoyance*

Drones generate a noise – drone is an English verb meaning 'making a buzzing sound'- which can be considered by people as a nuisance. Especially rotorcraft drones make relatively much noise.

This sound made by drones may cause people to develop a negative attitude towards drones, which again may result in people trying to seize or shoot at drones. If people, get distracted as a result of being annoyed, they might cause an accident.

The risks associated with this issue are:
- consequential and/or reputation damage;
- annoyance (noise).

3.2.17 *Environment*

Drones contribute to the environment to the extent that they consume energy and cause pollution. Especially rotorcraft drones are not very fuel-efficient compared to fixed-wing drones. Drones powered by batteries only generate pollution if the energy was conceived using fossil fuels. Batteries, however, have a limited lifetime and generate chemical waste.

The risk associated with this issue is:
- environmental pollution and global warming.

3.2.18 *Liability and insurance*

Drone pilots are responsible for flying their drones and the consequences in case this leads to damage. For recreational users this is, under normal circumstances, covered by their liability insurance. Professional users usually have a specific insurance covering their drone activities.

Insurance companies are starting to look into more detail in drones; they recognize the potentially huge increase in the use of drones and the risks associated with it [15]. It is anticipated that insurance companies more and more will be leading in the definition of safety and security measures. UVS International strongly believes that in the near future insurance companies will dictate the rules of drone flying.

The risks associated with this issue are:
- consequential and/or reputation damage;
- economic damage.

3.2.19 *Airspace and practice areas*

Current regulation leaves little to no airspace to practice and to perform drone flights for professional purposes. Professional drones which are under development and which have not been certified yet, should be able to be tested in special areas, dedicated for such purposes. In addition, research and development entities, investigating drones and drone applications, often want to use non-standard non-certified drones in a controlled environment.

Often, the only way to circumvent this issue, is to fly in military airspace, approved by the military aviation authorities.

The absence of practice areas for professional drone developers and users may result into illegal flights, potentially causing accidents and damage.

The Ministry of Infrastructure and Environment has recognized this issue and is working towards a solution. They have invited stakeholders to make known their wishes in this respect. The Ministry of Economic Affairs is also involved in discussions on this topic.

The risks associated with this issue are:
- consequential and/or reputation damage;
- economic damage;
- possibly others.

3.2.20   *Dynamics in developments*
In the area of drones, the developments in technology and in applications show a very rapid pace. It is very difficult to predict how the world of drones will look like within one year. On a daily basis, start-up companies come with new innovative ideas in technology and in the use of drones. Of course not all innovations will sustain, but we believe that there is enough momentum and we see a rapidly changing landscape. There is a certain risk that applications will arise which are unwanted, giving rise to ethical issues.

This highly dynamic environment requires a continuous monitoring effort of developments, both in technology as in applications, and perhaps also roadmapping of developments for different scenarios.

This issue could induce several possible risks.

3.3   **Overview of Risks**

From the inventory of issues, derived from various sources, a list of risks has been compiled, see the table below. The risks have been subdivided in five different categories:

- safety risks;
- security risks;
- privacy risks;
- economic risks;
- environmental risks.

Although some risks may be put in more than one category, we decided to put only a single category label to each risk. Economic risks often are consequential risks related to safety risks; as a result of a drone crash not only the safety of people is at stake, but economic losses will occur more often.

#	Description of risk	Type of risk
1	Damage to other aircraft or other colliding objects	Safety
2	Damage to people and property on the ground	Safety
3	Damage to (critical infrastructure)	Safety
4	Consequential and/or reputation damage	Economic
5	Prevent other aircraft from flying	Safety
6	Loss of drone	Economic
7	Loss of information stored in the drone	Security
8	Privacy infringement	Privacy
9	Economic damage	Economic
10	Security breach	Security
11	Terrorist attack	Security
12	Panic/disturbance of people on the ground	Security
13	Crime	Security
14	Annoyance (noise)	Environment
15	Environmental pollution and global warming	Environment
16	EM spectrum congestion	Environment

Table 3.2 Description of risks

4 Risks

4.1 Introduction

In the previous chapters an inventory of risks related to the issues found has been made, see Paragraph 3.3. With respect to risk analysis and risk management, many different definitions and methods prevail. In this chapter, first we define risks and methods to deal with risks, associated with the use of drones in the airspace. A separate paragraph addresses risk management and finally the issue of loss of link and all associated risks and effects is worked out in detail, as an example.

4.2 Risk Definition

Generally
Risk is sometimes described as the potential to lose something of value. This may just be interpreted as losing money, but other values like health, safety, well-being, a clean environment or reputation also represent value. It is quite obvious that these values are difficult to measure, represent or compare impartially.

Generally, a 'risk' is defined as the product of the likelihood an accident or event occurs and the impact, the expected loss to be expected. In other words: A risk describes an uncertain event or condition that, if it occurs, has an effect on at least one of the values to be protected against loss. The product of likelihood and impact gives a certain quantification of the loss when the effect actually occurs. It implies a certain mathematical comparability between risks, although the underlying values are most difficult to quantify.

Listing these products for many, usually orthogonal risks brings an overview of 'low', 'medium' and 'high' risks, where particularly the latter category may be subject of measures to be taken. Risks could be treated in different traditional ways:

1. *Risk acceptance*
   This treatment does not reduce effects of likelihood, but is considered a conscious choice to explicitly accept the risk when e.g. the cost of measures are unacceptable or the possible effects could rather easily be compensated. Low risks are frequently accepted in such a way.
2. *Risk avoidance*
   This treatment is the opposite of risk acceptance. It implies that action is to be taken to avoid any exposure to the risk whatsoever. In the drones case, it would possibly result in abandoning the use of drones at all.
3. *Risk limitation*
   The most common treatment, is taking (additional) measures to either reduce the likelihood or prevent a harmful event could occur, or to reduce, minimize or even remove the effects a risk might cause.
4. *Risk transference*
   This treatment implies the involvement of a willing third party, a risk is outsourced to. Typical implementations are insurances, covering e.g. financial risks. Today, many insurance companies develop their cyber risk

insurances. However, they also face the difficulty of estimating the true risk to insure and the required evidence to determine their responsibility.

The most appropriate measures to be taken ('controls') are usually selected based on very traditional risk assessments, where each risk is examined and treated separately within a tightly defined scope, like an organization.

Specifically in the drones domain
With respect to the risks associated with the use of drones in the airspace, the application of the definitions as used by EASA is proposed, with one extension, leading to five categories:

–   Safety risks:
  –   mid-air collision with manned aircraft and other unmanned aircraft;
  –   harm to people;
  –   damage to property, in particular critical and sensitive infrastructure;
–   Privacy risks / data protection:
  –   unlawful collection of personal data;
  –   unsecure transmission and storage of personal data;
–   Security risks:
  –   all forms of intentional misuse of drones;
–   Economic risks:
  –   consequential and/or reputation damage due to an accident;
  –   loss of drone;
  –   espionage;
–   Risks to the environment / environmental protection:
  –   noise (especially at night);
  –   pollution;
  –   radio spectrum

The level of risk to be estimated associated with these categories depends on:
–   the energy and the complexity of the drone (kinetic and potential energy);
–   the population density of the overflown area;
–   the design of the airspace and traffic density.

However, quantifying the risks associated with these categories is not trivial.

4.3   Risk Management

4.3.1   *Traditional Risk Management methods*
As described earlier, traditional risk assessment methods are all based on the assumption that risks to a certain extent act orthogonally, with little mutual influence within a well-defined scope, like an organization or an outsourced service. In usual 'chains' of collaborating organizations, each of the links will assess its risks and take measures, completing the chain.

However, the days that a limited number of organizations collaborate in chains, capable of managing their risks adequately to assure the continuity, safety and security of the chain itself, are far behind us. Complexity, distributed responsibilities, outsourcing and constantly evolving risks in the cyber domain prove the static

traditional paper annual risk assessment method to be insufficient again and again. This is mainly caused by the fact that organizations tend to work in networks, with very complex mutual connections in a frequently changing and evolving environment: the networked organizations structure. Traditional risk management strategies will finally collapse, as both the scope the risk management applies to and the dynamic character of risks to take into account simply expand too fast to keep proper track on in the near future. This may finally reduce traditional risk management methods to a cloak of risk controls, covering the most obvious local risks but discarding the systematic risks, making them obsolete.

4.3.2   *Networked Risk Management (NRM) method*
TNO developed the NRM method to deal with the flaws of traditional risk management methods in complex networked environments, particularly suited for highly dynamic cyber security risks. NRM drastically simplifies risk assessment and risk management, bringing it back to the bare essence without the unbearable burden of assessing all the compilation of stakeholders and generally updating all dynamic risks through the network.

NRM is based on the simple fact that any organization or organizational entity is responsible for a number of obligations towards others, where it should rely on some expectations from other organizations or organizational entities, see Figure 4.1. Both obligations and expectations are usually described in Service Level Agreements (SLAs). Both obligations and expectations are easily defined as a countable, usually very limited list of items an assignable manager is responsible for.
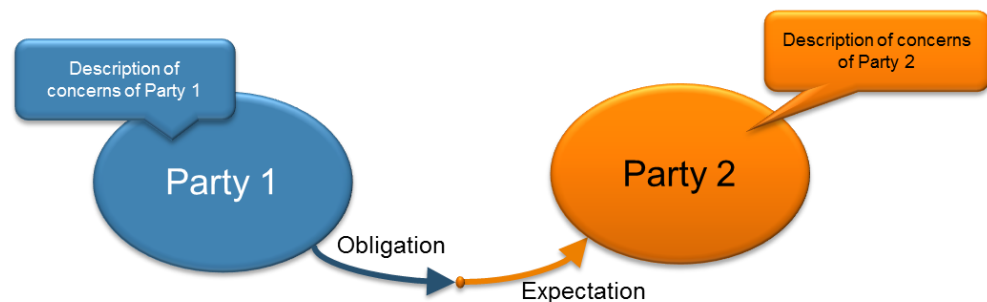
Figure 4.1 Obligations vs. Expectations between two stakeholders

The NRM method quickly assesses where the organizational misfits are to be found in broader scope, identifying potential (cyber) risks that nobody took into account (hazardous), identifying (cyber) risks that were taken into account but actually do not establish a serious risk in the network and finally clarifying what responsibility and measures are to be taken by whom. Even assumed expected obligations nobody asks for and expectations that nobody addresses are made transparent, optimizing the risk management efforts to its essential means. As a simple example, Figure 4.2 shows some relevant stakeholders in the issue of drones using the national airspace and their concerns ('obligations'):
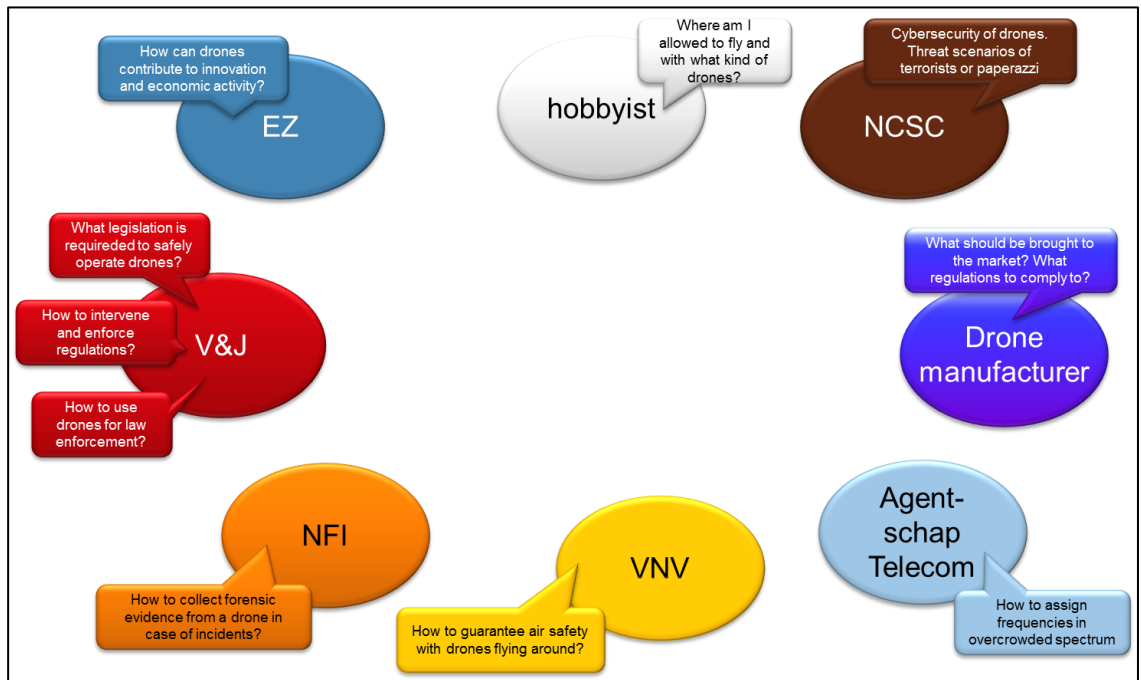
Figure 4.2 Stakeholder's obligations

The figure shows in general what responsibilities and concerns ('obligations') the various stakeholders may encounter, all from their angle of view. Figure 4.3 shows an example of expectations that may exist.
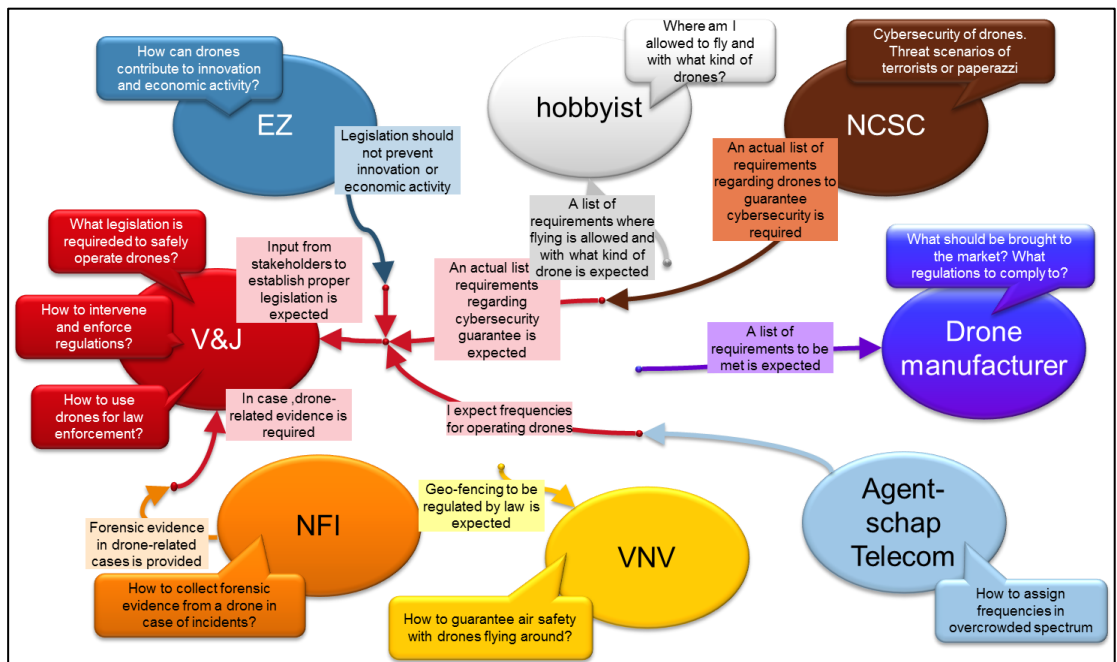
Figure 4.3 Stakeholder's obligations and expectations

The essential translation between the stakeholder's obligations and expectations towards each other in terms of risk is assessed under the assumption that any

stakeholder has certain likelihood to lose its capability to meet its obligations towards others. These obligations are subject of discussion in advance between these two stakeholders only! As a result, these two stakeholders decide what measures are necessary on which side, who bears responsibility, how violations are reported, how e.g. continuity is guaranteed and what dynamic risks are to be addressed by whom.

Risk Management for the drones case
The drones case is well-suited to apply the Networked Risk Management method to, as it is complex, multi-stakeholder, networked, dynamic and very difficult to control using traditional scoping.

The interviews with various stakeholders made clear that the risks associated with the use of drones in the national airspace are not very clear at all. It is perceived, for instance, that there is a non-negligible risk of small drones being ingested in passenger aircraft jet engines, but the probability of occurrence and the effect of such an event are not very clear and certainly not quantified. In these interviews it was stressed that the government has the responsibility to create a clear and quantitative picture of these risks, implying specific research efforts. It may be inviting to introduce certain risk mitigation measures as they seem to be useful or effective, but without a proper analysis the overall effects may be negative.

In addition, the importance of the authorities setting a quantitative acceptable level of risk, such as 10^{-6} for lethal accidents, for instance in order to give drone manufacturers a specific target to design on, should not be underestimated. The market is expected to respond to legal guidelines, taking all the risks and effects into account, as manufacturers only have a limited view on both stakeholders and risk appetite.

4.4   Risk Analysis: Loss of Link

As an example, the threat of a loss of link introduces multiple risks. The presumed context for the risk analysis regarding loss of link is a flying drone under direct control of a flight controller operated by the drone operator, see Figure 4.4.
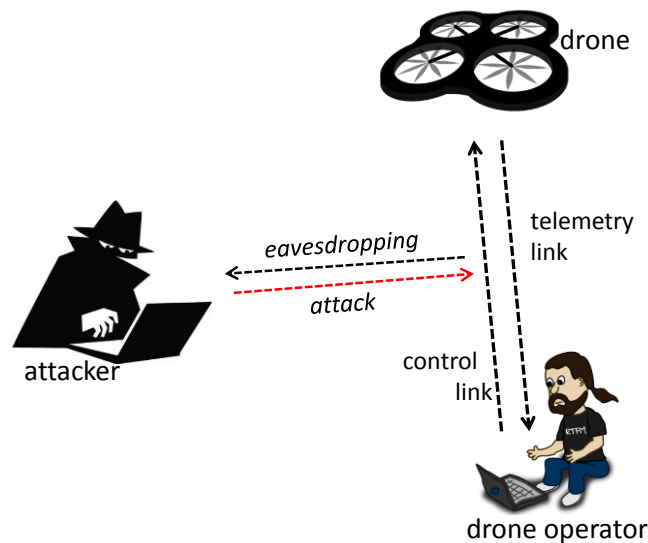
Figure 4.4 Drone link loss risk analysis context

Autonomous drones, capable of flying and navigating by themselves, are out of scope for this risk analysis. Using the flight controller the drone operator controls altitude, speed and heading of the drone as well as possible other sensor functionality such as taking a picture or video capturing. To have proper control, it is mandatory the drone operator has (virtually) immediate feedback, i.e. the drone responds quickly to the controller's actions. Generally, the control link will be wireless and unidirectional. Yet, a drone might send back telemetry data as part of the control link's protocol. Other data such as pictures or (real-time) video are not considered to be part of the control link and normally use a different dedicated video link or local storage. Aspects regarding radio chip and firmware implementations of transmitter and receiver are out of scope as well.

The control link is based on radio communication and thus vulnerable to:

– Eavesdropping of radio signals;
– Disturbance of radio signals;
– Unavailability of the radio signals;
– Use of 'fake' radio signals to take control of the drone.

These vulnerabilities are to be taken into account, all with certain likelihood to come true. However, the probability of occurrence is very difficult to quantify.

The impact of losing the control link is losing direct remote control of the drone. Often (but not necessarily all the time) this will result in loss of control of the drone and possible undesirable drone behaviour. As a result, the drone might crash and/or hit an object or a person. Additionally to direct physical damage the impact might be financial as the drone operator is generally responsible and accountable for damage caused by the drone.

Possible causes with respect to drone control are (not exhaustive):
– Drone moves out of range of radio signal;
– Object blocks radio signal;
– Introduction of errors in received control link data due to radio interference;

— Drone does not receive control link data due to severe radio interference;
— Drone receives control link data that does not actually originate from the controller but from an attacker;
— High latency between action taken by controller (operator) and the moment the drone receives the control link data related to this action;
— Slow update rate of control link data.

Some causes could be prevented; others simply have to be accepted. Possible measures to be taken against the likelihood a control link gets lost or reducing the effects of losing the control link may include the implementation of the following measures.

Reduction of likelihood
— a properly defined fall back link
  This redundant solution reduces the likelihood of losing the control link.
— a robust radio link protocol, tolerant to radio interference.
  For instance frequency hopping and DSSS techniques can be used to limit the impact of radio interference in crowded frequency bands (such as 2.4 GHz ISM band).
— measures to prevent and/or disallow others from using the radio spectrum used by the radio control link.
— a mechanism to detect and signal radio link reception weakness.
  This may lead to a signal to the operator the drone is about to lose radio contact.
— a mechanism the drone can distinguish between radio link information.
  This may enable the drone to identify genuine controller and possible fake radio link information from an attacker. A possible solution is digitally signing the radio link transmitter signal, using a unique (and secret) cryptographic key.
  Verification of the digital signature will determine the genuine originator.

Reduction of impact
— a properly defined fall back behaviour
  This might go as far as having the drone flying autonomously, based on input from its sensors and/or a pre-defined flight route. Another example is to have the drone turn around when it moves out of range of the radio signal.
— integrity checks, such as a CRC
  These may detect possible errors in the received data, leading to temporarily ignoring the control link data when integrity has possibly been compromised.
— error correcting mechanisms
  These may lead to temporarily ignoring the control link data when errors cannot be corrected and thus integrity cannot be assured.
— a radio link with low latency and high update rate of radio link information
  This enables the drone to react almost instantaneously to the operator's actions. Control links via WiFi or a telecom network are more vulnerable to variations in network performance.

Selection of the most appropriate i.e. effective or efficient measures ('controls') mentioned is virtually impossible without a thorough analysis of both likelihood and impact. It is strongly recommended to investigate these parameters before control selection to prevent an inadequate set.

5   Consideration of Technical Measures

5.1   Introduction

This study is primarily aimed at the technical measures that can be taken to enhance the safety and the security of the use of drones in the national airspace. Policy measures and legal measures [4] may be very effective to some or more extent to enhance safety, but are out of the scope of this study. Some measures described here are not of a technical nature, but do have (some) technical consequences. For this reason we have included these measures in this report.

Again, we mention that it is not possible at this stage, to quantify the level of risk reduction to be achieved by each of these measures. Furthermore, it is important to notice that some measures, meant to reduce risks, might introduce new risks. As an example, the introduction of a kill switch reduces the risk associated with unlawful use of drones. However, if other people are able to hack the security measures of the kill switch, and succeed in entering the 'back door' , the consequences might be worse. These effects will be clearly indicated if applicable.

The technical measures presented are based upon thorough knowledge of a number of specific technical issues available at TNO, while additional information and insights have been collected through literature and Internet search, and through brainstorming. These measures differ in Technology Readiness Level (TRL).

We first present in Paragraph 5.2 a longlist of technical measures describing each specific measure and describing how it may address one or more issues, mentioned in the previous chapter. If the measure introduces new specific issues or risks, this will be mentioned explicitly.

In Appendix C we provide a slide for each of these technical measures with a short description and the issues which are addressed by that measure. The number of issues addressed by one specific measure, is not proportional to a decrease in risk. Furthermore, for each technical measure, a qualitative ranking of the technical measure on four dimensions is given:

- technology readiness;
- cost;
- time to implementation;
- commitment from stakeholders.

In Paragraph 5.3 an overview is presented of all technical measures presented in combination with the issues they address and the above mentioned qualitative ranking on the four dimensions.

In Paragraph 5.4, we indicate a number of technical measures which can be implemented relatively easy and quickly, although their contribution to the reduction of risks cannot be quantified yet.

In the last three paragraphs of this chapter, three specific technical measures will be explained and highlighted in more detail:

- geofencing/no-fly zone (Paragraph 5.5);
- kill switch (Paragraph 5.6);
- traffic management (Paragraph 5.7).

5.2 Technical Measures and Technical Aspects Related to Non-Technical Measures

5.2.1 *Limiting technical capabilities of drones*

A number of technical measures can be defined to limit the performance of a drone, in order to decrease the risk of an accident to happen or in order to decrease the effects as a consequence of an accident. The latter relates to the fact that the impact of a drone on another object or a human being is proportional to its velocity squared.

Some drones can attain high speeds and large accelerations. It needs no explication that it requires a very experienced operator to fly a drone at such conditions, otherwise accidents, such as collisions with other aircraft, buildings and trees and losing contact with the drone, will be frequent. In addition, in case of geofencing or in case the drone is equipped with sensors for collision avoidance, the reaction time to avoid entering the no-fly zone or to avoid a collision might be too short. In general, such a limitation will be applied through the software, although hardware solutions are feasible too.

In case where drones fly a speed competition on closed circuits, these limitations shall of course not be imposed.

An altitude limitation for drones could also be an important measure to take, which can be implemented fairly easily.

To prevent that a drone flying on autopilot shows unexpected or unwanted behavior, some limitations could be installed in the autopilot software. Think for instance about limiting the distance between drone and pilot. In addition, software and/or autopilots could be tested and certified and put on an 'approved' list (RAVT initiative of UVS International).

5.2.2 *Kill switch*

A kill switch is a general name for the possibility to remotely control a drone from the outside by a third person, not being the drone operator. The kill switch command must override the command and control as issued by the operator. Such a kill switch might for instance enable law enforcement authorities to control a drone carrying out suspicious or unlawful activities or to force a drone to land after entering a no-fly zone.

The ability to use a kill switch shall exclusively be given to law enforcement authorities; it requires the cooperation of manufacturers to create a 'back door'

through which the control signal of the kill switch can override all other control signals. This kill switch may take effect directly on the drone and/or on the drone ground control station. It should be taken care of that kill switch allows for proper control.

Such a kill switch requires a very sophisticated security system, otherwise any smart hacker may use the same back door to control other peoples' drones.

In Paragraph 5.5 the kill switch is described and discussed in more detail.

5.2.3   *Registration and identification*

For various purposes it is required to be able to know who is the operator/owner of a drone. In case a drone is lost, the owner can be traced, in case a drone causes damage, the responsible person can be traced and in case a drone is involved in unlawful operations, law enforcement personnel can make use of owner/operator information.

In the US, the Department of Transport has decided that all drones beyond a certain mass, need to be registered. In November, a Task Force was installed to advise the Federal Aviation Administration (FAA) on the best way to carry out this registration process. In its final report [19] the Task Force proposes a recommendation that only unmanned aircraft of 250 grams or less may be exempted from registration, based upon an assessment of lethal effects of crashing drones.

In summary the Task Force issued the following recommendations:
- UAS that weigh under 55 pounds and above 250 grams maximum take-off weight and that are operated outdoors in the national airspace are subject to registration;
- the registration system shall be owner-based, each registrant will have a single registration number that covers any at all UAS that the registrant owns;
- registration is mandatory prior to operation of a UAS, not at the point of sale;
- only the name and the street address of the registrant are required, other data is optional;
- there is no citizenship requirement;
- persons must be 13 years of age to register;
- registration is free of charge;
- the system for entry of information into the database is web-based and also allows for multiple entry points;
- a certificate of registration will be sent to the registrant at the time of registration; the certificate will contain the registrant's name, FAA-issued registration number, and the FAA registration website that can be used by authorized users to confirm registration information;
- the registration number shall be affixed to the aircraft, unless the aircraft's serial number is used as the registration number.

Mid-December, the FAA issued the final regulations [20], charging $5 for each registration after a period of one month of free of charge registration.

In Europe we also can see an increased interest in mandatory registration of drones.

In addition to a registration number fixed to the drone, the addition of a transponder or a small beacon to a drone allows, in principle, to broadcast a unique ID of a drone. Transponders primarily function for collision avoidance purposes and do not necessarily broadcast the aircraft ID, but this functionality could easily be added.

Commercial companies[3] offer small transmitters (12 grams) to be strapped to a drone. Such a device transmits in the 900 MHz range, which signal can be picked up by a handheld device, allowing the operator to trace back his drone, in case it was lost. The system does not use GPS or cellular communication networks.

5.2.4   *Visual observability*

If drones are clearly visible, by means of special striping (such as this ambulance drone[4]), bright colors and for instance strobe lights, this increases airspace safety, because manned airborne platforms will be able to see them earlier and from a larger distance. In the various position papers, written by various airline associations, this item is always strongly advocated.

From a point of view of safety on the ground it works the same; if drones are better visible, people on the ground have more time to detect them and, if necessary, to avoid them. The same reasoning holds of course for purposes of law enforcement. In practice, it very much depends on the circumstances if visibility enhancing measures have a real effect.

Measures to enhance visual observability are easy and cheap to implement.

5.2.5   *Collision avoidance*

An important step to increase the airspace safety and the safety on the ground would be to have a so-called sense-and-avoid (SAA) system mounted on every drone. At present, various initiatives and projects are being undertaken to install and test such systems on larger unmanned aircraft, as a prerequisite for military UAV's to fly in regular airspace. For smaller drones, however, such devices are still too heavy and require too much power. There is one company, Panoptes, which

---

[3] http://www.uavfind.com/
[4] http://www.tudelft.nl/actueel/laatste-nieuws/artikel/detail/ambulance-drone-tu-delft-vergroot-overlevingskans-bij-hartstilstand-drastisch/

sells the so called eBumper[5], to be mounted on a DJI drone, which is a device to avoid the drone colliding to obstacles. A number of acoustic (ultrasonic) emitter/receiver devices, like applied in cars as parking assistants, is mounted to the drone. As soon as one or more of these devices detect an obstacle, the autopilot automatically diverts the drone to avoid the collision. In some models the acoustic sensors are combined with stereo cameras and object detection algorithms, to improve performance. Such a functionality properly works to avoid static objects and slowly-moving dynamic objects. A certain velocity is required to function properly.

The same functionality could be obtained by use of the forward facing camera of the drone in combination with an algorithm to detect obstacles. At MIT[6] an algorithm has been developed enabling a drone to fly at 50 km/h while avoiding obstacles. Such an algorithm, however, is not yet available for commercially available drones.

Another option might be to combine First Person View to fly the drone with Augmented Reality, through which known obstacles in a certain area, could be brought under the attention of the pilot.

5.2.6 Transponders

Transponders are devices which get their position from a global navigation satellite system like GPS and transmit their position periodically, typically once per second. At present Automatic Dependent Surveillance-Broadcast (ADS-B) is becoming the standard. It is replacing surveillance by means of radar systems; countries are building up rapidly more ADS-B ground stations, to increase coverage. In the second generation of the

---
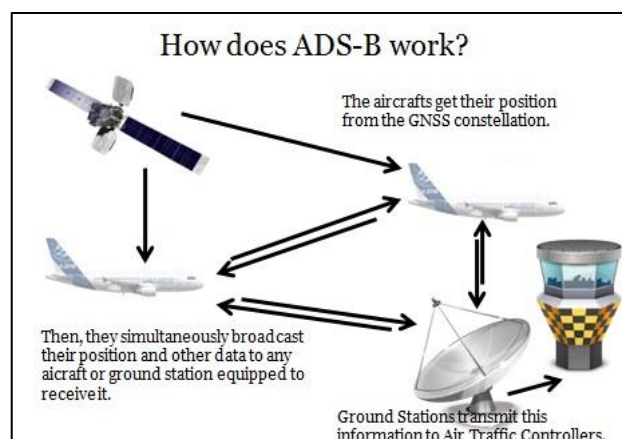
[5] http://www.panoptesuav.com/ebumper/
[6]

http://www.roboticstrends.com/article/watch_mit_drone_autonomously_avoids_obstacles_at_30_mph

Iridium telecommunications satellite constellation, ADS-B transponders will piggyback, meaning that in 2018 full global coverage will be assured. ADS-B has a much more accurate air picture than can be obtained by radars, both in terms of position accuracy as in time accuracy.

Current ADS-B transponders are relatively heavy and require significant power. Google has recently[7] announced that it is pursuing to design, develop and produce ADS-B transponders, suitable for small drones. A possible negative consequence of many drones equipped with such transponders is a congestion of the frequency spectrum. This issue, however, will be considered in the Google project.

5.2.7   *Detection/tracking/logging*

This measure refers to a combination of all possible means to know where drones are flying or have flown. A number of different techniques exists to detect drones, such as radar, electro-optic cameras, infrared cameras, acoustic devices and electronic listening devices. A combination of different detection techniques is required to achieve a robust system, because detection of very small drones is not straightforward. In [21] an overview is presented of various detection techniques and their capabilities.
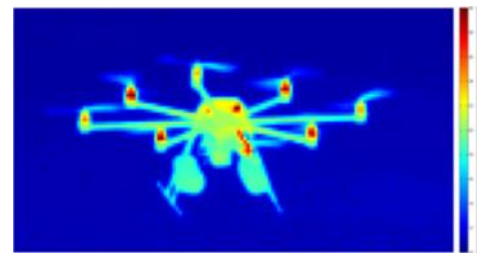
After detection, drones could be tracked in time; each individual sensor could cue one or more other sensors to aid in tracking the drone, depending on coverage and detection capabilities.

All detection and tracks could be logged.

5.2.8   *Telecom networks to track drones*

Existing cellular networks could be used to keep track of drones. If drones would be in direct contact with a cellular network, information about the position of the drone can be sent to a traffic management system and vice versa, information about no-fly zones and other aircraft can be sent to the drone. Even without the exact GPS location of the drone, the network could determine its position, by triangulation.

At present such a system would not work, because most cellular network antennas are directed towards the ground and not towards the air. NASA is considering this technology as one of the constituents of its UAS traffic management system (UTM), together with PrecisionHawk[8], Harris,

---
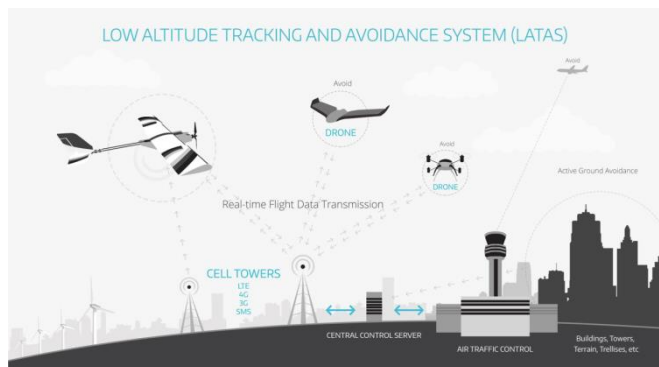
DigitalGlobe and Verizon. Their proposed LATAS[9] tracking and avoidance system is also based on communications using cellular networks.

Of course, some changes to the drone itself need to be made (addition of GSM module) and modifications in ground infrastructure and possibly in some high-altitude cellular nodes are required.

5.2.9 Airspace division

In the present regulations, small drones already are restricted in flight altitude. In a step towards further increasing airspace safety, Amazon [23] has proposed to subdivide the airspace in a number of layers:

− below 200 ft (61 m) for 'low and slow' drones;
− between 200 ft (61 m) and 400 ft (122 m) as a high-speed corridor for beyond line of sight flights (such as packet delivery);
− a no-fly safety zone between 400 ft (122 m) and 500 ft (152 m);
− beyond 500 ft (152 m) for manned aircraft.
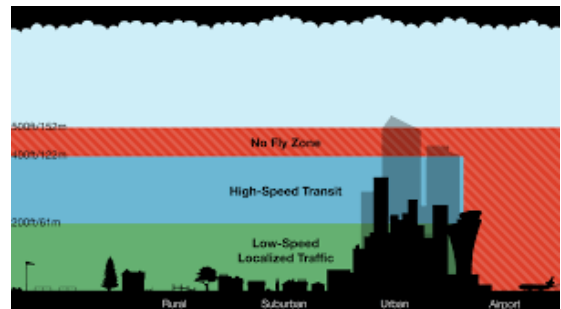
Such a division of the airspace would significantly contribute to airspace safety. It is mandatory, however, that drones are programmed not to leave their specific layer.

Amazon also proposes that access to airspace is coupled to the capabilities of drones.

5.2.10 Apps

Smartphone applications ('apps') may significantly contribute to the safe flying of drones. Many different apps are being developed, with different purposes (possibly combined into a single app):

− providing education about the rules and about safe flying to the drone operator;
− providing actual data about no-fly zones (NOTAMs) and desirable failsafes;
− providing actual data about weather conditions;
− providing actual data about the whereabouts of other aircraft;
− control of the drone;
− flight planning and checking available airspace;
− sending back information on the actual drone position.

In principle, apps just provide information to the user or send information to the air traffic management system. In case the app would be coupled to or integrated with the flight control system, information about no-fly zones could directly lead to the drone not entering this area and carrying out the specific failsafe for this area.

Through apps it is possible to stimulate desirable behavior.

---

[9] http://flylatas.com/

To get a good working system, it is required that apps are updated regularly; preferably the smartphone or tablet used for control of the drone has permanent access to Internet; for the provision of the actual drone position information to the traffic management system, this is a requirement. Another drawback is possible vulnerability for hacking.

5.2.11　*Flight planning*
If the pilot of a drone would make a flight plan in advance, as is required for most manned aviation, this would contribute to improved situational awareness about the airspace. The flight plan can be checked against other flight plans and the area and time window can be cleared for this specific flight.

A drawback of course is that people might not stick to the flight plan or submit a flight plan but do not fly. The advantage is that it can be established relatively easily through a website, and that the drone pilot can be aided to have the flight as safe as possible. It can be done in advance, so a real-time network is not required.

Should submission of a flight plan in advance become mandatory, it is expected to get a lot of resistance. If flight planning can be carried out by a smartphone app, see previous section, and the app will submit the flight plan to the central air traffic management system automatically, it might become a very useful addition to the integral air picture.

5.2.12　*Air traffic management systems*
A traffic management system gathers information about all aerial traffic in a certain area, and manages the traffic in such a manner that collisions are avoided and traffic flows smoothly. The best known concept of such a system is NASA's Unmanned Aircraft System Traffic Management System (UTM[10]). It uses a combination of techniques to obtain a complete air picture.

The UTM system would '*enable safe and efficient low-altitude airspace operations by providing services such as airspace design, corridors, dynamic geofencing, severe weather and wind avoidance, congestion management, terrain avoidance, route planning and re-routing, separation management, sequencing and spacing, and contingency management.*

One of the attributes of the UTM system is that it would not require human operators to monitor every vehicle continuously. The system could provide to human managers the data to make strategic decisions related to initiation, continuation, and termination of airspace operations. This approach would ensure that only authenticated UAS could operate in the airspace. In its most mature form, the UTM system could be developed using autonomicity characteristics that include self-configuration, self-optimization and self-protection. The self-configuration aspect could determine whether the operations should continue given the current and/or predicted wind/weather conditions.

NASA envisions concepts for two types of possible UTM systems. The first type would be a Portable UTM system, which would move from between geographical areas and support operations such as precision agriculture and disaster relief. The

---

[10] http://utm.arc.nasa.gov/index.shtml

*second type of system would be a Persistent UTM system, which would support
low-altitude operations and provide continuous coverage for a geographical area.
Either system would require persistent communication, navigation, and surveillance
(CNS) coverage to track, ensure, and monitor conformance.'*

NASA foresees a stepwise approach to increase the capability of the system. NASA
is pursuing this capability in close cooperation with the FAA. It is anticipated that so-
called Airspace Service Providers act as an intermediate between drone operators
and air traffic control, maintaining databases of no-fly zones, providing weather
information, obstacle/terrain information, traffic information and flight plans.

The NASA UTM concept

Part of such a concept is the ability to deal with drones with different capabilities:
−   'basic' drones that are piloted by remote control (LOS);
−   'good' drones, which have an Internet connected ground station and the
    operator responsible for separation;
−   'better' drones, which have Internet connected drones which automatically
    separate;
−   'best' drones, which have SAA to avoid non-collaborative objects (such as
    birds).

In Paragraph 5.6 air traffic management is discussed in more detail.

5.2.13   *Establishing no-fly zones*
It is important that people know where not to fly. Basic regulations already prescribe
where drone flight is allowed. However, it is not always the case that people flying
drones know the rules, resulting in many incidents, especially near no-fly zones
such as airports. For reasons of safety it is mandatory to have no-fly zones. Static
no-fly zones are of course quite straightforward to communicate; dynamic no-fly
zones, in case of a public event, an accident or a disaster can presently not be
communicated very quickly. These so-called Notice-to-Airmen (NOTAM) generally
take a couple of days to become effective.

The concept of using smartphone apps or websites with actual no-fly zone data to be able to instantaneously get a complete picture of no-fly zones, will solve a lot of these problems. If a drone pilot always has easy access to the actual status, a lot of incidents may be prevented.

Please note that informing the pilot about no-fly zones does not automatically implicate that the pilot will not fly his drone into this area. Only if the no-fly zone is enforced, through geofencing, this will be the case. The majority of the users, however, will strictly respect no-fly zones.

5.2.14   *Geofencing/enforcing no-fly zones*
Geofencing in essence means that the drone knows its own position and has access to a database in which no-fly zones are registered. The drone has been programmed not to enter such a zone. Geofencing is considered to be a very effective measure, especially for the great majority of users that has no intention to break the law. The measure has no effect on the flight performance of the drone, so users will not experience any adverse effect of this measure.

For effective application of this measure, it is required that this feature is installed in the flight control software of the drone. The DJI company already has this feature available for static objects like airports, and most probably other companies will follow. It also requires that the database of no-fly zones is actualized frequently.

Geofencing does not prevent flight in all 'forbidden' areas; such as roads, population areas, et cetera.

At present there is no means of conceiving a dynamic (temporary) no-fly zone, for instance in case of a large event or an incident. It is expected that this will be possible in the near future, through the use of apps. Commercial service providers already provide access to a database of no-fly zones, which can be updated instantly. If drones, before taking off, make a connection to such a database, they have an actual knowledge of no-fly zones. 3D Robotics has announced a future cooperation with such a service provider for the purpose of geofencing.

A possible drawback of such a system could be the dependence on commercial companies, especially if their databases would not be up to date.

In Paragraph 5.4 the technical measure of geofencing is discussed in more detail.

5.2.15   *Beacons to establish no-fly zones*
In case of an urgent requirement to establish a no-fly zone, for instance in case of an accident where Helicopter Emergency Medical Service (HEMS) is required, a beacon could be placed, sending a signal to declare a no-fly zone. If a drone is sighted at such an occasion, the helicopter cannot land. Of course, drones and/or the drone ground control station should be suited to receive such a signal and the control software should recognize the signal. It would require at least some software modifications and possibly hardware modifications.

The advantage of such a system is that it has an immediate effect. Establishing a no-fly zone through the Internet requires the drone to be in continuous contact with the Internet, which in reality will not be the case.

5.2.16   *Securing of the control link*

The control link is vulnerable to electronic attack [33], [34], [35] and [36]. Technical measures to protect the link against attacks will increase safety and security. To prevent hacking and spoofing, first of all encryption of the signal is important. Features like frequency hopping will further reduce the risk. If the frequency hopping uses a relatively broad part of the spectrum, or if the control signal is redundant over several frequencies, even jamming becomes more difficult.

It is desirable that a drone is able to detect if the control signal is compromised; in that case it should be able to autonomously carry out a robust failsafe. This feature should be independent from the control system (security by design) and should be certified.

It is desirable that software updates cannot be uploaded to a drone by a wireless connection. Firmware and updates should be 'signed'.

Access to the remote control of the drone could be enabled by a unique personal identification key.

It is advised to take notice of all lessons learned with respect to cybersecurity on the Internet.

Due to the sensitivity of this topic, we will not go into detailed possible technical measures.

5.2.17   *Securing of the information downlink*

Attack on the information downlink has no safety risk - unless the information downlink is used for control, such as when flying beyond line of sight - , only a risk in the area of security. Here also measures like encryption and frequency hopping will prevent the most common methods of electronic attack. Most issues mentioned in the previous section, also apply here.

5.2.18   *Impact limiting devices*

To mitigate the effect of a drone impact, impact limiting measures may be taken. A good example is the addition of a parachute. Several commercial companies offer an add-on parachute, to prevent damage to the drone and its payload, in case of emergency. The parachute can be activated manually, but efforts are going on to incorporate a safety system in the drone to activate the parachute automatically in abnormal flight situations. The additional mass decreases the flight time, and depending of the location where the parachute is mounted, it might affect its flying behavior and stability. In addition, a parachute requires a certain altitude of the drone, to take time to deploy. In some countries or areas (e.g. Hong Kong) a parachute system is mandatory.

Another measure which could be taken is to design the drone in such a way, that it has minimal impact on the object it collides with, just like cars, which are designed to absorb a maximal amount of energy by deforming their structure, thereby decreasing the momentum inflicted on the object of collision. If for instance, the arms of the main structure of the drone break off easily at impact, less damage might be inflicted. Also the shielding of sharp edges et cetera, will have a positive effect.

We anticipate that in the future, like for cars, drones will be subjected to crash tests and receive a rating for crashworthiness (like the NCAP star system). Such a rating will be mandatory to get the aircraft certified and insured. UVS International has emphasized this point on several occasions.

5.2.19   Propellers

The propellers of a drone are a serious source of injuries to people. Very recently, in the UK a toddler[11] lost one of his eyes due to the propellers of a drone. It seems a very simple measure to mandate shielding of the propellers by a structure, as some manufacturers already do. The drawback of such a measure, however, is that it adds weight and may affect flight performance. On the other side, such a protective structure also prevents damage to the drone itself, which might be a good selling point to drone users.

One may also consider to look at the material of which the propellers are made. Metal or carbon propellers will inflict much more damage due to their large strength and stiffness. Plastic propellers will break more easily.

5.2.20   Pilot's license

Requiring the drone pilot to obtain a license is not really a technical measure, but it could be enforced by technical measures, such as the provision of a unique identification key, to unlock the control station. It will certainly contribute to airspace safety and ground safety. Presently, a license is required only for professional flying of drones. An option could be to get a discount on the insurance premium if one obtains a license, or other possible advantages, such as increased airspace access.

5.2.21   Education and PR

Although not an explicit technical measure, education and information of drone safety aspects to the public is considered to be a very important issue. As the cost of drones decreases and the availability increases, many people purchase a drone for recreational purposes (Christmas gifts); most of them do not know the rules and cannot wait to fly the drone as soon as possible. This already has led to many fly-aways and crashes, due to ignorant use of the drone. If for instance, the home

---

[11] http://www.bbc.com/news/uk-england-hereford-worcester-34936739

position of the drone has not been set correctly, it may want to fly to China if the command 'go home' is activated (assuming the drone was built in China).

It is important to promote safe use of drones, and safety is primarily about people acting in a safe manner. Basic flight safety rules should be communicated:

− where can I fly, what locations are suitable for flying?
− practice the control of your drone;
− keep your drone always in sight;
− use the right failsafe settings, or you might lose your drone;
− take care of your equipment;
− et cetera.

Campaigns directed to make the public aware of the rules for flying drones and of the safety aspects when flying drones, may very effectively contribute to more safety. In many countries such a campaign has started, such as in the US [12] [13] and in the Netherlands [14]. Campaigns may consist of websites giving information, commercials, attention in TV programs, organization of special workshops, leaflets in the box in which the drone is sold, posters in the shops of drone sellers, banners on the websites of drone sellers, et cetera. The B4UFLY campaign in the US already has launched an app for smartphones to support public information (picture on the right), combined with for instance information about no-fly zones.

5.2.22   Safety requirements

The conception of safety requirements to be posed to drones will certainly have a positive effect on safety. Nowadays, only professional drones have to be certified. A drone which is considered to be safe, according to certain standards, will attract more customers and will be cheaper to insure.

In our opinion, authorities need to establish safety standards (above a certain mass level) and require that also consumer drones are tested against these standards. See also the sections on impact limiting devices and propellers.

5.2.23   Reporting incidents

In the aviation world it is quite usual to report all incidents, which has a very positive effect on safety. If incidents with drones were also to be reported, lessons learned could be drawn and safety could be enhanced. Future registration of drones will automatically lead to reporting of incidents which resulted in the crash of a drone and incidents in which the drone registration number could be identified.

Technical measures could be the introduction of a black box in the aircraft, logging flight data and automated incident reporting in case of a crash by the aircraft or by the ground control station.

Mandatory reporting of incidents most probably will not work.

---

[12] http://www.faa.gov/uas/b4ufly/

[13] http://www.knowbeforeyoufly.org

[14] http://www.rijksoverheid.nl/drones

5.2.24   *Rewarding good behavior/perks*
Safety in the air and safety on the ground is very much dependent on the behavior of the drone pilot. We believe that, like for car insurance, a bonus/malus system for insurance premiums will affect human behavior. Such a system can be based on rewarding incident free flying years. Another idea would be to actively monitor the flying behavior of the pilot, through an app, submitting the information to the insurance company, just the way some insurance companies are proposing nowadays for cars, promising lower rates. This measure, which could be supported by technical measures, of course only works if insurance companies actively demand safe flying.

Of course, the bonus or perks could also come from government, giving more rights and privileges to safe pilots.

5.2.25   *Pricing of safety measures*
In case certain safety measures, as mentioned earlier in this chapter, are not yet mandatory, people could get these attributes at a reduced price, to stimulate safe flight. Government and/or insurance companies could stimulate this. Perhaps the perks, to be earned by safe flying, could result in a discount on safety equipment.

5.2.26   *Drone circuits*
To prevent people racing their drones at tremendous speeds in regular airspace, the conception of special drone flying (racing) circuits will help increase airspace safety. It should be fun to go with a drone to a special circuit, and race against other drone pilots. It could also be highly attractive for public and become a real event, like Formula 1 racing.

5.2.27   *Noise reduction*
The noise produced by drones is primarily generated by its propellers, and in case of combustion engines by the combustion chamber and the gears. In general a larger number of smaller engines (and propellers) will generate less sound than a smaller number of bigger engines. Ducting the propeller will reduce the noise generated by propeller tip vortices. Finally, aerodynamic design of propellers can be optimized for low noise production.

5.2.28   *Pollution reduction*
In case drones a driven by electricity, they do not produce pollution while flying. Batteries, however, have a limited lifetime and must thereafter be treated as chemical waste.

Recently, new concepts have emerged using fuel cell technology, for instance using hydrogen as a fuel. This of course, is also very environmentally friendly. Then only the production of energy or hydrogen can be influenced to be as green as possible.

It should be noted that rotorcraft drones require more energy to fly than fixed wing drones, not only resulting in less endurance but also in higher fuel consumption.

5.3   Preliminary Assessment of Technical Measures

In the figure below, an overview is given of all technical measures described (first column) in Paragraph 5.2, the issues being addressed by each technical measure (second column, most important effects in red) and a qualitative impact assessment (third column). For the sake of completeness and clarity, the list of issues is summarized below.

#	Description
1	Airspace safety
2	Safety on the ground
3	Airworthiness
4	Evolving capabilities
5	Unpredictable behavior
6	Privacy infringement
7	Espionage using drones
8	Vulnerability to jamming, spoofing, hacking, eavesdropping
9	Frequency spectrum
10	Loss of link
11	Legislation
12	Communication
13	Unlawful use
14	Law enforcement
15	Annoyance
16	Environment
17	Liability/insurance
18	Airspace and practice areas
19	Dynamics in developments

Table 5.1   Issues identified

For each technical measure it was assessed which issue they address, i.e. if the technical measure has been implemented, the risk associated with the issue will be diminished or the issue as such will have disappeared. Issue numbers marked in red are significantly affected by the measure, numbers marked in black only slightly or indirect. In case a measure has a negative effect on any issue, we have mentioned it in the various sections of Paragraph 5.2.

The four impact categories are: the estimated cost of implementation of the technical measure, the technological complexity, the required time to implement and the expected resistance.

Technical Measure	Applicable to following issues	Cost of Technical Measure	Technological complexity	Time to implement	Expected Resistance
1. Limiting technical capabilities of drones	1, 2, 4, 5	1	1	1	3
2. Kill switch	1, 2, 5, 10, 13, 14, 17	3	2	3	3
3. Registration & Identification	13, 14, 17	2	2	2	2
4. Observability	1, 2, 14	1	1	1	1
5. Collision avoidance	1, 2, 17	2	2	2	1
6. Transponders	1, 2, 14, 17	2	2	2	1
7. Detection/tracking/logging	1, 14, 17	3	3	3	1
8. Telecom networks to track drones	1, 13, 14, 17	2	2	3	2
9. Airspace division	1, 14	1	1	1	1
10. Apps for sharing flight information and practice	1, 5, 12, 13, 14, 17, 18	2	1	2	1
11. Flight planning & approval	1, 14, 17	2	1	1	3
12. Air traffic management systems	1, 13, 14	3	3	3	1
13. Establishing No-fly zones	1, 2, 13, 14, 17, 18	1	1	1	1
14. Enforcing No-fly zones	1, 2, 5, 10, 13, 14, 18	1	2	2	1
15. Beacons to establish no-fly zones	1, 2, 12, 13, 14	2	2	2	2
16. Communications link	1, 2, 6, 7, 8, 10, 13, 17	2	2	1	1
17. Information downlink	6, 7, 8, 13	2	2	1	1
18. Impact limiting devices	1, 2, 17	2	2	2	2
19. Propellors	2, 17	1	1	1	1
20. Pilot's licence	1, 2, 5, 17	2	1	1	2
21. Education and PR	1, 2, 19	2	1	2	1
22. Safety requirements	1, 2, 17	1	2	2	2
23. Reporting incidents	1, 2, 14	1	1	1	3
24. Rewarding good behavior/perks	1, 2, 17	1	1	2	2
25. Pricing of safety measures	1, 2, 17	2	1	1	1
26. Drone circuits	1, 2, 13, 14, 15, 16, 18	2	1	3	2
27. Noise reduction	15, 16	2	2	2	1
28. Pollution reduction	16	2	3	3	2

Table 5.2 *Longlist of technical measures to enhance the safe and secure use of drones, addressing one or more issues identified, combined with a qualitative assessment of feasibility.*

The green (1) category means respectively low cost to implement the measure, low technological complexity, short time to implement and none to low public resistance to implement the measure. The red (3) category means respectively expensive to implement, high technological complexity, long time to implement and large expected public resistance. The yellow (2) markings represent in between values.

It must be stressed that this is a first educated guess, not founded by investigation and perhaps biased by definitions of terms.

If we sort the technical measures in the order of ease of implementation, the order is represented in Table 5.3.

Technical Measure	Cost of Technical Measure	Technological complexity	Time to implement	Expected Resistance
Observability	1	1	1	1
Airspace division	1	1	1	1
Establishing No-fly zones	1	1	1	1
Propellors	1	1	1	1
Pricing of safety measures	2	1	1	1
Limiting technical capabilities of drones	1	1	1	3
Apps for sharing flight information and practice	2	1	2	1
Enforcing No-fly zones	1	2	2	1
Communications link	2	2	1	1
Information downlink	2	2	1	1
Pilot's licence	2	1	1	2
Education and PR	2	1	2	1
Reporting incidents	1	1	1	3
Rewarding good behavior/perks	1	1	2	2
Collision avoidance	2	2	2	1
Transponders	2	2	2	1
Flight planning & approval	2	1	1	3
Noise reduction	2	2	2	1
Registration & Identification	2	2	2	2
Beacons to establish no-fly zones	2	2	2	2
Impact limiting devices	2	2	2	2
Drone circuits	2	1	3	2
Telecom networks to track drones	2	2	3	2
Safety requirements	1	2	2	2
Detection/tracking/logging	3	3	3	1
Air traffic management systems	3	3	3	1
Pollution reduction	2	3	3	2
Kill switch	3	2	3	3

Table 5.3   Technical measures sorted in order of ease of implementation

5.4   Easy-to-Implement Measures

Some of the measures presented in this chapter are relatively easy to implement.
We will indicate a few measures which can be implemented soon or which are
already being implemented.

5.4.1   *Limiting technical capabilities of drones*

For manufacturers it is very easy to limit the technical performance of a drone
through software measures. Many drones already have a feature that the pilot can
select such an option. Most recreational drone pilots would have no objection to
such a measure, because they will have better control of their drone; unexpected
behavior and large accelerations will not take place.

5.4.2   *Observability*
To increase the observability of drones by choosing the right colors, striping or by adding strobe lights, is quite straightforward. These features will hardly affect the performance of the drone. The impact of increased observability, however, depends on the specific situation. The measure is advocated strongly by airline pilot associations.

5.4.3   *Airspace division*
To declare different airspace layers for different purposes, is of course just a matter of regulations and legislation. If drones have to automatically obey these altitudes, a form of geofencing is required. The main objection against this measure might be to reach consensus about the necessity of it.

5.4.4   *Apps for sharing flight information and practice*
Apps for smartphones and tablets are being developed and offered at present. Initially, these apps have limited functionality, but they will have additional features being implemented at a rapid pace. They offer an ideal platform for communication of no-fly zones, for weather alerts, for education of drone pilots, for making flight plans, et cetera. A point of concern might be the responsibility for keeping actual the database of no-fly zones, if this responsibility is in private hands.

5.4.5   *Establishing no-fly zones*
In combination with access to internet, through apps or through websites, it has become quite easy for government authorities to declare and communicate no-fly zones. This information can be accessed by drone pilots at any moment through the Internet. As mentioned above, apps will greatly enhance communication about no-fly zones.

5.4.6   *Enforcing no-fly zones*
This measure is mentioned here, because it already has been implemented by the largest drone manufacturer DJI, which means that the other manufacturers may follow quickly. Some organizational effort is required, however, to have an official database specifying the permanent and temporary no-fly zones.

5.4.7   *Propellers*
The shielding of propellers is already quite common for a large number of drones, not only for protection people from getting hurt, but also for protecting the drone for getting damaged. The repercussions on drone flight performance are limited, much less than for instance an add-on parachute.

5.5   **Detailed Assessment of Geofencing/No-Fly Zone as Technical Measure**

No-fly zones are areas in which it is not allowed to fly for reasons of safety and/or security, such as airports and other prohibited areas. Geofencing is a technology to prevent drones to accidentally enter no-fly zones.

Geofencing roughly works as follows. The drone knows its position using the onboard Global Navigation Satellite System (GNSS), such as GPS. It also has access to a database that contains all no-fly zones. When a drone is flying towards a no-fly zone and reaches the border of the no-fly zone, it will not continue its flight

path. Instead it will stop, and may start hovering, may initiate a landing or do otherwise, as it is programmed to do.

The main advantage of geofencing is that it is very effective. It is regarded as an effective means to prevent drones (of ignorant users) from entering no-fly zones. Also, it has little or no negative effect on the flight performance. Notice, however, that geofencing can potentially be tampered with, and cannot stop drone users with bad intentions.

No-fly zones are often drawn on a 2D map as simple shapes (e.g. circles). However, notice that no-fly zones also involve an altitude and thus are 3D objects which can have any shape.
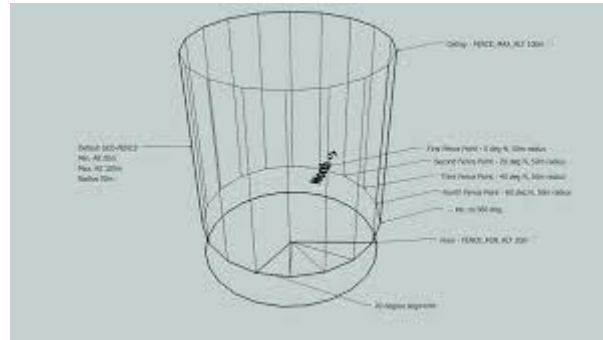
In current implementations, the no-fly zone database resides at the drone, and requires regular updates by the user. It only contains static objects, mostly airports. Current implementations are not intended to contain each and every prohibited area such as urban areas, critical infrastructure, stadiums, roads, etc. Also, they do not support temporary no-fly zones, such as during a special event or an incident. A well-known implementation of such no-fly zones for drones is featured by the DJI company, the largest seller of consumer drones (http://flysafe.dji.com/no-fly).

If dynamic no-fly zones are to be supported, a static no-fly zone database that resides at the drone is no longer sufficient. To support dynamic no-fly zones, instant update of the no-fly zone database is required. Also, to support each and every prohibited area such as mentioned above, a very large database is required.

In order to implement such complex system of no-fly zones, one requirement is to have a data service that dynamically provides the current no-fly zone information. One such service that has been announced is http://www.airmap.io/, which provides dynamic airspace information for various types of users. Note that the so-called Notices to Airmen (NOTAM) are the current means to inform the public and the professional community about the conception of temporary no-fly zones. The use of a data service drastically reduces the time to inform the users.

Taking a no-fly zone data service as a starting point, it can be envisioned that such a service can be used in different ways. It could be used to:
− inform users about the no-fly zones in their area, e.g. via a smartphone app or website;
− inform users when their drone approaches or enters a no-fly zone, e.g. via their control station;
− enforce that the no-fly zone is entered, using geofencing in a similar way as described above.

Option 1 puts no requirements on the drone (or control station). Yet it can be a very effective and highly useful way to inform drone users about no-fly zones. A well informed users makes better decisions. One example of such a smartphone app is the B4UFLY Smartphone App: http://www.faa.gov/uas/b4ufly.

Options 2 and 3 do put certain (strong) requirements on the drone (and control station). They require that the drone has a GNSS capability and that the drone (or control station) has a datalink capability (access to Internet) in order to access the no-fly zone data service. They also require that the data service is always available. Option 3 additionally requires that the no-fly zones are enforced in the drone's flight control logic.

Although several visions on the future of drones involve drones that are interconnected and have advanced communication capabilities (for example http://flylatas.com/) current drones do not have such capabilities. Also, apart from the DJI geofencing capability, no other implementation that enforces no-fly zones is known presently. Besides, it must also be considered that if the communication capabilities of drones increase, this probably also introduces new vulnerabilities. For example, if drones become more connected they could potentially be hacked or hijacked easier.

In conclusion, it can be stated that geofencing using a limited set of static no-fly zones could be an effective means to achieve that (ignorant) drone users do not fly in these no-fly zones. However, it would already be quite a strong requirement to mandate such no-fly zones for every drone as not every drone has a GNSS and the no fly zones need to be implemented in the drone's flight logic. Instead, informing users of the existence of no-fly zones using a website or smartphone app is considered a possibly effective means that is achievable on a relatively short term. Mandating the enforcement of no-fly zones, i.e. dynamic no-fly zones and each and every prohibited area, is considered too strong a requirement for the short term.

5.6 Detailed Assessment of the 'Kill Switch' as Technical Measure

5.6.1 Introduction

In this document a kill switch is defined as the possibility to remotely control a drone from the outside by a third person, not being the drone operator. The kill switch command must override the command and control as issued by the operator. While the purpose of a kill switch is to enable law enforcement authorities to control a drone carrying out suspicious or unlawful activities, the functionality of the kill switch shall depend on its intended use. For instance, a kill switch may force a drone to land, return to home or stop the engines forcing the drone to crash after entering a no-fly zone.

The ability to use a kill switch shall exclusively be given to law enforcement authorities; not only does this require the cooperation of manufacturers to create a 'backdoor' through which the control signal of the kill switch can override all other control signals. There are also challenges when it comes to enforcing kill switches on drones that are already sold, or are imported from countries where legislation does not enforce the use of kill switches. Standardization of kill switch schematics across countries could provide a partial solution to the latter problem.

The application of the kill switch may take effect directly on the drone and/or on the drone ground control station of the operator. However, such a kill switch requires a sophisticated security system; otherwise skilled hackers may use the same backdoor to control other people's drones. Furthermore, by adding the functionality of a kill switch, this also introduces the risk of the kill switch intervening unintentionally during flight.

5.6.2   *Physical security recommendations*
A physical security recommendation that may lower the risk of failure to intervene is to design the mechanism with security by isolation and security by design principles in mind. Following the above principles, the kill switch shall be implemented as a physically separated system. The reason for this becomes apparent in case of a fly-away. The definition of a fly-away is loss of control, generally attributed to a failure of the radio link-up between the radio control transmitter and the receiver on the aircraft. When the drone is not responding to radio control signals, the kill switch may not work as intended when it is operating on the same system or on the same frequency band. This separate system shall operate on a different frequency and shall be shielded to lower the risk of interference and jamming attempts. Attackers may possibly try to record the kill signal, store it and replay the kill signal for malicious purposes. As a countermeasure, it is important to apply strict delay times. This significantly reduces the chances of possible replay attacks.

5.6.3   *Tamper resistance and tamper evidence*
The kill switch shall be tamper resistant and leave evidence once a tampering attempt has been made. For instance, when a drone is turned on, it performs a series of pre-flight checks, to see if all components are working as expected. A technical measure that may be implemented is to check before take-off whether the kill switch has been tampered with. If this is the case, the drone may refuse to take off and signal that the drone has been tampered with using for example its LED indicators.

5.6.4   *Secure communication recommendations*
After examining the physical security of the kill switch, this paragraph focuses on the communication link between the lawful interceptor and the drone and/or ground station. Implementing a low latency communication link with a high update rate of positioning information ensures that the drone can react almost instantaneously to the kill signal. A mechanism should be implemented such that the kill switch can distinguish between the genuine kill signal from a lawful interceptor and possible fake information from an attacker. Verifying signatures prior to establishing a connection, integrity checks and the use of strong cryptography that is properly implemented are possible solutions to this problem. From the outside, the lawful interceptor may prevent or disallow others from using the frequency range of the kill switch. It is important to fortify the system of the lawful interceptor as well. Consider separating the system from other parts of the network and secure according to best practices (NSA[15] , SANS[16] , NIST[17]) Specifics regarding the design and

---

[15] https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/

[16] https://www.sans.org/media/score/checklists/linuxchecklist.pdf

[17] https://web.nvd.nist.gov/view/ncp/repository

architecture of the kill switch should remain secret and shall only be supplied on a need to know basis.

5.6.5 Overview

Next table gives an overview of technical measures regarding kill switches for drones, for instance to enforce no-fly zones.

Table 5.1   Kill switch solutions

Technical Measure	Intended Function	Pros and cons
Kill switch, hardware solution	Shut off motors, resulting in crashing the drone	+ in principle works with all new drones + works when regular frequency range is denied. + works when drone is not responding - challenge to persuade operators of older models to implement kill switch - risk of kill switch intervening unintentionally during flight - backdoor may be used for malicious intent
	Take over control, land	+ full control + non-destructive + possibility to secure forensic evidence - generic module, needs however to interface with flight controller. - cooperation needed of manufacturers - backdoor may be used for malicious intent - possible delay time
	Return to home	+ removes threat from no-fly zone + (semi)real-time + operator friendly - limited forensic evidence - cooperation needed of manufacturers - return to home position may be altered during flight - backdoor may be used for malicious intent
Kill switch, software solution	Shut off motors, resulting in crashing the drone.	+ no physical adaptation of drones + no cooperation needed of operators + can be easily updated + can be used for some older models. - may fail when drone becomes unresponsive - risk of kill switch intervening unintentionally during flight - backdoor may be used for malicious intent
	Take over control, land	+ full control

		+ non-destructive
		+ possibility to secure forensic evidence
		- may fail when drone becomes unresponsive
		- cooperation needed of manufacturers
		- cost to develop modules for non-cooperative manufacturers.
		- backdoor may be used for malicious intent
	Return to home	+ removes threat from no-fly zone
		+ (semi)real-time
		+ operator friendly
		- may fail when drone becomes unresponsive
		- limited forensic evidence
		- cooperation needed of manufacturers
		- return to home position may be altered during flight
		- backdoor may be used for malicious intent

5.7 Detailed Assessment of Traffic Management as Technical Measure

5.7.1 *Introduction*

When operating drones there is the risk of in-air collisions. Obviously this is a concern for 'regular' aviation but with the foreseen increased operation of drones there is an additional risk of in-air collisions between drones. Note that weather conditions also play a significant role in the control of a drone. To lower the risk of in-air collisions it would be beneficial to obtain a complete aerial picture of drones and other aircraft flying in a specific 3-dimensional geographic area. When it is known where drones are present in the air, even if not allowed or without permission, one can take evasive actions such as diverting a plane or drone.

Specifically Amazon and Google advocate more 'order' in the airspace since they intend to use drones intensively and obviously like to reduce risks regarding in-flight collisions (mainly foreseen with other drones). Amazon has proposed to subdivide the airspace in specific layers, see earlier in this chapter). NASA is working on an Unmanned Aircraft System (UAS) Traffic Management (UTM) (see http://utm.arc.nasa.gov), that is aimed at enabling civilian low-altitude airspace and unmanned aircraft system operations by establishing an infrastructure for safe management of low altitude operations. Such a system could be complemented by human operators, to oversee the automatic traffic management system.

5.7.2 *Technical measures*

There is a number of technical measures that can help to establish an aerial picture of flying drones to enable an air traffic management system.

A detection network of one or more sensors can be used to detect drones within a certain geographic area. The most universal implementation would be a sensor network that is capable of detecting any kind of drone. For instance, radar and/or

optical sensors might be used. Yet, technically this might not be easy to implement for all kinds of drones. A drone can be quite small and move at a high speed. Buildings and obstacles may shield the presence of a drone. The advantage, however, is that no technical adjustments to drones, nor cooperation of the drone operators, are necessary. The drone is in this sense passive. Note that a detection network is not limited to sensors positioned on the ground. Sensors can also be fitted to drones and/or airplanes and used stand-alone or networked (exchanging sensor information between different parties either directly or indirectly).

To ease detection of drones by a sensor network one could fit drones with a transponder similar to, or identical to, the transponders used in regular aviation. The transponder would periodically transmit identification and possibly position/heading of the drone. The sensor network would be composed of sensors that specifically can pick up the transponder signals and derive the transmitted information. From this collected information an accurate aerial picture can be established if all drones are fitted with transponders. While the sensors to receive transponder signals might be easy, or easier, to implement, it requires that drones are fitted with a transponder. The drones therefore have to be active and their transponders should transmit genuine and accurate information. Note that the ADS-B transponders used in regular aviation do not have any security features that for instance guarantees the integrity and accuracy of the information transmitted by the transponder. Depending on the range of the specific transponders fitted in drones, a rather dense network of sensors might be needed. A transponder fitted in a drone will use up some of the energy budget of the drone by adding size, weight and power consumption. A possible drawback of fitting all drones with transponders is the congestion of the frequency spectrum. This may lead to ineffective and incomplete detection of all drones present in a certain part of the airspace.

Instead of fitting drones with transponders, a drone, or its operator, could actively 'push' the drone's identification and position information via Internet to a server (through a WiFi connection or through 3G, 4G or 5G cellular networks). The advantage obviously is that there is no need for a sensor network. Yet, it is expected that the pushed information will be less real-time than when using a sensor network. Furthermore, a server on Internet might be vulnerable to Denial-of-Service attacks or the server might at some point even be compromised. Also Internet connectivity with sufficient bandwidth and low latency is required to be able to push the flight information of the drone to the server.

If the drone is fitted with a capability to directly connect to cellular networks (3G, 4G, 5G), it not only can actively send information to the network, but its position may also be determined by triangulation through the cellular network send and receive masts.
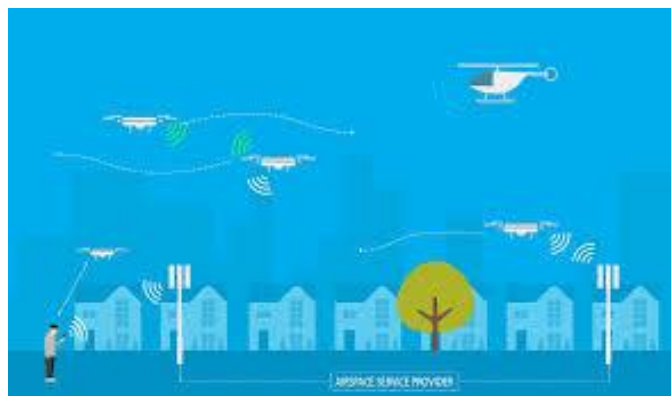
To counter the disadvantages mentioned above, drone operators can submit their intended flight plan to a server before starting the actual flight. No real-time Internet connectivity is needed in this case and the drone operator could get feedback regarding the flight plan for instance if and when the intended flight crosses no-flight zones. The interpretation of the flight plan and feedback regarding possible issues could be fully automated. No requirements regarding the drone are necessary but obviously there is no enforcement of the submitted flight plan. The drone operator might in the end simply fly not at all or fly somewhere else due to circumstances.

The overall idea of establishing an air traffic management system is that the air picture is built up through a number of different sources (detection, transponders, flight plans, apps, et cetera), which ensures a redundant and reliable system. Even so-called non-cooperative drones, aircraft without for instance a transponder, could be localized through various means of detection.

5.7.3 Overview

The next table gives an overview of possible technical measures to help establish an aerial picture regarding drones and thereby helping to improve air safety and reduce the risk of in-air collisions with drones.

Table 5.4   Overview of different implementations of technical measures

Technical measure	Pros and cons
Detection network, passive drones	+ in principle works with all drones + no adaptation of drones + no cooperation needed of operators + real-time - sensor complexity - sensor detection capability - size of sensor network
Detection network, active drones	+ sensor complexity + could be compliant with regular aviation + real-time - drones to be fitted with transponder - drone performance due to transponder - possible congestion of transponder frequency spectrum - integrity and accuracy of information
Aerial picture server, pushing drone position information	+ limited ICT complexity - real-time network connectivity drone-server - cooperation of operator - integrity and accuracy of information
Aerial picture server, pre-flight plan submission	+ limited ICT complexity + can provide feedback to operator + no real-time network connectivity needed + works with any drone - cooperation of operator - integrity and accuracy of information

6 Law enforcement

Legislation and regulations in the area of flying drones are important in the light of a rapidly changing technological capability. At present, the Netherlands has a first set of rules for flying drones, issued mid-2015. It is foreseen that legislation and regulations will be updated in a few consecutive steps, directed by the developments and decisions taken in the European context.

By nature, legislation requires enforcement of the law, in case of breach. Most cases of breaching the law will be due to people not knowing the law or people not able to fly their drone in a controlled manner, resulting in unintentional breach of the law.

A second group of law breach consists of people breaking the law for the fun or the thrill and even posting videos of such actions on the Internet to show their audacious actions, or NGO's using drones in an unlawful manner to attract media attention, media to get high-value front page pictures (the benefits far more than the possible sanctions) et cetera.

A third group concerns the criminal use of drones, for instance for reconnaissance of an area for future crimes, for smuggling or for eavesdropping and espionage.

Last but not least is the use of drones for terrorist activities, using the drone to cause panic, to hurt people, or using specific payloads to achieve their purpose.

In all these cases, law enforcement authorities would like to enforce the law and stop the flight of drones in areas where it is prohibited. The conception of no-fly zones, possibly enabled by geofencing, certainly will keep away most of the drones, and in particular those drones that do not have an intent to break the law.

If geofencing does not work, other measures are required. In general, it is required to adopt an holistic approach. Depending on the situation, on the scenario and on the risks involved, a specific combination of measures may be employed to counter the illegally flying drone. Such a combination exists of detection, classification and identification techniques and techniques to 'attack' the drone. These can be subdivided into so-called 'soft-kill' techniques and 'hard-kill' techniques. The former techniques are various measures taken in the electromagnetic spectrum, such as jamming or spoofing the signals to the drone. The latter techniques are measures to physically disable or remove the drone from its position. An important factor to decide which techniques to apply, is the consideration whether collateral damage may be allowed or not. If a drone flies above a crowd of people, shooting it down may result in worse effects than chasing it away.

In general it must be noted that all techniques and measures of countering UAV's have their difficulties and deficiencies. Drones are difficult to detect, have an extreme agility and can be put in position in a very rapid manner. In addition, as countermeasures evolve, also counter-countermeasures are developing. Drones which navigate and fly autonomously, are difficult to counter using soft-kill techniques like jamming or spoofing.

It is outside the scope of this document to go into detail into techniques concerning countering drones. The government has set a course of action, led by the National Coordinator for Security and Counterterrorism (NCTV). It has issued an innovation competition, in which four companies were awarded a project to demonstrate C-UAS technologies. In addition, TNO has developed C-UAS technology for a number of years within the framework of R&D for the Ministry of Defense, which has led to a number of demonstrations of specific techniques.

For reasons of tracing and identification of drone pilots, a system of registration of drones might be introduced, like the one issued in the US by the Federal Aviation Administration.

In the EASA Technical Opinion [31] it is proposed that member states have to designate the responsible authorities for the enforcement of the regulations, in particular in the 'open' category where the recommendation is to rely on the law enforcement agencies.

7   CCTV Cybersecurity and Drones

This chapter discusses additional risks introduced by deploying drones fitted with a camera within/in combination with closed-circuit television (CCTV)[18] systems.

7.1   CCTV Systems

CCTV systems mostly consist, see Figure 7.1, of one or more cameras that can be monitored remotely. For instance video data of each camera is communicated, streamed, via a communication infrastructure to a, in general central, location where the video stream of each camera can be monitored and recorded. Initially, the video streams were communicated in an analogue manner, e.g. as a composite video signal. Modern CCTV systems are mostly digital and video streams from cameras are communicated in digital form, usually encoded by a video codec. Digital video streams have the advantage that they, for instance, can be transported over IP networks. Besides remote monitoring and recording, cameras can be also controlled remotely, e.g. zooming in/out or changing the direction of the camera.
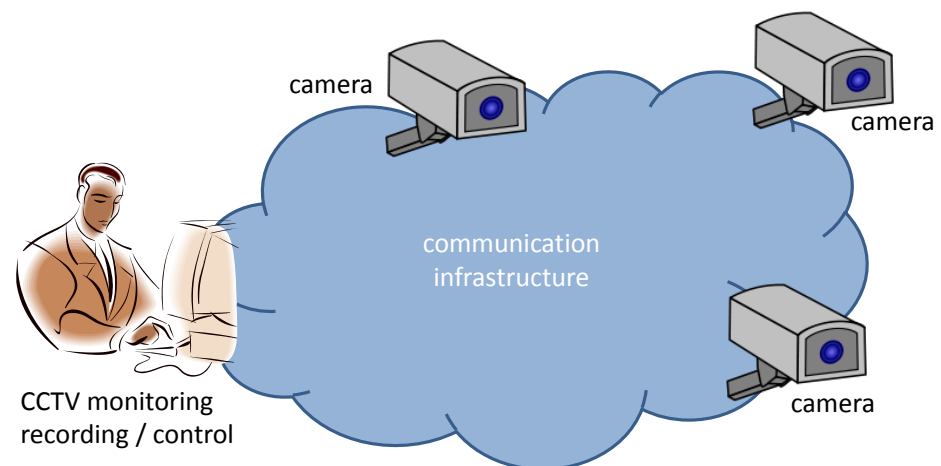
Figure 7.1 CCTV system overview

For current video surveillance systems the EN ISO 22311:2014 standard gives provisions for data/access security and integrity and for privacy. It specifies a common output file format. For this reason, it seems attractive to apply this standard also for drones which are part of a video surveillance system. However, this is not yet common practice.

7.2   CCTV Cybersecurity

Traditional CCTV systems use a communication infrastructure based on a fixed wired network installed in a physically secure environment, e.g. a building. Over the years however, the initially stand-alone CCTV systems have become networked and nowadays often have (sometimes unknown to the owner of the CCTV system) some kind of Internet connectivity. This connectivity could be limited to a single

---

[18] Another, more modern term for CCTV is Video Surveillance System (VSS)

connection, see Figure 7.2, or could be more extensive if Internet is being used as communication infrastructure, to which cameras are directly connected to, see Figure 7.3. Internet connectivity makes a CCTV system vulnerable to attacks from the Internet. An attacker could get access to, or manipulate, live/recorded video streams, take control over the cameras, or otherwise sabotage the CCTV system. NCSC has issued two fact sheets (see [37] and [38]) that provide a checklist and guidelines for technical as well as organizational measures to secure ICS/SCADA-systems (these include the CCTV systems discussed above).
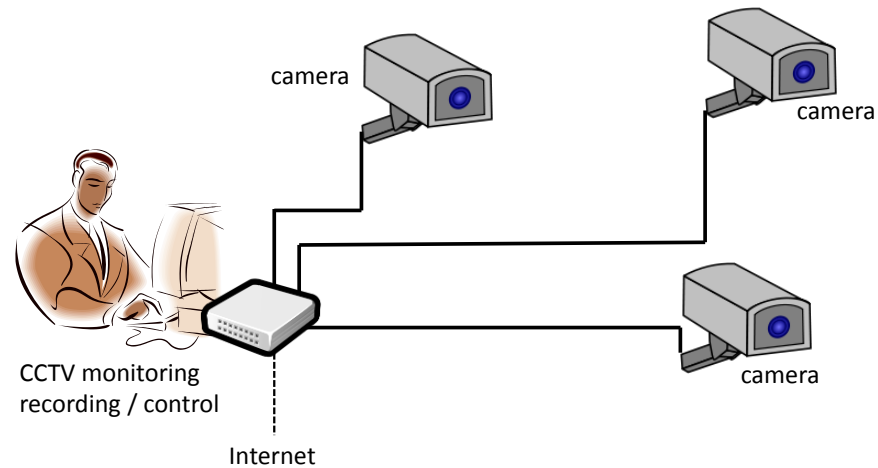
Figure 7.2 Networked CCTV system with Internet connectivity
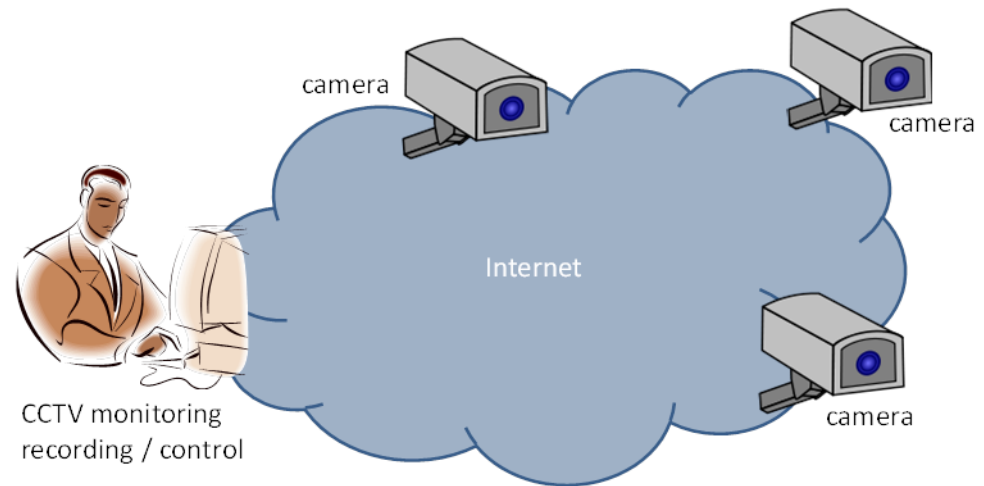
Figure 7.3 Networked CCTV system with Internet communication infrastructure

Measures to secure a CCTV system will be aimed at reducing the risks associated with (possible) vulnerabilities regarding the three main components within a CCTV system: the cameras, the communication infrastructure and the monitoring/control location.

7.2.1 Camera

A camera is vulnerable if it can be easily accessed physically. Therefore in general, measures are in place to prevent direct physical access to a camera, for example by the use of fencing or fitting the camera in a virtually inaccessible place. It is more difficult to prevent against "blinding" attacks[19] where a strong light source is pointed at the lens of the camera. If a camera is networked it might be accessible logically, possibly even from Internet. Unless it is certain the communication infrastructure cannot be accessed by outsiders, camera access control needs to be implemented in order to restrict access (control/video streams/software) to authorized users.

7.2.2 Communication infrastructure

The communication infrastructure for video streams and camera control is least vulnerable if a strictly wired communication network is used which is physically, and logically, completely shielded from possible attackers. Yet, this is usually not the case nor feasible. Sometimes it might not even be clear for the CCTV system owner how the connectivity between cameras and the monitoring location has actually been implemented, for instance if this connectivity is provided by another party. Since it is not easy to physically shield access to wireless communication, specifically the use of wireless cameras, see Figure 7.4, increases the vulnerability of the communication network to eavesdropping, disruption, and false packets. This also holds in case communication between cameras and the CCTV monitoring is routed via third-party networks such as the Internet.
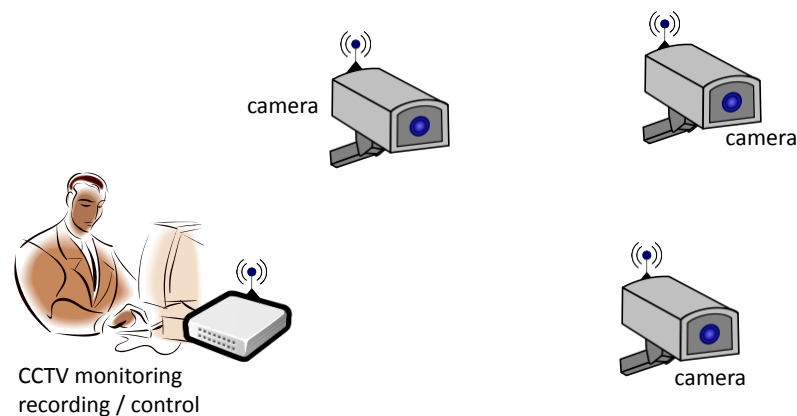
Figure 7.4 CCTV system using wireless cameras

Eavesdropping and falsification of traffic can be tackled by implementing end-to-end security between the cameras and the CCTV monitoring. This concerns the video streams as well as control signals. To prevent direct logical access of network components, i.e. the cameras and CCTV monitoring, network access control and encryption should be implemented. Yet, this cannot protect against network disruptions such as increased delays, packet loss, or even complete unavailability. Service Level Agreements (SLA's) could be used to limit such disruptions. Ultimately, a redundant communication network between cameras and CCTV monitoring could be a deliberate choice.

---

[19] Strictly speaking this is not a cyber risk.

7.2.3 CCTV monitoring

In case the location where CCTV video streams are monitored and stored for later reference has Internet connectivity, the CCTV system is vulnerable to attacks from the Internet and therefore direct access to any part of the CCTV monitoring facility as well the cameras should be prevented. There is little difference in this respect with generic measures, such as the use of firewalls, taken by organizations to protect their Internet-connected ICT systems.

7.3   CCTV Deployment of Drones

Drones fitted with cameras are already widely available and in the future it is expected that their reliability will be improved, their cost lowered and their functionality extended. One might expect that drones fitted with a camera will (or even currently already are) deployed as part of a CCTV system. Compared to a physically fixed camera, a drone can be easily and quickly deployed as well as positioned where desired or needed.

A CCTV system composed of drones with camera, see Figure 7.5, is comparable to a CCTV system using wireless cameras. The obvious difference is that a drone with camera can move around, either autonomously or under manual control.

drone with camera

drone with camera

CCTV monitoring
recording / control
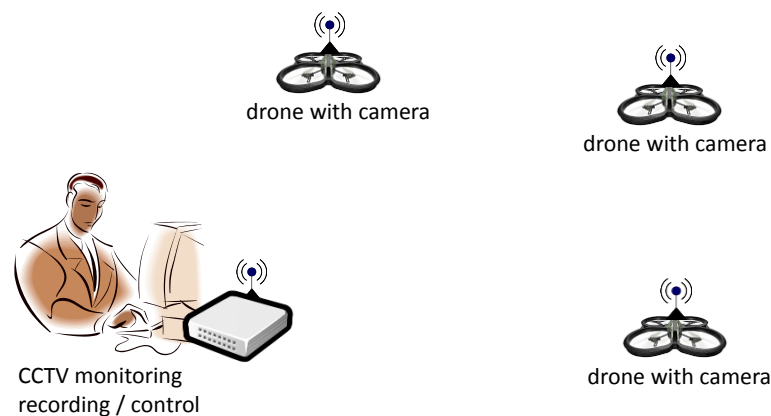
drone with camera

Figure 7.5 CCTV system composed of drones with cameras

Just as the introduction of Internet connectivity poses additional security risks to a 'traditional' CCTV system, using drones for CCTV will also yield additional security risks. Aspects that one has to be aware of in this respect are the limited operation time of a drone due to energy constraints, e.g. battery operation and the limited control over possible physical access of outsiders to a drone in case of operational failure.

The main issues regarding operation of a drone as CCTV camera are:
−   *Protecting the video stream*
     Just as a CCTV system with wireless cameras, the wireless video stream from the drone needs to be protected against eavesdropping or manipulation. Yet, to save energy video links from drones generally are not encrypted and thus vulnerable to eavesdropping. In order to be able to trust the video stream from a

drone camera measures have to be taken that facilitate verification of the authenticity of a video stream.

– *Different regulations*
Regulations apply to the placement and operation of CCTV cameras. A moving drone with camera might not meet applicable regulations under all circumstances, e.g. regarding privacy protection. Also other, additional, regulations will apply such as those regarding the safety of drone operation. A drone operator needs to be aware of possible restrictions and/or the drone should be programmed such that it will not violate any restrictions.

– *Control link protection*
A drone with camera is remotely controlled via a wireless control link and this control link needs to be protected against being taken over or disturbed by an attacker. Furthermore, the drone needs to be fitted with a failsafe mechanism that is activated when the control link is lost.

– *Limited operation time*
A drone with camera will need to return home before the end of its operation time and possibly needs to be timely relieved by another drone with camera to meet surveillance requirements of the CCTV system.

– *Operation time variance*
The operation time depends on various factors such as battery depletion, how the drone is operated, external factors (e.g. wind). It can be difficult to accurately predict the operation time. During operation of the drone battery usage and expected remaining operational time should be closely monitored.

– *Information inside drone*
Compared to cameras that are physically fixed, a drone is more suspect to fall in the wrong hands in case of an operational incident. An attacker could get access to, or even change, information stored in the drone. The amount of sensitive information stored in the drone should be limited and protected.

8 Conclusions and Recommendations

Based upon an extensive assessment of the literature, interviews with relevant stakeholders and experience from previous projects, an overview was made of issues related to the introduction of drones in the national airspace. The risks, associated with these issues were documented and discussed and a list of technical measures to enhance the safe and secure use of drones was conceived.

One of the risks identified, related to the loss of communication between the operator and the drone, was explained in more detail.

Those technical measures, that may be achieved at little effort and at short notice, were identified in specific:
- limiting technical capabilities of drones;
- observability;
- airspace division;
- apps for sharing flight information and practice;
- establishing no-fly zones;
- enforcing no-fly zones;
- propellers.

Three different technical measures, being the establishment of no-fly zones, the so-called kill switch and air traffic management were discussed in more detail.

In the area of drones, technology is developing in a very rapid pace. In addition, the number of drones sold annually, increases exponentially. It is hardly possible for the authorities to keep pace in establishing proper legislation and in enforcement of the laws. It is mandatory that all players in this area come up with and agree on specific measures to assure the safe use of drones in the national airspace. A number of measures to be taken is suggested in this report.

Due to the rapid pace of technology, it is recommended that a survey like this, be renewed and updated within one year.

We recommend that the government continues to have an active role in legislation and rulemaking discussions in the national and international arena. Cooperation with industry and users may be an effective path to standardization and certification.

With respect to risk assessment and risk mitigation, we recommend that quantitative risk assessment studies be carried out, which may serve as an unbiased source of information for policy making and safety requirements definition. If the government sets or adopts quantitative safety requirements (standards), industry will have a standard to adhere to. We anticipate that such a standard will also be required for insurance purposes.

All measures and recommendations proposed here, will be much more effective if taken in an international (European) context.

9   References

[1]   Kamerbrief 620345, 2 maart 2015, Minister van Veiligheid en Justitie, Staatssecretaris van Infrastructuur en Milieu, Minister van Economische Zaken.

[2]   *Miniature UAVs: an overview*, P.W.L. Weimar, J.S.F. Kerkkamp, R.A.N. van de Wiel, P.P. Meiler, J.G.H. Bos, TNO, 2014.

[3]   Kamerbrief *Regelgeving voor drones*, IENM/BSK-2015/87396, Staatssecretaris van Infrastructuur en Milieu.

[4]   *Het gebruik van drones – een verkennend onderzoek naar onbemande luchtvaartuigen*, B.H.M. Custers, J.J. Oerlemans, S.J. Vergouw, Wetenschappelijk Onderzoek- en Documentatiecentrum, Ministerie van Veiligheid en Justitie, 2015, Boom Lemma uitgevers.

[5]   *Informatie over toezeggingen AO Drones*, kamerbrief 708413, Ministerie van Veiligheid en Justitie, 2 december 2015.

[6]   *Drones en privacy, handleiding voor een gebruik van drones dat voldoet aan de waarborgen voor bescherming van de privacy*, Ministerie van Veiligheid en Justitie, 25 november 2015.

[7]   *Risk Analysis of UAV Operations in the Netherlands*, M.M. van der Voort, R.M.M. van Wees, Report TNO 2014 R10139 (Restricted), April 2014.

[8]   *The Real Consequences of Flying Toy Drones in the National Airspace System*, W. Hulsey Smith, Freddie L. Main III, Aero Kinetics Aviation, 2015

[9]   *Airborne threats of low level Remotely Piloted Aircraft System (RPAS)*, Vereniging Nederlandse Verkeersvliegers, March 2015.

[10]   *The RPAS 'Open Category' in EASA's Concept of Operation for Drones*, European Cockpit Association AISBL, 23 July, 2015.

[11]   *Close encounters of the drone kind*, Michael Peck, Aerospace America, November 2015.

[12]   *Safety Considerations for Operations of Different Classes of UAVs in the NAS*, R.E. Weibel, R.J. Hansman jr., Massachusetts Institute of Technology, AIAA-2004-6421 and AIAA-2004-6244, 2004.

[13]   *UAS Safety Analysis*, A. Dershowitz, Exponent Inc, December 16, 2014.

[14]   *Airborne threats of low level Remotely Piloted Aircraft System (RPAS)*, European Cockpit Association AISBL, 24 March 2015.

[15]   *Drones Take Flight – Key Issues for Insurance*, Emerging Risk Report – 2015, Lloyd's.

[16] *Riga Declaration on Remotely Piloted Aircraft (drones) 'Framing the Future of Aviation'*, European Union, Riga, 6 March 2015.

[17] *Advance Notice of Proposed Amendment 2015-10 – Introduction of a regulatory framework for the operation of drones*, European Aviation Safety Agency, TE.RPRO.00040-003, July 31, 2015.

[18] *Concept of Operation for Drones – A risk based approach to regulation of unmanned aircraft*, European Aviation Safety Agency, TE.GEN.00400-003.

[19] *Unmanned Aircraft Systems (UAS) Registration Task Force (RTF) Aviation Rulemaking Committee (ARC)*, Task Force Recommendations Final Report, November 21, 2015.

[20] *Registration and Marking Requirements for Small Unmanned Aircraft,* Federal Aviation Administration, RIN 2120-AK82, December 2015.

[21] *Final Report of NIAG SG-170 Study on Engagement of Low, Slow and Small Aerial Targets by GBAD*, Rob Munday, Report NIAG-D(2013)0015, July 2013.

[22] *Drone Sightings and Close Encounters: An Analysis*, Dan Gettinger and Arthur Holland Michel, Center for the Study of the Drone, Bard College, December 11, 2015.

[23] *Determining Safe Access with a Best-Equipped, Best-Served Model for Small Unmanned Aircraft Systems*, Amazon, 2015.

[24] *Autonomous Vehicle Technology – A Guide for Policymakers*, RAND Report RR-443-1, 2014.

[25] *Integration of civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, FAA, November 2013.

[26] *Beleidsvoornemen Veiligheidsregelgeving drones*, Ministerie van Infrastructuur en Milieu.

[27] *Beantwoording van de 7 vragen uit het Integraal afwegingskader voor beleid en regelgeving (IAK), Internetconsultatie Beleidsvoornemen Veiligheidsregelgeving drones*, Ministerie van Infrastructuur en Milieu.

[28] *Regeling van de Staatssecretaris van Infrastructuur en Milieu, van 23 april 2015, IENM/BSK-2015/11533, houdende de vaststelling van regels voor op afstand bestuurde luchtvaartuigen,* Staatscourant nr. 12034, 30 april 2015.

[29] *Besluit van 23 april 2015 tot wijziging van het Besluit bewijzen van bevoegdheid voor de luchtvaart, het Besluit luchtvaartuigen 2008, het Besluit vluchtuitvoering en het Besluit burgerluchthavens (regels voor op afstand bestuurde luchtvaartuigen)*, Staatsblad van het Koninkrijk der Nederlanden nummer 163, 2015.

[30] *Onbemande vliegtuigen (UAV)*, Brief van de Minister van Veiligheid en Justitie, de Staatssecretaris van Infrastructuur en Milieu en de Minister van Economische Zaken, brief 30806, 28 augustus 2015.

[31] *Introduction of a regulatory framework for the operation of unmanned aircraft*, European Aviation Safety Agency, Technical Opinion, TE.RPRO.00036-003, 18 December 2015.

[32] *Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council*, 7 December 2015.

[33] *Exploring Security Vulnerabilities of Unmanned Aerial Vehicles*, Nils Rodday, University of Twente, Master's Thesis, July 2015.

[34] *Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles*, Alan Kim, Brandon Wampler, James Goppert, Inseok Hwang, Hal Aldridge, AIAA.

[35] *The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment*, Kim Hartmann, Christoph Steup, 5th International Conference on Cyber Conflict, 2013.

[36] *On the Requirements for Successful GPS Spoofing Attacks*, Nils Ole Tippenhauer, Christina Pöpper, Kasper B. Rasmussen, Srdjan Čapkun.

[37] *Uw ICS/SCADA- en gebouwenbeheersystemen online*, Factsheet FS-2012-01, versie 2.1, Nationaal Cyber Security Centrum, Ministerie van Veiligheid en Justitie, 17 december 2015.

[38] *Checklist beveiliging van ICS/SCADA-systemen*, Factsheet FS-2012-02, versie 2.1, Nationaal Cyber Security Centrum, Ministerie van Veiligheid en Justitie, 17 december 2015.

10   Signature

The Hague, March 2016   TNO

E.W. Vos   P.J.M. Elands
Head of department   Main author

A   Interviews

A.1   Introduction

In order to obtain a complete and actual overview of as many relevant issues and risks as possible, associated with the use of drones in the Dutch airspace, a number of interviews was held with relevant stakeholders:

- Agentschap Telecom (Dutch Telecom Agency);
- National Cyber Security Center (NCSC);
- Vereniging Nederlandse Verkeersvliegers (VNV);
- Netherlands Forensics Institute (NFI).

It was anticipated to hold interviews with:

- Ministry of Infrastructure and Environment (I&M);
- UVS International;

but it appeared to be not possible to find a suitable moment in time. However, from a number of symposia and briefings, the main issues mentioned by both stakeholders at these occasions, will be highlighted here.

Where appropriate, possible technical solutions to enhance safety have been discussed during these interviews.

A.2   Interview with Geert Bondt (Agentschap Telecom)

An interview was held by telephone with Geert Bondt (Agentschap Telecom – Telecom Agency) on November 4, 2015. Geert works at the Security Department of the Agentschap Telecom (AT) and has responsibility for (the protection of) the frequency spectrum for aviation purposes. From TNO Jeroen Laarakkers and Pieter Elands were present.

Geert runs a special programme concerning drones; his working group is looking at the effects of the introduction of (large amounts of) drones in the Dutch national airspace on the radio spectrum and the measures the AT might need to take. His working group has contact with manufacturers with whom they had several site visits and the group has organized a working conference. From these contacts AT has got the impression that drone manufacturers hardly have thought about the use of the frequency spectrum and the possibility to request a specific part of the frequency spectrum for drones. The market is starting to get organized and is finding its way to the government; the government is starting to learn the needs of the market.

Geert indicates that presently airspace safety attracts a lot of attention, but AT is not concerned with that topic. The government does not (yet) have a single point of

contact for drones, although the Ministry of Security and Justice seems to be taking the lead.

An issue indicated by Geert is the possibility to allocate[20] a part of the frequency spectrum for use by drones. The market has not yet indicated to have a need for this, but this need might arise in the future.

Geert explains how the situation in the frequency spectrum with respect to the use of drones presently looks like.

5 GHz
In the international framework, already a long time ago, it was envisaged that unmanned aircraft need to be operated by remote control. At the World Radio Conference (WRC2012) a decision was taken to allocate a part of the radio spectrum (5030-5091 MHz) for Command and Non Payload Communication (CNPC). This part of the spectrum is only to be used for radio applications required for the safe and efficient execution of the flight itself. Use of this part of the spectrum is foreseen for networks on earth and for big unmanned aircraft transporting cargo and perhaps passengers in the future. There will be only serious use of this part of the spectrum on the longer term, however, when full integration of unmanned aircraft in the controlled airspace has been achieved. The frequency band, however, is not yet available for permanent allocation of frequencies, because technical standards and a so-called band plan still have to be conceived.

2300-2495 MHz
The National Frequency Plan (NFP) recently has been changed, allowing companies having a permit to use somewhat more power in the frequency band between 2300 and 2495 MHz, provided they adhere to the extra conditions coupled to the permit. Because at present drones have to fly in Visual Line of Sight conditions and at a safe distance from urban areas, no specific problems with other use are foreseen. This changes accommodates a need for frequencies for the payload; however, it is not considered to be a solid permanent solution.

The AT notices that within the near future, the use of small drones, making use of various different sensor types, increases rapidly. The data generated by these sensors and sent to the ground control station, cannot be sent through the 5 GHz band mentioned above. Presently, the permit-free part of the frequency spectrum is being used for this purpose, but it is unclear whether this part of the spectrum is and remains suitable for this purpose. AT is investigating this and expects more critical requirements for availability of the radio interface and from that the possible future demand for an exclusive frequency allocation for the payload. AT hopes and expects the market to pick up this issue.

Cybersecurity is a point of concern. It is hardly possible to protect against jamming; attention has given to good failsafe modes in case of jamming. Besides jamming, spoofing is considered as a real risk (for instance in the form of a replay attack), which should be countered with specific protection measures (such as time stamping). Also the data coming from the sensor need to be protected against

---

[20] Non-exclusively

eavesdropping. If standards are being developed, adequate cybersecurity shall be an integral part of the standard. Interfaces often form the weakest parts in security.

Another issue is the clarity of regulations. In some situations, it is unclear whether the aviation authorities (Ministry of Infrastructure and Environment), the security authorities (Ministry of Security and Justice) or the telecom authorities (Ministry of Economic Affairs) are in charge. According to current legislation, a drone with a mass less than 150 kg is exempted from EASA rules, which means that the radio equipment for the control of the aircraft falls under the Radio Equipment Directive. If EASA changes this limit to 0 kg, which is expected in the future, these small drones fall under aviation legislation and is a different authority responsible for the technical requirements for the radio equipment.

Another issue concerns the possible use of transponders for every drone. If every drone is going to transmit its position and its identity, the risk of congestion of the spectrum comes up. Presently, this problem is already arising with the use of ADS-B, together with the issue of shadowing (unwanted reflections). Specific technical solutions, such as selective questioning and answering, are required.

A possible solution is to simultaneously use various different networks (WiFi, 4G, 5G, etc.) to get a complete air picture, without congesting one specific part of the spectrum. A disadvantage, however, is that if a single drone should be able to broadcast at various different networks, this requires a complicated architecture. Identification of a drone by means of a built-in chip seems an option, for instance using a short range RFID chip or a high-power RFID chip.

Another issue concerns the control of drones through public telecom networks (4G, 5G). It is difficult to oversee all aspects and consequences of this form of control. It might be more difficult to track and trace the operator, because he may be at a much larger physical distance. A secondary effect might be the ever increasing number of applications making use of the telecom networks, possibly leading to an overload in times of crises. Who is responsible for sufficient capacity?

If drones are going to use sensor systems, which emit electromagnetic radiation, such as radar, it may have an effect on the availability of sufficient frequency spectrum, depending on the number of drones and the power and bandwidth they use.

Geert considers geofencing as a good solution. Using separate beacons to warn a drone pilot that he is approaching a no-fly zone is a good option. And to counter drones whose pilot does not want to obey the no-fly zones, active measures should be at hand of the authorities.

Geert expects the aviation authorities to pursue further standardization and introduction of new technologies to increase safety, in close cooperation with industry. If the government stimulates the use of 'safe drones', the public demand will increase and industry will start to produce. The bigger the concern about airspace security, the faster this development will be.

A.3 Interview with Diederik van Luijk (National Cyber Security Center)

The interview with Diederik van Luijk of the National Cyber Security Center was held by Jeroen Laarakkers and Pieter Elands at November 3, 2015. Diederik is cybersecurity analyst at the NCSC.

In cybersecurity the principles of availability, integrity and confidentiality are considered as a standard when looking at digital data. Availability primarily concerns the robustness and availability of the control signals from the ground control station to the drone, integrity concerns both the control signals to the drone and the data feed from the sensors and confidentiality concerns privacy aspects and the security of data. With these principles in mind, Diederik sees the following issues concerning the use of drones:

1. protection of the control signals of the drone;
2. protection of the data stream from the sensor systems of the drone;
3. protection of the drone software against the insertion of malware;
4. protection of the software of the remote control of the drone against insertion of malware;
5. the use of drones equipped with jammers;
6. the use of drones which insert malware in other drones.

If, for one reason or the other, security gets compromised, the following risks/threats may occur (related issues between parentheses):

− jamming or spoofing of the control signals of the drone (1);
− relay attack (man-in-the-middle) (1);
− replay attack (1);
− jamming or spoofing of the data feed from the sensors of the drone (2);
− breach of privacy, having impact of the personal life of individual people (1,2);
− third persons, possibly with bad intentions, get insight in the data recorded by the drone (2);
− a so-called 'botnet' of drones (make a distinction between control by WiFi and control by 3G, 4G, 5G) (3);
− manipulation of autonomous control by the drone (3);
− manipulation of the remote control (4);
− all thinkable forms of criminal and terrorist behavior using drones (5,6).

With respect to possible technical measures, the following items have been discussed:

− encryption of radio signals should always be applied, taking the additional cost for granted;
− there is hardly any protection possible against jamming;
− it is desirable that a drone can detect if a (control) signal is compromised, for instance in the form of a replay signal; in case of near real-time applications, this becomes more difficult;

    − it is important that a drone in case of loss of link or in case of detection of spoofing has a robust failsafe which can be executed autonomously; the autonomy software should be certified;

    − it shall be impossible to provide a software update to a drone by remote control; a hardware connection shall be made in all cases;

    − firmware and updates should be 'signed' (identifiable);

    − access to the drone control system could be controlled by a unique personal key, especially for professional use; watch however, for fraud;

    − equipping a drone with a transponder, broadcasting identity and position seems a good measure; its feasibility however, is not clear yet;

    − the regulation/control of the supply chain of drones seems quite impossible;

    − the mandatory installation of a kill switch (back door) is not a good option; the risks of misuse (such as DDOS attacks) are for more severe than the benefits;

    − it is desirable to be able to detect, classify and identify each drone, this may be facilitated by technical features applied to the drone;

    − create consumer demand for 'cyber-secure' drones, which are protected against the most common cyberattacks;

    − introduce type certification for drones, with increasingly severe requirements for larger and professional drones.

Diederik indicates that it might be worthwhile to use the lessons learned from internet cybersecurity and from the protection of 3G, 4G and 5G telecom networks, in particular because drones will be more and more using those.

Diederik cites two references:

    − *Autonomous Vehicle Technology – A Guide for Policymakers*, RAND [24] ;

    − *Integration of civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, FAA [25]

Diederik explicitly mentions the rapid pace of technology development and its effect on the issues mentioned above, risks and technical measures. The present insights most probably will be valid only for a limited period of time.

A.4   Interview with Wouter Houben and Jeffry Aenmey (Vereniging Nederlandse Verkeersvliegers (VNV))

An interview was held on Friday, November 20th, with Wouter Houben and Jeffry Aenmey of the 'Vereniging Nederlandse Verkeersvliegers (VNV)', the Dutch Association of Airline Pilots. The aim of this interview was to assess issues and risks associated with the introduction of drones in the Dutch airspace, from the point of view from the VNV. From TNO Jeroen Laarakkers, Pieter Elands and Anna Günzel participated in the interview.

The VNV refers to two publications, which clearly point out the position of the VNV with respect to this topic [9] [10] :

    − 'Airborne Threats of Low Level Remotely Piloted Aircraft Systems (RPAS)', position paper for the VNV, March 2015;

– 'The RPAS 'Open Category' in EASA's Concept of Operations for Drones', European Cockpit Association, July 2015.

The VNV is concerned about airspace safety, in particular about a possible collision between a small RPAS and a manned aircraft. More in particular, RPAS are considered as a threat for helicopter operations, for operations near airports and for areas where low level flying is allowed. The threat concerns the ingestion of a small drone in a jet engine, which is considered to lead to an engine failure or worse and the collision of a small drone with the main rotor, tail rotor or glare shield of a helicopter, inflicting fatal damage. Special attention is required for operations in the area of the North Sea, because a relatively large amount of manned aircraft traffic occurs in that area, such as helicopter flights to offshore platforms. In addition, at some point national airspace stops and international airspace commences. Some form of conformity seems desirable.

VNV is worried about legislation lagging behind reality and about little effort by law enforcement authorities to detect and act on drones flying in restricted airspace. The so-called Open Category concerns drones which can be bought commercially by the public. There is a lot of innovation going on in this category, generating more and more capabilities for drone users. The concern of the VNV is that people buy such a drone and go fly it, without knowledge of its possibilities and potential and without knowledge of the rules, and unintentionally create hazardous situations.

The VNV is less worried about drones flown by professional users, since they have already shown sufficient awareness and concern about airspace safety.

For the specific measures proposed by the VNV, to enhance safe flight in the Dutch airspace, the reader is referred to the publications.

Furthermore, the VNV urges that the authorities execute proper risk assessment on the introduction of drones in the airspace. Little is known about the possible effects of collisions between drones and manned aircraft; this needs to be assessed in more detail. The Ministry of Infrastructure and Environment just has erected a Project Group to address this issue. In addition, the government has started a campaign to inform the public of the risks associated with flying drones, a fly-safe campaign.

As a bottom line, due to the existing safety risks for manned aviation, the VNV is opposed to drone flights in the Open Category, unless proper measures have been conceived and written down in legislation and are being enforced by the authorities.

A.5   Interview with Zeno Geradts (Netherlands Forensics Institute (NFI))

Present: Zeno Geradts (NFI), Boyd Timmerman (NFI - intern forensic investigation), Jeroen Laarakkers (TNO), Klaas Jan de Kraker (TNO), Anna Günzel (intern TNO). Zeno works as a senior forensic scientist at NFI. In this role, he is responsible for building sufficient forensic investigation expertise for (remains of) drones.

Gathering of forensic proof

NFI could be requested to look into (the remains of) drones to gather forensic proof in criminal law investigations, mainly to determine who owns the drone (identification of the driver). This can be achieved by "classic" forensic investigation of remains, for example using DNA residues, but also by investigating the drones' flight data.

Currently, the NFI does not have significant 'drone practice'. This type of investigation should now take place as 'ordinary' investigation:

- investigation of the remote control; this is often a smartphone (if available);
- investigation of the available chips in the drone (route of the drone, identification, etc.);
- investigation of the drone itself (type, serial numbers, etc.).

Through one of the chips for example, flight data of the last 20 flights could be provided. One of the problems here could be that explicit user permission should be granted via the remote control to share the flight data, while the remote control is not always available. The chip can be looked into directly, but the flight data is usually encrypted. Therefore, the NFI prefers to have remote control on hand.
It would help the NFI if the data are stored in a standard format. Until now, each drone manufacturer uses its own formats, what cripples or makes forensic investigation inefficient.

Risks of drones
Meanwhile, Zeno made a first start with the identification of the drones from a forensic perspective, but these activities should be demand driven. A few brainstorms were organized. Zeno classifies the use of drones for terroristic purposes as a possible risk. Drones are identified as a topic the NFI must build up forensic knowledge in, but this is just an average priority. So far, standard digital research seems to be satisfactory; for NFI a drone is no 'special' digital device. Linux is commonly used as Operating System (that is used in drones) and there are less specific commercial forensic tools available. The only specific feature of drones from this perspective is actually the 'third dimension'; they can fly everywhere, for example over and around buildings, possibly bringing other offences with it.

Using transponders would improve the implementation of a standardized identification, to help the forensic investigation. Vehicles already have a Vehicle Identification Number (VIN). A similar solution could be a complementation for drones. Such a serial number, completed with a solid administration would be appreciated from the forensic perspective. This option should at least be applied in Europe. Only application in the Netherlands would not make much sense.

Finally, Zeno mentioned that the time of forensic investigation could be drastically decreased in case of an admission for drones, where the use of drones would be regulated, for example through a registration system.

Collaboration with third parties
The NFI has a research commission for forensic traces of drones paid by the police.

Summary

From the NFI perspective, particularly the gathering of forensic proof is relevant through connecting the drone to the pilot of the drone (identification).
Zeno finds that the following points are of interest:

– Standardization regarding storing of flight data;
– Standardization of identification numbers and administration, resembling VINs;
– Admission for drones according to a registration system.

A point is that criminal users can easily build their own drones of single components.

A.6 Issues Presented by the Ministry of Infrastructure and Environment

Within the time frame available, it was not possible to arrange for an interview with Ron van de Leijgraaf of the Ministry of Infrastructure and Environment, Department of Airspace Safety. His department is primarily concerned with airspace safety, accompanying legislation and communication. Recently a public information campaign was started, to inform people who buy and fly drones about the dos and don'ts. In addition, his department is concerned with the establishment of special areas for testing and flying drones for R&D purposes, for instance drones which are used for professional purposes, but which have not been certified yet. A number of places in the Netherlands is considered for such purposes, amongst which Twente Airport, Woensdrecht Airport and Valkenburg Airport.

A.7 Issues Presented by UVS International

Although it was not possible to arrange for an interview with Peter van Blijenburgh of UVS International, within the available period of time, we used the information he presented at the 'Werkconferentie Drones' organized by the NCTV on May 28 of this year and at the TU Delft RPAS Symposium on December 10 of this year.

UVS International[21] represents 25 national RPAS associations in 23 countries and is involved in all relevant international initiatives with respect to the safe use of RPAS in the airspace. These initiatives involve legislation and regulations, but also projects to develop technologies required for safe operation of RPAS.

From his presentations, we have summarized the following issues:

– it is necessary to have RPAS autopilots validated, to be sure they do not steer the drone in an unexpected manner; UVS International has taken the initiative for the conception of the RPAS Autopilot Validation Tool (RAVT), a tool to assess the safety of drone autopilots;
– electronic tagging of drones is required to be able to identify the drone (liability, law enforcement) and its actual position (airspace safety);

---

[21] http://uvs-international.org/

- insurance companies will in the future have an important say in safety requirements and certifications;
- certification of drones should cost at maximum € 4000,- to stimulate SMEs to develop new drones;
- geofencing is a useful means to increase airspace and ground safety; its operation should be added to the RAVT;
- although flight schools may help to increase the flight skills of drone pilots, the certificates they issue have no formal value;
- UVS International proposes that a promotional organization be started, consisting of industry, R&D organizations and governmental organizations to enhance and stimulate technology development and proper legislation and rules.

A.8 Concluding Remarks

The different stakeholders we interviewed have different views and positions with respect to the use of drones. For those stakeholders that experience a large possible impact of the use of drones on their businesses and operations, the concern is much bigger. In general, we think that issues to do with safety, which could lead to (fatal) accidents require the highest priority to be taken care of.

Another important observation has to do with risk perception. A risk is defined as an event (usually an unwanted event) that may occur. The severity of a risk is the product of the probability of the event and the impact of the event, if it occurs. For most of the risks, mentioned in the interviews, there was little or no knowledge about the probability and the impact, making the perception of risks a very subjective issue. As an example, the probability of a drone hitting a commercial airliner has not been assessed yet in an objective study, and in addition, the impact of a drone hitting a commercial airliner is not known very well either. Some studies argue that this impact is less severe as impact by a bird; other studies conclude the opposite [8], [9], [10], [11], [12], [13] and [14]. We strongly recommend a thorough integral risk assessment study, to be able to distinguish between the real risks and the risks which are only perceived as such, but that are not real risks. Due to the multidisciplinary nature of the risks associated with the use of drones in the national airspace and the various different stakeholders with different interests, a multidisciplinary (integral) risk approach is mandatory. In Chapter 5, this issue is addressed in more detail.

From the interviews in the previous paragraphs, from discussions with other stakeholders in the past and from various publications on this subject, we notice that the different issues related to drones, such as airspace safety, privacy, ground safety are taken care of by various different government entities. In a worst case scenario this could lead to contradiction in requirements.

For this reason we suggest that the government takes the responsibility to establish a one-stop government office or entity, which addresses all issues related to drones, both for civilians as well as for professional users.

The interdepartmental working group on UAV's is an excellent vehicle to exchange information and to discuss policy between the various players within the government, but it does not serve (yet) as a one-stop shop entity for people outside the government.

Another issue to be tackled by the government is that of risk assessment and risk acceptance. The risks associated with the use of drones in the national airspace are not very well established yet; at best some qualitative picture is available, but not a quantitative risk assessment. And as a consequence, the government has to set an acceptable level of risk, such as the probability of a lethal accident caused by a crashing drone. This gives users and manufacturers of drones the right guidance to design, develop, build, test and certify their drones.

In the EASA Technical Opinion [31] it is proposed that operators of unmanned aircraft carry out a so-called specific operation risk assessment (SORA), to be approved by the National Aviation Authority (NAA) of Qualified Entity (QE). It also proposes that industry and standardization bodies come with standards to address risks. In our opinion addressing of risks and development of standards for risk assessment require an initiating and guiding role of the national and international authorities.

B   Slides per Issue

AIRWORTHINESS

Description

› airworthiness of drones and certification of drone pilots are considered important requirements for enabling drone flights that are performed safely

Risks

› this issue relates to issue 'airspace safety' and to issue 'safety on the ground' and hence to the risks mentioned in relation to those issues
› risks: 1,2,3,4,5,6,7,12

Stakeholders

› drone regulation authority
› drone manufacturers
› drone users
› insurance companies
› drone certification authority
› flight schools

EVOLVING CAPABILITIES OF DRONES

Description

› The capabilities of drones are evolving quickly; it is possible that in a short period of time, new (safety) capabilities become available, possibly even capabilities that are currently not foreseen

Risks

› this issue may have both a positive and a negative effect on all risks identified
› a consequence of this issue might be legislation lagging behind (which is not a risk as such)
› risks: all

Stakeholders

› drone regulation authority
› drone manufacturers
› drone users

UNPREDICTABLE BEHAVIOR

Description

› currently drones are flown using a remote control, but autonomous flying also occurs, making use of waypoints, follow-me and failsafes
› one expected future technology development is that drones become more autonomous
› in certain situations their flight behavior could become unpredictable and hence potentially dangerous

Risks

› this issue relates to issue 'airspace safety' and to issue 'safety on the ground' and hence to the risks mentioned in relation to those issues
› risks: 1,2,3,4,5,6,7,12

Stakeholders

› drone manufacturers
› drone users

PRIVACY INFRINGEMENT

Description

› In the perception of many people the most prominent issue with drones is infringement of privacy
› most drones carry a camera and hence they can make video recordings of people, also in private places
› the people recorded not always notice that they are recorded, and if they do, they have no means to counter this privacy invasion

Risks

› privacy infringement
› risks: 8

Stakeholders

› civilians
› law enforcement
› drone users

ESPIONAGE USING DRONES

Description

› drones could be used for espionage, i.e. for observing commercial enterprises or government agencies and for stealing valuable information
› this results in economical damage and security breaches

Risks

› economic damage
› security breach
› risks: 9,10

Stakeholders

› commercial enterprises
› government agencies
› law enforcement
› drone users

VULNERABILITY TO JAMMING, SPOOFING, HACKING, EAVESDROPPING

Description

› drones have several digital vulnerabilities, for example:
  › the control signal could be jammed, spoofed or hacked, which could lead to loss of link
  › the GPS signal could be jammed or spoofed
  › the data downlink signal could be eavesdropped
  › the drone could be hacked or bugged

Risks

› this issue relates to issue 'airspace safety', to issue 'safety on the ground', to issue 'privacy infringement' and to issue 'espionage' and hence to the risks mentioned in relation to those issues
› risks: 1,2,3,4,5,6,7,8,9,10,11,12

Stakeholders

› civilians
› law enforcement
› drone manufacturers
› drone users

FREQUENCY SPECTRUM

Description

> If the number of drones increases too much, or other equipment that uses the same frequencies consume too much bandwidth, frequency bands may get full

> as a consequence drone control links or data links may fail; this probably causes the drone to enter a fail safe mode or worse

Risks

> damage to other aircraft or other colliding objects
> damage to people and property on the ground
> damage to (critical) infrastructure
> consequential and/or reputation damage
> prevent other aircraft from flying
> EM spectrum congestion
> risks: 1,2,3,4,5,16

Stakeholders

> telecommunications Authority
> drone manufacturers
> drone users

LOSS OF LINK

Description

> If the control link between the drone and ground control station breaks, the drone becomes uncontrolled; the drone may enter a failsafe mode, e.g. it may enter the return home failsafe mode and return to its starting location automatically or enter other failsafe modes

> if not all safe flight rules are obeyed such automatic flight may not be safe after all; the drone could hit another object

Risks

> this issue relates to issue 'airspace safety' and to issue 'safety on the ground' and hence to the risks mentioned in relation to those issues

> risks: 1,2,3,4,5,6,7,12

Stakeholders

> drone manufacturers
> drone regulation authority
> drone users

LEGISLATION

Description

> drone technology is emerging and is developing very rapidly; development of corresponding legislation is lagging behind

Risks

> this issue is not considered to comprise a risk as such, but it may introduce other risks

Stakeholders

> drone regulation authority
> drone manufacturers
> drone users
> law enforcement

COMMUNICATION

Description
› there is room for improvement in the communication about the legislation
› government has started an information campaign

Risks
› this issue is not considered to comprise a risk as such, but it may introduce other risks, caused by drone users who do not obey the law, even unintentionally

Stakeholders
› drone regulation authority
› drone manufacturers
› drone users

UNLAWFUL USE

Description
› unlawful use of drones comprises various types of use:
  › unintended violation of rules by recreational users
  › users knowingly breaking the law for specific reasons
  › the use of drones for a terrorist strike

Risks
› this issue relates to issue 'airspace safety', to issue 'safety on the ground', to issue 'privacy infringement' and to issue 'espionage' and hence to the risks mentioned in relation to those issues
› terrorist attack
› panic/disturbance of people on the ground
› crime
› risks: 1,2,3,4,5,6,7,8,9,10,11,12,13

Stakeholders
› civilians
› VIPs
› law enforcement

LAW ENFORCEMENT

Description
› drone flights can take place at locations where in fact they are prohibited; law enforcement currently has little means to prevent or abort such flights
› illegal flights are a potential safety and security risk
› tracking of users might be difficult
› countermeasures may inflict collateral damage

Risks
› the use of countermeasures may cause collateral damage, related to issue 'airspace safety' and issue 'safety on the ground'
› risks: 1,2,3,4,5,6,7,12

Stakeholders
› law enforcement
› drone users

ANNOYANCE

Description
› drones generate noise which can be considered by people as a nuisance
› if people get distracted, they may cause accidents

Risks
› annoyance (noise)
› consequential and/or reputation damage
› risks: 4,14

Stakeholders
› law enforcement
› civilians
› drone manufacturers
› drone users

ENVIRONMENT

Description
› drones generate pollution and contribute to global warming
› like other aircraft they consume relatively large amounts of energy

Risks
› environmental pollution and global warming
› risks: 15

Stakeholders
› law enforcement
› civilians
› drone manufacturers
› drone users

LIABILITY/INSURANCE

Description
› people are responsible for the consequences that result from flying their drones, e.g. when they cause damage.
› currently, i.e. without a drone owner registration system, it is hard to establish liability in case of a drone incident
› insurance companies are changing their policies considering the increased use of drones

Risks
› consequential and/or reputation damage
› economic damage
› risks: 4,9

Stakeholders
› law enforcement
› civilians
› insurance companies
› drone users

C   Slides per Technical Measure

REGISTRATION AND IDENTIFICATION

Description
› Unique registration number for drones, enabling to identify the owner
› Mandatory in the US
› Proposed in Europe

Issues addressed
› Unlawful use
› Law enforcement
› Liability and insurance

Impact
› Cost of technical measure: medium
› Technological complexity: medium
› Time to implement: medium
› Expected resistance: medium (if enforced)

VISUAL OBSERVABILITY

Description
› Application of bright colors, striping and strobe lights to enhance visibility
› Effect depends on situation

Issues addressed
› Airspace safety
› Safety on the ground
› Law enforcement

Impact
› Cost of technical measure: low
› Technological complexity: low
› Time to implement: short
› Expected resistance: low

COLLISION AVOIDANCE

Description
› Application of sense-and-avoid systems to drones
› Acoustic system already available (eBumper)
› Object detecting algorithms for forward looking camera

Issues addressed
› Airspace safety
› Safety on the ground
› Liability and insurance

Impact
› Cost of technical measure: medium
› Technological complexity: medium
› Time to implement: medium
› Expected resistance: low

TRANSPONDERS

Description

> Application of a transponder to a drone, which broadcasts its position periodically
> ADS-B is being investigated to be used for drones
> Requires significant decrease in size, weight and power consumption
> May have adverse effect on frequency spectrum

Issues addressed

> Airspace safety
> Safety on the ground
> Law enforcement
> Liability and insurance

Impact

> Cost of technical measure: medium
> Technological complexity: medium
> Time to implement: medium
> Expected resistance: low
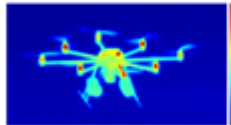
DETECTION/TRACKING/LOGGING

Description

> A combination of all possible means to detect and track drones
> Only a combination of detection techniques will work
> Much work done for defense purposes

Issues addressed

> Airspace safety
> Law enforcement
> Liability and insurance

Impact

> Cost of technical measure: high
> Technological complexity: high
> Time to implement: long
> Expected resistance: low

TELECOM NETWORKS TO TRACK DRONES

Description

> If drones can make use of the existing cellular network they could send their position to the network
> The position of the drone could be estimated by the network through triangulation
> An issue might be the downward direction of present antennas
> Presently under investigation by NASA and Verizon

Issues addressed

> Airspace safety
> Unlawful use
> Law enforcement
> Liability and insurance

Impact

> Cost of technical measure: medium
> Technological complexity: medium
> Time to implement: long
> Expected resistance: medium

AIRSPACE DIVISION

Description
> The subdivision in layers of the airspace:
> > Below 200 ft for 'low and slow' drones
> > Between 200 and 400 ft as a high-speed corridor
> > A no-fly safety zone between 400 and 500 ft
> > Beyond 500 ft for manned aircraft
> Advocated by Amazon and perhaps implemented in the NASA UTM concept

Issues addressed
> Airspace safety
> Law enforcement

Impact
> Cost of technical measure: low
> Technological complexity: low
> Time to implement: short
> Expected resistance: low

APPS

Description
> Apps for smartphones or tablets for:
> > Providing education
> > Actual data on no-fly zones, weather, positions of other aircraft
> > Flight planning
> > Drone control
> > Sending back position information to the network

Issues addressed
> Airspace safety
> Unpredictable behavior
> Communication
> Unlawful use
> Law enforcement
> Liability and insurance
> Airspace and practice area

Impact
> Cost of technical measure: medium*
> Technological complexity: low
> Time to implement: medium*
> Expected resistance: low

* depending on features implemented

FLIGHT PLANNING AND APPROVAL

Description
> Planning in advance the flight with a drone
> Submission of the flight plan to authorities
> Getting additional information and approval

Issues addressed
> Airspace safety
> Law enforcement
> Liability and insurance

Impact
> Cost of technical measure: medium
> Technological complexity: low
> Time to implement: short
> Expected resistance: high (if enforced)

AIR TRAFFIC MANAGEMENT SYSTEMS

Description

› Gathers information about all aerial traffic in an area
› Manages traffic to avoid collisions
› Uses a combination of techniques and sources
› Drones with better SAA capabilities get better access to airspace
› Example: NASA UTM

Issues addressed

› Airspace safety
› Unlawful use
› Law enforcement

Impact

› Cost of technical measure:	high
› Technological complexity:	high
› Time to implement:	long
› Expected resistance:	low

ESTABLISHING NO-FLY ZONES

Description

› Declaration and publication of areas where it is not allowed to fly a drone
› Temporary no-fly zones may be communicated by internet

Issues addressed

› Airspace safety
› Safety on the ground
› Unlawful use
› Law enforcement
› Liability and insurance
› Airspace and practice area

Impact

› Cost of technical measure:	low
› Technological complexity:	low
› Time to implement:	short
› Expected resistance:	low

ENFORCING NO-FLY ZONES

Description

› The drone knows its position and has access to an actual database containing no-fly zones
› The flight control system of the drone prevents the drone to fly into a no-fly zone
› Already implemented by DJI, other manufacturers to follow

Issues addressed

› Airspace safety
› Safety on the ground
› Unpredictable behavior
› Loss of link
› Unlawful use
› Law enforcement
› Airspace and practice area

Impact

› Cost of technical measure:	low
› Technological complexity:	medium
› Time to implement:	medium
› Expected resistance:	low

BEACONS TO ESTABLISH NO-FLY ZONES

Description
> A beacon to be put at a location where a no-fly zone is to be established
> Drones which receive the signal automatically know to keep a safe distance
>> passively (the operator gets a signal)
>> actively (geofencing is activated)
> Particularly useful for emergency situations

Issues addressed
> Airspace safety
> Safety on the ground
> Communication
> Unlawful use
> Law enforcement

Impact
> Cost of technical measure: medium
> Technological complexity: medium
> Time to implement: medium
> Expected resistance: medium

SECURING OF THE CONTROL LINK

Description
> Measures to protect the link to electronic attack:
>> encryption
>> frequency hopping
>> smart use of the spectrum
> For reasons of sensitivity, no details are provided

Issues addressed
> Airspace safety
> Safety on the ground
> Privacy
> Security of information
> Vulnerability to jamming, hacking, spoofing and eavesdr.
> Loss of link
> Unlawful use
> Liability and insurance

Impact
> Cost of technical measure: medium
> Technological complexity: medium
> Time to implement: short
> Expected resistance: low

SECURING OF THE INFORMATION DOWNLINK

Description
> Measures to protect the link to electronic attack:
>> encryption
>> frequency hopping
>> smart use of the spectrum
> For reasons of sensitivity, no details are provided

Issues addressed
> Privacy
> Security of information
> Vulnerability to jamming, hacking, spoofing and eavesdropping
> Unlawful use

Impact
> Cost of technical measure: medium
> Technological complexity: medium
> Time to implement: short
> Expected resistance: low

IMPACT LIMITING DEVICES

Description
> Add-on parachutes (commercially available)
> Crash absorbing structures

Issues addressed
> Airspace safety
> Safety on the ground
> Liability and insurance

Impact
> Cost of technical measure: medium*
> Technological complexity: medium*
> Time to implement: medium*
> Expected resistance: medium*

*some measures are readily available and cheap, others require a lot of effort

PROPELLERS

Description
> Shielding the propeller
> Prevents injury to persons
> Prevents damage to the drone

> Soft propeller material (plastic instead of metal)

Issues addressed
> Safety on the ground
> Liability and insurance

Impact
> Cost of technical measure: low
> Technological complexity: low
> Time to implement: short
> Expected resistance: low

PILOT'S LICENSE

Description
> Not a technical measure
> Can be enforced through technical measures (unique key for ground control station)
> Provide reduction in insurance premium if license has been obtained

Issues addressed
> Airspace safety
> Safety on the ground
> Unpredictable behavior
> Liability and insurance

Impact
> Cost of technical measure: medium
> Technological complexity: low
> Time to implement: short
> Expected resistance: medium

EDUCATION AND PR

Description

› Inform drone pilots about:
  › where to fly and other regulations
  › how to control their drone
  › keep the drone insight
  › using the proper failsafes
  › taking care of equipment

Issues addressed

› Airspace safety
› Safety on the ground
› Hype effect

Impact

› Cost of technical measure:	medium
› Technological complexity:	low
› Time to implement:	medium
› Expected resistance:	low

SAFETY REQUIREMENTS

Description

› Setting safety standards for drones:
  › reliability of propulsion
  › effect at impact
  › energy absorption at impact
› Enables certification
› Will be demanded by insurance companies

Issues addressed

› Airspace safety
› Safety on the ground
› Liability and insurance

Impact

› Cost of technical measure:	low
› Technological complexity:	medium
› Time to implement:	medium
› Expected resistance:	medium

REPORTING INCIDENTS

Description

› Voluntary reporting of incidents
› Black box in aircraft
› Automatic reporting by aircraft or ground control station in case of accident
› In the aerospace world reporting of incidents has provided many lessons learned, increasing aviation safety

Issues addressed

› Airspace safety
› Safety on the ground
› Law enforcement

Impact

› Cost of technical measure:	low
› Technological complexity:	low
› Time to implement:	low
› Expected resistance:	high (if enforced)

TNO innovation for life

REWARDING GOOD BEHAVIOR/PERKS

Description

› Introduction of a bonus/malus system like that of car insurances
› Actively monitor flying behavior; good behavior gives credits, reckless behavior gets penalties
› Government could reward good behavior with extra privileges

Issues addressed

› Airspace safety
› Safety on the ground
› Liability and insurance

Impact

› Cost of technical measure: low
› Technological complexity: low
› Time to implement: medium
› Expected resistance: medium

TNO innovation for life

PRICING OF SAFETY MEASURES

Description

› Stimulate the adoption of devices which enhance the safety of drones by means of price reductions
› Reductions could be provided by the government or by insurance companies

Issues addressed

› Airspace safety
› Safety on the ground
› Liability and insurance

Impact

› Cost of technical measure: medium
› Technological complexity: low
› Time to implement: low
› Expected resistance: low

TNO innovation for life

DRONE CIRCUITS

Description

› Provide for special areas (circuits) where drones can be raced safely
› Prevents people from reckless behavior at other places
› Attractive for the public

Issues addressed

› Airspace safety
› Safety on the ground
› Unlawful use
› Law enforcement
› Annoyance
› Environment
› Airspace and practice area

Impact

› Cost of technical measure: medium
› Technological complexity: low
› Time to implement: long
› Expected resistance: medium

NOISE REDUCTION

Description
> Reduction of noise produced by:
>> application of (more) smaller engines
>> ducting of propellers
>> aerodynamic design of propellers

Issues addressed
> Annoyance
> Environment

Impact
> Cost of technical measure: medium
> Technological complexity: medium
> Time to implement: medium
> Expected resistance: low

POLLUTION REDUCTION

Description
> Reduction of energy consumption
> Use of green energy

Issues addressed
> Environment

Impact
> Cost of technical measure: medium
> Technological complexity: high
> Time to implement: high
> Expected resistance: medium

D   Slides per Risk