New Generation of Counter UAS Systems to Defeat of Low Slow and Small (LSS) Air Threats

Jacco Dominicus
Royal Netherlands Aerospace Centre NLR
Amsterdam
THE NETHERLANDS

Jacco.Dominicus@nlr.nl

ABSTRACT

Detecting, classifying, identifying, tracking and defeating low, slow and small air threats presents a major challenge for existing sensor and effector systems. So-called first generation Counter Unmanned Aircraft Systems (C-UAS) systems often rely on detecting the datalink from the controller to the drone which provides limited capability against current threats. However, this means of detecting drones is a challenge when operators manipulate standard datalinks and it will not work at all against current and future autonomous drones. Other current methods of detecting and neutralising drones include for example combining radar with optical sensors. These systems are not always reliable, can generate large numbers of false alerts and are often manpower intensive to operate. The NATO SCI-301 Research Task Group (RTG) has been working on specifying what second generation C-UAS systems should entail. This paper will outline the findings of this RTG over the past three years.

1.0 INTRODUCTION

Low, slow and small (LSS) air vehicles, also known as drones or small Unmanned Aircraft (UA), are a relatively new development within the realm of aviation. Drones have brought new capabilities to a large part of the world's population by providing a low-cost airborne platform serving many applications, ranging from leisure flying to aerial photography and parcel delivery. Military use of small drones includes Intelligence, Surveillance and Reconnaissance (ISR) missions, weapon delivery and direct attack.

These types of drones have also introduced the concept of airpower to entities that previously had no access to the third dimension. Historically, applying airpower was reserved for well-funded and well-staffed organisations such as the world's armed forces. Operating even relatively small manned aircraft requires a significant investment in equipment, logistics, maintenance, manpower, training and infrastructure. In contrast, modern small drones are widely commercially available at low costs and are easy to operate. Most of these drones provide an ISR capable platform instantly out-of-the-box, and they can be relatively easily modified to serve as a weapon's delivery platform or as a direct attack object. Dedicated military drones in general are more sophisticated and capable, yet perform similar missions.

NATO identified, at an early stage, the utility and potential of Unmanned Air Systems (UAS). It is however naïve to assume that adversaries will not use similar systems against NATO's interests. Therefore, it is essential that NATO develops an effective means to counter the threat posed by LSS air vehicles. The challenges involved are numerous and range across the complete kill-chain; detection and identification of low-flying small objects with small visual, IR and RCS signatures can be problematic. Timelines between initial detection and the drone posing an immediate threat are often short, therefore decision making must be performed relatively quickly. Once the decision is made to intervene, it may be hard to find an effector that creates the desired effect. In addition, a range of effects may be required, where taking down the drone is just one of the desired effects.

Existing air defence systems were never designed to deal with LSS air vehicles. They may provide some capability, but suffer from significant limitations against this type of threats. In addition, the effectors they employ (mostly highly capable missiles) tend to be expensive, making them unsuitable to engage these now ubiquitous targets on a structural basis.

Dedicated Counter-UAS (C-UAS) systems do exist and are currently operational. Many of them are based on detecting the datalink between the operator and the drone, and intervention is performed by jamming, spoofing or manipulating this datalink. This concept works as long as the drone is dependent on a datalink and the C-UAS system recognises the signals. When the drone is operating autonomously (thus not requiring a datalink), this concept will not be effective.

Other C-UAS systems now being used employ an active radar for initial detection and an electro-optical (EO) sensor for further investigation and identification of the contact. In present systems, the radar has an operator who hands over the radar contacts to the operator of the EO system. Decision making on intervention can be performed by these two operators, or is delegated to a higher echelon. The effector is often operated by yet another individual. While this concept may work against a variety of threats, including autonomous drones, it is very manpower intensive to operate. In practice, this concept is applied during high exposure events, such as the G-20. For a limited amount of time (say a number of days), the local airspace is monitored for the presence of drones and actions are taken whenever suspicious activity is detected. While this concept and the associated manpower can be justified for these types of events, it is impossible to apply this concept for the year-round protection of an air base or an army compound.

Some key components of an advanced first generation C-UAS system are shown in Figure 1. In this case it includes an active radar, passive RF sensors, EO/IR trackers, including a laser range finder complemented by a jammer for neutralisation.

A next generation of C-UAS systems will therefore provide better capabilities against current threats, be readily upgradeable as the threat develops in the future and will require significantly less manpower to operate than current first-generation C-UAS systems. In addition, it will be interoperable with existing Command and Control (C2) infrastructure, thus enabling integration with current short range air defence systems.

Figure 1: Detection and neutralisation components of the Falcon Shield system.

2.0 SCI-301 AND ITS BACKGROUND

The North Atlantic Treaty Organization (NATO) was founded in 1949 by 12 countries and currently consists of 30 member states. Part of NATO is its Science and Technology Organization (STO), led by the NATO Chief Scientist. Its Collaboration Support Office (CSO) supports the collaborative business model where NATO and partner nations contribute their resources to conduct cooperative research and information exchange. CSO in turn is subdivided into seven different panels and groups, of which SCI is the Systems, Concepts and Integration panel. Its mission is to advance knowledge concerning advanced systems, concepts, integration, engineering techniques and technologies across the spectrum of platforms and operating environments to assure cost-effective mission area capabilities. Experts from all NATO nations are invited to submit suggestions to the panel for new activities. The SCI panel assesses these suggestions and launches initiatives to form task groups that engage in an activity for a fixed amount of time on a certain relevant subject. Before a task group is commissioned by the panel to engage in its activity, a so-called Exploratory Team (ET) is started. This team has the task to investigate whether sufficient interest exists within the NATO nations and its approved partners for that particular subject to significantly contribute to the activity and share relevant information among the participants. One of the criteria for the ET to proceed as a task group is that enough member states are willing to participate.

Concerning C-UAS activities, the SCI panel approved an initiative in 2010. The activity was given the name SCI-241, “Defence Against UAV Attacks” and started out as an ET [1]. Although the subject of countering UAs was recognised as important, it proved to be difficult to raise enough commitment from interested states to contribute to this effort in order to migrate the ET into a Research Task Group (RTG). Part of this lack of commitment was caused by the fact that within NATO’s defence organisations, no one had the explicit task of countering small drones. Another factor was the reduced budgets that most defence organisations were facing in the aftermath of the worldwide economic crisis that started in 2008, leaving little room for launching new initiatives. In addition, the urgency of countering LSS air threats was not felt. As a result, SCI-241 held a number of meetings in the period of 2011 through 2016, but failed to transition to a RTG due to lack of interest of sufficient nations to participate.

Within the military domain, this indecisive sentiment towards countering UAs changed rapidly after the widespread operational use of LSS air vehicles in the East-Ukrainian conflict and by IS in Iraq and Syria. Both of these conflicts started in 2014, and the protagonists increasingly made use of and developed their LSS capability over the ensuing years of the conflicts. As a result, in 2016 the interest within NATO to contribute to a task group was overwhelming. The SCI panel approved the transition from an ET to a RTG, changing its number and title, resulting in SCI-301 “Defeat of Low, Slow and Small (LSS) Air Threats” [2]. NATO Nations that are participating in this group are: Belgium, Denmark, France, Italy, the Netherlands, Romania, Spain, United Kingdom and the United States. In addition, NATO Partner for Peace Switzerland is an active member of the RTG and the NATO body JAPCC (Joint Air Power Competence Centre) contributes to this group. SCI-301 held its first meeting in June 2017, filling the meeting rooms of the CSO facility in Paris beyond their capacity. This was a stark contrast with the struggle in the first years to raise enough interest for the subject, yet indicative of the rapid development of LSS air vehicles as a threat and the limited assets available to counter them.

In the civilian world, it was events like the drone that approached Angela Merkel at a stage during an election campaign in 2013, the alleged attack on Venezuelan President Maduro in August 2018, the Gatwick drone disruption at the end of that same year which closed down one of the busiest airports in Europe for a few days and a number of other notable events, which raised public awareness of drones as a potential threat and the need to have systems available to detect and neutralise them.

The SCI-301 RTG started in June 2017 and runs for a period of three years. Its main task is to reflect on current (so-called first generation) C-UAS systems and to propose what a second generation of these systems should entail. The RTG will advise NATO where additional research is required to develop and operate more

capable, more effective and more efficient systems to counter the current and future LSS air threat. In order to fulfil this task, the approach outlined below was adopted.

The group is subdivided into four teams:

A. Threats Horizon Watch, Operational Analysis and Modelling & Simulation
B. Novel Detection and Identification
C. Future Effectors
D. Networking and Autonomy

Each team is led by a team lead who coordinates the activities within their team. Management meetings are held on a regular basis with the RTG chair, the co-chair, the secretary, the editor-in-chief and the team leads participating.

However, the most important activity that the RTG undertakes is to hold meetings where experts from the entire RTG get together to share information and experience while working towards the group's deliverables. After the first meeting in Paris in 2017, six more physical meetings were held, rotating among the nations contributing to the RTG. The last year, a number of virtual meetings took place.

Being a three-year study that started in June 2017, the RTG planned to finish its final report by summer 2020. While many RTGs ask for an extension at the SCI panel, the members of SCI-301 decided not to opt for an extension. The problem of countering drones for NATO was considered to be so urgent that it would not be appropriate to delay the delivery of a final report. However, when COVID-19 began to limit travel and made it difficult for SCI-301 members to perform their work, an extension for a year was requested. An interim report was written and distributed at the end of 2018 [3], which already contains some useful findings. The RTG's final report will now be finished during the summer of 2021.

When SCI-301 started as a RTG, NATO's C-UAS activities were fragmented and uncoordinated. During the past three years, however, NATO has established the Counter UAS Working Group, which brings together a wide number of C-UAS stakeholders with various backgrounds. Every two or three months, a meeting is held where information on actual deployment of UAS and C-UAS systems is shared, previous test events are discussed, new ones are announced and standards are established. This initiative has worked as a catalyst for C-UAS development and information sharing within NATO. The latest development is to include a number of selected partner countries to this Working Group.

It is interesting to note that quite a number of members of the SCI-301 RTG have not been able to complete their participation of the group until the end, because of the claims that were made in their respective countries to support their national C-UAS activities. Many of them were C-UAS experts and their expertise was required to solve urgent national issues. Members, as well as subgroup leads and even the first chairman had to step down from active participation and were replaced over the course of this RTG.

3.0 LSS AIR VEHICLES AS A THREAT

As stated in the introduction, small drones provide easily accessible utility to a wide variety of users. However, LSS air vehicles also lend themselves to malicious use by adversaries. Potential adversaries using drones range from single activists, terrorist organisations, insurgents to near-peer and peer nation state actors. Being small by definition, LSS air vehicles are limited in endurance, by the amount of payload they can carry and also by the range over which they can operate. Therefore, they provide a form of airpower to their users, but not the full scope of it. What they can and have brought to the fight is an ISR capability, for short range reconnaissance, indirect fire support, or providing a picture for setting off Improvised Explosive Devices (IEDs) at the appropriate time. In addition, LSS air vehicles have been used as weapon delivery

platforms, by enabling them to carry and deliver explosive devices such as grenades. LSS platforms have been employed as direct attack projectiles, guiding towards their targets and exploding upon impact, thereby sacrificing themselves during the attack. Finally, also adversary drones can be designed to be hunter-killer drones, made to seek and destroy other LSS air vehicles, or collide with larger airborne platforms.

A distinction can be made between commercially available drones and military drones. The commercial market is currently dominated by the Chinese DJI. In March 2020, it holds a market share in the U.S.A. of over 77% of consumer drones with no other company holding more than 4%. DJI's product range starts with the small Tello drone, features the ubiquitous Mavic (see Figure 2) and Phantom models and goes up to the professional Inspire 2. All these drones provide an instant ISR platform out-of-the-box, as they all come equipped with a camera and a datalink.

Commercially available drones are obviously not a weapon platform when bought by and delivered to the consumer. However, it is relatively simple to modify these drones into a weapon carrying platform or to transform them into a direct attack weapon by adding explosives and a fuse. In addition, it is possible to manipulate the standard factory-set datalinks, making it much more difficult to recognise that a drone is being operated in the area. For example, it is possible to control the drone and handle the video datalink over the 5G network, which hides the drone's signals from other omnipresent signals being communicated over this network. More advanced commercial drones are able to operate fully autonomously based on image processing, solely flying on visual cues, without the need of a datalink.

Besides acquiring commercially available drones and manipulating them to suit the specific needs of the user, it is also possible to construct LSS air vehicles in workshops using widely available components, such as engines, propellers, batteries, flight control systems, etc. Additive manufacturing (i.e. 3D-printing) makes it relatively easy to produce custom designed components. The attack on the Russian air base Khmeimim in Syria in January 2018 was allegedly performed using 13 armed self-build fixed-wing drones, made from plywood and insulating foam.

Figure 2: DJI Mavic Pro commercial drone.

The last category of LSS air threats are the military drones. These are produced by manufacturers of military equipment according to specifications set by defence organisations. Many NATO member states operate this type of drones themselves, such as the RQ-11 Raven. Potential adversaries have similar drones in their inventory. Extensive use of military drones was made in the recent Nagorno-Karabakh conflict.

All categories of LSS threats listed above can be used in all roles. In addition, they can be employed on their own, coordinated or in a swarm. A coordinated attack means the use of multiple drones that for example arrive at their target from different directions at a pre-determined time. In this concept, there is no interaction between the drones once they are on ingress towards their targets. In a swarm, multiple drones do interact with each other during their flight phase. Because of the low costs of LSS air vehicles, scenarios involving multiple drones are realistic.

Within SCI-301, Team A was responsible for the threat horizon watch. The work included keeping track of developments of LSS air vehicles, their concepts of operation and their level of autonomy. In order to assist the RTG in benchmarking new technologies for detection, decision making and effecting LSS threats, the team defined so-called vignettes that are representative of the potential adversary use of drones in a variety of scenarios. The six vignettes that were worked out are:

- Protection of Base
- Protection of Heavy Manoeuvre Force
- Armoured Manoeuvre
- Dismounted Forces
- Ship Navigating Narrow Strait
- Urban Warfighting

- Figure 3 depicts a graphic of one of the vignettes as produced by Team A.

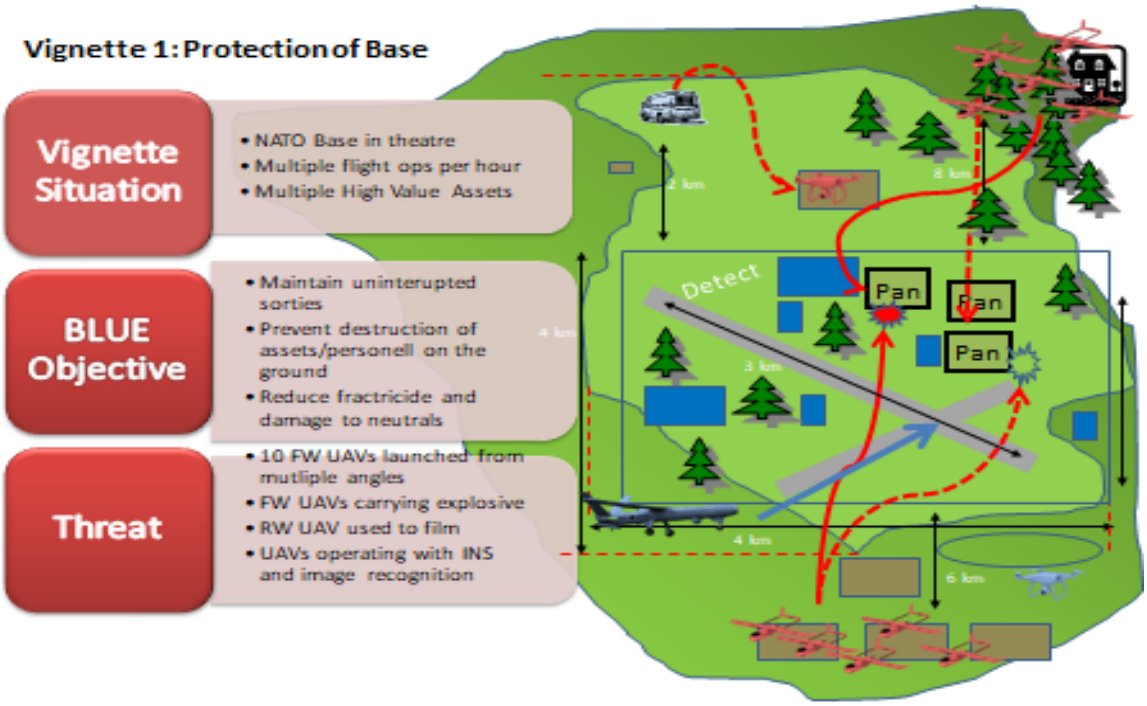

Figure 3: Example of a SCI-301 vignette.

4.0 COUNTERING LSS AIR VEHICLES

It is important to realise that it is not the concept of UAs in itself that presents a problem to NATO's air defences, but rather the size, low operational altitudes and the availability of small UAs. Larger UAs that fly at higher altitudes can be detected and engaged in a similar fashion to their manned equivalents. This was recently demonstrated by Iran in June 2019, when they shot down a U.S. RQ-4A Global Hawk UA using a radar-guided surface-to-air missile. Numerous other examples exist, such as the air-to-air engagement against a Georgian drone in 2008 in the Abkhazian conflict. The drone filmed the engagement by a MiG-29 up until its own destruction.

The problems associated with countering LSS air threats are numerous and not easily solved. The process of countering LSS air threats is depicted in Figure 4 and is rather generic in nature. The same basic process applies to countering threats other than drones. A recent publication of JAPCC [4] provides a thorough account of countering UASs.

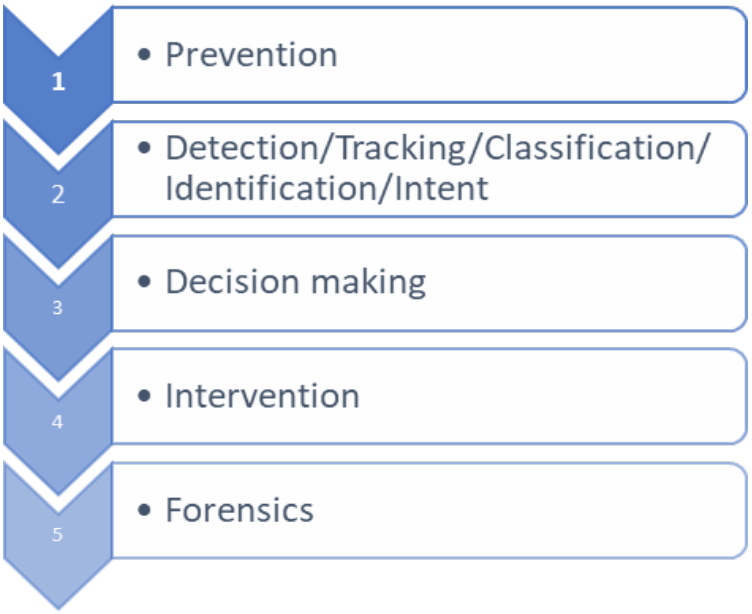

Figure 4: The process of countering LSS air threats.

4.1 Prevention

Preventing an adversary from owning and operating LSS air threats is nontrivial. In the civil domain, preventing malicious use of drones can be performed by imposing regulations and informing the public about them. Enforcing these regulations and applying penalties when they are violated all contribute to limiting the unintended and unwanted use of drones. Examples of policy that prevent the misuse of drones is registration of drones, equipping certain sized drones with transponders, demanding pilot training and certification for commercial operations and creating no-fly zones for drones. The latter restriction can be pre-programmed in drones equipped with GPS, disallowing them to operate inside these areas. While this so-called geofencing is relatively easy to tamper with, the user should be aware that he or she is doing something that is not allowed. Drones that do not obey these rules and regulations stand out from drones that do comply, thereby making it easier to go after drones which have potentially nefarious intentions. In the military domain, however, this concept of prevention will have limited utility; it will work for example when protecting a national air force base from inadvertent drone infringements. However, it will not work against insurgents who operate drones to support their activities in deployed areas of operations.

For larger weapon systems, it is relatively easy to prevent widespread proliferation by for example export control of the weapon systems themselves and their enabling technologies. While nations do not control production, sales and exports of weapon systems of non-allied countries, it is usually possible for intelligence agencies to keep track of where these weapon systems are located and who operates them. This task is virtually impossible for drones: the worldwide sales of commercial drones runs into the millions each year. Trying to find out who is searching the internet for instructions on how to manipulate or weaponise a drone or who is acquiring components for such purposes may lead to some results, but remains a daunting task.

The bottom line is that any potential adversary who wants to use LSS air vehicles against NATO's interests can most likely acquire and prepare these drones without being noticed before they actually deploy these assets.

4.2 Detection, Tracking, Classification, Identification & Intent

Work on detecting LSS air vehicles is performed by Team B of SCI-301 and is focussed on the difficulties due to their inherent small size and their low operating altitudes. The following requirements for detection systems can be defined:

- **The ability to reliably detect** – This means almost no false negatives (drones which are present but that remain undetected), and very few false positives (the system indicating a detected drone, where in reality there is nothing there, or for example a bird instead of a drone) within a specified range. This must be performed in a wide variety of terrains and settings, including urban environments.
- **The ability to accurately track** – This requires a position of the drone in direction, range, altitude and possibly also its velocity.
- **The ability to classify and identify** – Classifying means the ability to determine the type of drone, for example discriminating between a quadcopter and a fixed-wing drone. Identification means being able to state the exact type of drone, e.g. it is a DJI Mavic Air 2.
- **The ability to determine intent** – This means the ability to tell the mission of the drone, for example whether it is executing an ISR mission, and if so, what it is the operator is interested in, or if it is there to deliver explosives or to perform a direct attack and what its target is.
- **The ability to locate and identify the operator** – This means determining where the drone is operated from and who controls it.
- **The ability to disseminate the information to a human being** – In order to inform a human decision maker, the information collected must be processed, logged and presented to this person.
- **The ability to integrate the detection system in a wider context** – Although the sensor or C-UAS system may operate standalone, ideally it is interoperable with existing military or civil infrastructure.
- **The ability to do all of the above in a timely manner** – Timelines in a counter drone scenario can be short, hence the requirement to perform the detection, tracking, etc. quick enough to allow for decision making and neutralisation if necessary.
- **The ability to do all of the above for multiple drones** – Because it is plausible that multiple LSS air threats are present at the same time in many relevant scenarios, the requirement for the system is to be able to detect and track multiple drones without being saturated.
- **The ability to do all of the above in various weather conditions** – Malicious use of drones may be undertaken in varying meteorological conditions, during day and night, although certain drones and certain missions are limited in their operations themselves when for example the visibility is reduced.

- **The ability to do all of the above with limited manpower** – For any sensor system, there will be a requirement for the amount of people that are needed to operate it.

Several methods of detecting LSS air vehicles exist and are briefly discussed below:

- **Passive RF** – This detection method is based on sensing the control datalink that is established between the operator and the drone and vice versa. Localisation of the drone and/or operator can be performed by using directional antennas or when using multiple geographically spaced antennas by means of the Time Difference Of Arrival (TDOA) mechanism. Identification of the drone is possible when the signals are known and recognised within the library of the detection system. It may be possible to intercept the video datalink from the drone to the operator, thus enabling observation what the UA operator is seeing. The method of passive RF detection is difficult in signal intensive environments (such as urban scenarios) or when signals have been manipulated. In addition, it will not work at all against autonomous drones that have no datalink at all.
- **Active RF (i.e. Radar)** – Drones typically do provide detectable echoes when RF signals are emitted in their direction. Due to the LSS air vehicle's size their radar cross section is small, making detection at significant ranges difficult. In addition, drones often produce echoes that are comparable with those of birds. Their flight profile and speeds are also alike, making it sometimes difficult to distinguish between the two. The benefit of using radars is that they are also capable of detecting autonomously operating drones. Classification or identification is possible using more sophisticated radars by counting the number of propellers, the number of blades and measuring their rpm. Localisation of the drone in direction, altitude and range is an intrinsic capability of radar systems.
- **Acoustic detection** – Drones typically have a distinctive acoustic signature which can be detected using sensitive microphones. With an array of microphones, it is possible to provide a direction and by means of triangulation an indication of range. The distance at which a drone can be detected depends on the noise levels at the source, background noise, atmospheric conditions and wind. It is commonly limited to a few hundred meters. Classification and identification presents a challenge for acoustic sensors, although some systems will be able to count the number of propellers and their rotational speeds.
- **EO/IR** – Electro-optical and infrared sensors are well suited for tracking drones. They may be less suitable for initial detection, but whenever a coarse cue is available from another source, the EO/IR sensor can be used to fine-track the contact. Using lenses or telescopes, it is possible to zoom in on the target and classify and identify the object. Optical sensors do provide an accurate directional localisation of their targets, but no direct range information. If the size of the object is known, distance might be approximated based on the image. Some optical sensors are complemented by laser range finders to accurately measure distance. Alternatively, range information can be determined using triangulation when multiple optical sensors are geographically distributed. EO/IR sensors are weather dependent.
- **LiDAR** – LiDAR sensors use laser imaging to scan for objects. Based on the echoes that return from the pulses emitted by the laser, accurate distance measurements can be made with high resolution. Radial velocities can be determined by means of Doppler shifts. LiDAR measurements can be accurate enough to not only detect flying objects, but also sense the induced airstream of their wings and propellers. LSS air vehicles may be on the small size for this application, though. Profiling the drone thus making an accurate 3D scan of the object enables the classification and identification of the drone. LiDAR is a weather dependent sensor.
- **Exotic sensors** – Some more exotic sensors that will need time to mature include active acoustic sensors (similar to SONAR, but in this case in the air rather than under water) and trying to detect weak spurious electromagnetic emissions, emitted from the electrical components of the drone, such as the electrical motors and on-board computers. Autonomous operating drones without a datalink will also emit these signals.

A human being such as a soldier can also serve as a sensor platform to detect and identify drones. The human is equipped with ears and eyes that enable them to hear and see a drone flying. This comes down to acoustic and EO/IR detection as mentioned above. Training the individual to recognise relevant drones can help to identify drones. However, the range at which a human being is able to detect drones is limited.

There is no single sensor that will fulfil all requirements in all circumstances against all possible types of drones. The consensus from the work performed by Team B of SCI-301 is that the future of drone detection systems is the ability to combine more than one sensor and applying the concept of sensor fusing. This process shall be aided by making use of advanced tools, such as Artificial Intelligence (AI) and image recognition. Any sensor system should ideally be integrated in other existing infrastructure and be interoperable with established C2 systems.

The ideal concept will depend on the intended application and its associated requirements. A concept that for example will work against a wide variety of LSS air threats, including autonomous ones, uses an advanced radar as a basis. In order to limit the amount of false negatives, it is operated in a highly sensitive mode, thus generating a number of false positives when in operation. The contacts generated by the radar are further investigated by another sensor, for example an EO/IR sensor or a LiDAR. This process should be automated using AI and image recognition to its maximum extent in order to limit the manpower requirements.

Another concept for a sensor system is an airborne platform, such as a drone carrying a single sensor or a mix of sensors. The benefit of this concept is that the detection range of most sensors is increased by the elevated altitude at which an airborne platform operates. In addition, the sensor carrying drone can close in on a contact in order to further investigate it. When equipped with a passive RF sensor, this concept may increase the chance of locating the drone's operator, which in many cases is desirable.

4.3 Decision making

Since timelines in countering LSS air threats can be short, it is essential that decisions on intervention can be made quickly. In some cases, it may be allowed to have the process of decision making fully automated, because one is essentially targeting an inanimate object. In addition, the effector may not be lethal or harmful towards humans or animals. However, when applying the effector poses a risk towards living creatures or can otherwise disrupt own operations or civilian life, appropriate Rules Of Engagement (ROE) must be established and adhered to. The term "meaningful human control" is often used in this context to guarantee that human perception and judgement is involved when deciding to use force that is potentially lethal or harmful. In order to facilitate a swift decision making process, the essential information must be presented in a clear and straightforward manner. In addition, a proposed decision can be made by an automated system, for example by using AI.

When making decisions, whether by a human being or by automation, one must consider the effects that one wants to achieve. Destroying the drone is not always a feasible, nor the most desirable effect. Possible other effects are treated in the next paragraph. In order to make the right decisions, it is of paramount importance to be informed about the contact and other considerations. Relevant information for decision making includes:

- What type of LSS air vehicle is it?
- What is the intention of the drone?
- Does it pose an immediate threat?
- What is its intended target?
- Who operates the drone?

- Where is it operated from?
- How many contacts are detected?
- Is it likely that more (undetected) drones are in the air or will be deployed?
- What is the most likely course of action when no intervention takes place?
- Which effectors are available for use?
- What is the preferred achievable effect?
- What is the most likely result of our intended action?
- What will be the adversary's response to our action?
- What is the risk involved with the proposed intervention?

4.4 Intervention

As introduced in the previous paragraph, a decision made to intervene with one or more LSS air threats involves a consideration on what effects should or can be achieved. The SCI-301 Team C study on potential future effectors therefore started with establishing a list of possible effects:

- **Ignore** – To disregard the detected UA and continue other activities.
- **Monitor** – To keep track of a previously detected UA.
- **Deceive** – To cause a person or a system to believe something that is not true. Military deception seeks to mislead adversary decision makers and operators by manipulating their perception of reality.
- **Coerce** – To force another party to act in an involuntary manner (either action or inaction) by using intimidation, threats or actions. Coercion is subdivided in deterrence and compellence.
- **Deter** – To force the target to refrain from taking action through the application of fear of punishment
- **Compel** – To force the target to cease or reverse an action that was already initiated by application of punishment or by threatening (more) punishment when the target shows no change in behaviour.
- **Distract** – To divert the attention from the operator and to prevent him from concentrating on his tasks.
- **Disturb** – To interfere with the normal functioning of the UA.
- **Delay** – To slow down the adversary's progress.
- **Deny** – To prevent the adversary from using UAs as an asset in certain areas or to disallow the use of assets that support the UA's operation.
- **Take over control** – To take possession of the control of the flight path of the UA, or of the control of the UA's sensors.
- **Capture** – To take into one's possession or control, potentially by the application of force.
- **Neutralise** – To render the explosives on board the UA ineffective.
- **Degrade** – To reduce the effectiveness or efficiency of adversary UA operations permanently or for a prolonged period of time.
- **Destroy** – To damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt. When it comes to persons, destroying is equivalent to eliminating the individuals.

The list of possible effects is further elaborated on in SCI-301's interim and final report, but this is not included in this paper due to space considerations.

The desired effect will depend on the situation. When a drone is detected that advances rapidly towards a compound and it is observed that it is carrying an explosive device, immediate neutralisation or destruction of the drone would most likely be the desired effects. On the other hand, when the drone is loitering and it appears that it is performing an ISR mission, other effects may be more appropriate and more effective in the long run. Keep in mind that the drone itself usually is inexpensive and might very well be considered to be expendable by its operator. Just taking it down will simply have the operator launch a replacement drone, but will not stop his mission. In this case, it would be much more interesting to investigate who is operating the drone, where it is operated from, what it is interested in, etc. This can for example be achieved by monitoring or capturing the drone. Deception or disturbing may be effective ways of countering the adversary's mission in this case.

After composing this list of possible effects Team C made a list of effectors. It thereby leveraged from previous work that was performed in NIAG studies (NATO Industrial Advisory Group) [5], [6], [7]. Possible methods of intervening with LSS air threats include:

- **RF Jamming** – This is currently one of the most popular effector techniques. It involves jamming the datalink from the operator to the drone (and/or vice versa) and may be specific for that connection or indiscriminate across a wide spectrum. In the latter case, it will most likely disturb a lot more than just the drone. The exact effect of a jammed datalink depends on the drone and its settings, but it will deny the operator from effectively providing control inputs to the drone and/or from receiving video feeds from the drone. When the datalink is lost for a prolonged period of time, some drones land on the ground, while others return to a predetermined location, for example their starting point.
- **RF Spoofing** – This technique is more sophisticated than jamming, since it intends to break into the datalink and take over control of the drone.
- **GNSS Jamming** – When drones are using GNSS signals (i.e. GPS, GLONASS, BeiDou or Galileo), jamming these signals might result in the drone hovering in place, landing at the spot or returning to a predetermined location using inertial navigation. Hence this effector will disturb the drone's intended operation. GNSS jamming will affect all receivers in the vicinity of the jammer, not just the targeted drone.
- **GNSS Spoofing** – This technique is again more advanced than jamming, and when applied cleverly, it can be utilised to make the targeted drone navigate to a desired location or to make it land or crash. It essentially deceives the drone's navigation system that it is in another location than it actually is. Similar to jamming, it will affect all receivers in the vicinity.
- **Nets** – Nets are designed to entangle the drone and/or its rotors or propellers. The main benefit of using nets is that they are potentially able to capture the targeted drone intact, providing the opportunity to perform forensic investigation on the captured drone. In addition, they reduce the risk of collateral damage. Present systems are restricted in range and have difficulties with manoeuvring targets or when used in high wind conditions.
- **Jet streams** – Concentrated flows of both air and water have been demonstrated to disturb drones in-flight. The disturbance can potentially be significant enough to take down the drone and destroy it upon impact with the ground. A blast of a nearby explosive detonating can have a similar effect. The range at which these methods are effective is usually limited.
- **Projectiles** – All kinds of kinetic projectiles can be employed to engage drones, including bullets, grenades and missiles. Manually aimed small arms have a very low probability of hitting their targets, though. More promising concepts against LSS air threats are radar aimed guns using smart

ammunition rounds that expand into many smaller pellets in the vicinity of their targets, laser guided rockets and small and simple guided hit-to-kill projectiles. Advanced missiles that were designed to intercept traditional aerial targets (such as manned aircraft) can and have been used against drones, but they are not always effective and it is hard to justify the cost ratio between the effector (often expensive) and the target (cheap and expendable). An example of this is the shoot down of a quadcopter using a Patriot missile in 2017. The effect of using a projectile against a drone is to at least degrade the target, but most of the times it will destroy the drone after a successful intercept.

- **Lasers** – Depending on their wavelength, the output power, beam quality, atmospheric propagation and the distance of the engagement, lasers can have a range of effects on their targets. At lower power levels a laser can blind or dazzle an EO/IR sensor, such as a camera on-board the drone, thus potentially distracting the operator, disturbing the drone's operation or denying the use of the drone's EO/IR sensors. At higher power levels, lasers may permanently damage the optics and/or the sensor resulting in a degradation of the drone. At yet even higher power levels, a laser may precisely target the drone itself, leading to its destruction. In favourable meteorological conditions,UAs can be engaged from several kilometres distance by advanced HEL systems. See Figure 5 for an example of a High Energy Laser (HEL) engagement.

Figure 5: Laser engagement of a DJI Tello drone.

- **High Power Microwaves** – HPM effectors emit a strong Electro Magnetic Pulse (EMP) with the intention to incapacitate or damage the electronics on their targets. This damage may result in an incontrollable drone, falling from the sky and crashing into the ground, thus destroying the drone. In other scenarios, the damage done to the electronics of the drone degrades the drone. HPM effectors can be directional, but it is impossible to accurately aim at a single drone at range, since the HPM beam will always diverge somewhat. This limits the range at which HPM effectors can be applied, but has the potential benefit of targeting multiple drones (e.g. a swarm) in a single engagement.
- **High intensity ultrasound** – This type of effectors emits high intensity acoustic signals that disrupt IMU sensors. This can disturb the drone, or result in a crash of the drone, thus destroying it. Being a high frequency sound signal, the propagation of the signal is limited and this type of effector must be brought relatively close to its target in order to have an effect.

- **Birds of prey** – This method has actually been operational using trained eagles that capture rogue drones in-flight. The concept has now been abandoned, because of the high level of training needed and the manpower involved.

Like sensors, effectors can be either ground-based (fixed or mounted on ground vehicles), hand-held, or UA-based, for example in case of a hunter-killer drone.

After making the list of effectors and mapping them to the list of possible effects, Team C selected the most promising concepts for effectors against next generation LSS air threats and scored their value in a matrix for SCI-301 vignettes.

4.5 Forensics

The last element in the process of countering LSS air threats is the forensics, which focusses on the collection, preservation and analysis of evidence relating to a C-UAS situation, for example to determine the sequence of preceding events, identify the responsible entities and/or determine a modus operandi. This also involves assessing the effect that was attained with the intervention. This part is also referred to as Battle Damage Assessment (BDA). In addition, one could investigate what type of drone was used by the adversary, if and how it was modified, how it was operated, who was operating it, from where it was launched and recovered, etc. Even if the rogue drone remained undetected and/or no action was taken, it might still be possible to learn from the incident and to take appropriate measures to prevent a future repeat of the incident. A C-UAS system can facilitate performing forensics by logging all information that it observes during operation.

5.0 FIRST AND SECOND GENERATION C-UAS SYSTEMS

Reference [8] gives an overview of C-UAS systems and was originally published at the beginning of 2018, and updated at the end of 2019. It states a total of 537 C-UAS related products, from 277 different manufacturers. Out of these 537 products, 175 systems are capable of detection only, 214 are purely effectors and 138 are combined systems capable of doing both. It should be noted that not all systems considered are equally mature and not all of the described systems are operational. The vast majority of these systems is based on detecting the RF datalink between the operator and the drone and most of the intervention systems (>75%) are based on jamming or spoofing (the datalink, GNSS signals or both). The members of the SCI-301 RTG also assessed current C-UAS systems, while many of them have personal experience of these systems at demonstrations, tests or in actual deployment. From previous NATO work, manufacturer information, publicly available sources, their own background, expertise and the work performed over the course of the 3-year study within the RTG, the members of SCI-301 have made the following reflections on current systems and an outlook towards a second generation of C-UAS systems:

- **Datalinks** – Many of the current drones depend on a datalink from the operator to the UA and vice versa. Hence, it makes perfect sense that the majority of first generation C-UAS systems are based on detecting the datalink and subsequently intervening with this datalink for their effectors (usually jamming or spoofing). As noted earlier, there is a trend to manipulate standard datalinks, making it more difficult (if not impossible) for a C-UAS system to distinguish between a drone control signal (or the drone's video link) and other signals. In addition, it is seen that drones are capable of autonomous operations, thus not emitting any signals during their airborne phase. Hence, the relevant question is: is there a place for C-UAS systems based on this principle in the second generation of C-UAS systems? The answer is: definitively so. One of the reasons for that answer is that, although it might be possible to evade being detected or affected by such a system, it makes it more difficult for a potential adversary to deploy standard commercial off-the-shelf drones. Forcing them to manipulate their UASs affects the availability and might be noticed by intelligence agencies.

In addition, knowing that a datalink will be detected denies the adversary from certain utility that a drone normally would provide, such as real-time ISR. Using a drone as an observation platform for setting off an IED at an appropriate time is for example impossible without a datalink. Finally, passive RF detection is one of the few possibilities of directly locating the operator of the drone, monitoring what it is the operator is looking at and for taking over control of the adversary's drone. It is therefore anticipated that systems based on detecting and affecting datalinks will remain the basis and serve as a first layer of LSS air threat defence. Second generation systems will be able to detect more signals, including manipulated datalinks and will be more sophisticated affecting their target drones, with a focus on taking over control, rather than just denying the operator to send control signals to its UA.

- **Detection, tracking and identification** – When not (solely) depending on passive RF, current C-UAS systems are usually a combination of a radar and other sensors. While it is acknowledged by the SCI-301 RTG that the concept of having multiple sensors is the key towards reliable UA detection, the current implementation of it could benefit from further development. First of all, it is felt that initial UA detection can be improved by using modern techniques, such as Active Electronically Scanned Arrays (AESA), bi- or multi-static radars, cognitive radar and millimetre wave radar. A handover to another sensor will remain necessary in order to reduce the number of false positives and to further investigate the contact, enabling identification and possibly to determine the intent of the drone. However, this handover should be automated in second generation systems, without requiring human intervention. While EO/IR sensors continue to be good candidates for this role, LiDAR should be considered more often as an auxiliary sensor. At shorter ranges, acoustic sensors offer potential benefits. One of the key enablers for quicker and less manpower intensive observation of UAs is the use of automatic image recognition, made possible by applying AI techniques, such as machine learning. Automated sensor fusion where information from all available resources and sensors is merged into a single Common Operational Picture (COP) is the last step towards the next generation of systems for detection, tracking and identification of UAs. The way in which this COP is presented to a human operator warrants careful consideration. Everything the system observes and processes needs to be logged so as to facilitate post-event operational analysis and forensics.
- **Preparation** – The process of preparation can enhance the effectiveness of current and future systems. Preparation involves the process of information gathering of what type of LSS air vehicles the potential adversaries operate and how they operate them. It is also of paramount importance for training AI to recognise images and patterns in the adversary's operation. Part of preparation is also a laydown plan of sensors and effectors, in concert with the local terrain and assumed adversary positions and actions. Integration with other sensor systems and C2 infrastructure needs to be considered. Future systems should provide tools for making this plan in order to quickly deploy a C-UAS system when necessary.
- **Decision support** – Operator decision support for the majority of current systems is limited to providing a visual overview of the actual situation. Most systems provide a two-dimensional topographical view to the operator, sometimes assisted by aural alerts to draw attention to newly discovered contacts or to warn for a perceived imminent threat. Second generation decision support should be much more sophisticated, providing at least a prioritised list of threats that is updated continuously while the situation is changing. True decision support would also incorporate available effectors and advise on what effector to use on what target, taking into consideration what the desired effect is on that specific target. The risk of employing the effector with respect to possible collateral damage inflicted and applicable ROEs should be taken into account. Second generation decision support systems should migrate from having humans-in-the-loop towards having humans-on-the-loop. Fully autonomous decision making and intervention might be considered when applying the effector is low-risk or when the threat level is high. The focus of the development of

decision support systems should be to match available effectors with targets, minimise the risk of erroneous (proposed) decisions, shortening timeliness and reducing manpower requirements.

- **Interoperability and integration** – Current C-UAS systems are often standalone systems having limited connectivity with other existing infrastructure, such as other sensor systems or C2 systems. The next generation of C-UAS systems will have to utilise an open, flexible and modular framework that allows for ease of interoperability between various C-UAS modalities and integration into existing C2 systems, while maintaining compliance with NATO policies on interoperability. Standards should be imposed and enforced, making sensors, C2 systems and effectors of C-UAS systems vendor agnostic from an integration point of view.
- **Effectors** – Most current C-UAS systems only have a single method of intervening with a LSS air threat at their disposal, where the prevalent effector is jamming or spoofing of the datalink. Other contemporary systems deploy a net or use smart airburst munitions, but very few systems currently operational are known to employ truly distinct effectors. Next generation systems ideally would have multiple effectors to choose from, being able to tailor the effect to the threat and situation at hand. Matching the use of an effector with a specific target should be part of the decision support as mentioned earlier.
- **Cost effectiveness** – While costs should not be the primary consideration when protecting lives and interests of our own military and civilian population, it is conceivable that defending against LSS air threats is not sustainable when applying expensive effectors. The adversary can use drones in large numbers at the same time or keep coming with replacement drones and continue its operations. This type of attrition warfare is easily lost when no low-cost effectors are available. Effectors that are promising in this respect and deserve further study and/or development include for example small and simple hit-to-kill self-sacrificing projectiles that collide with their targets and Directed Energy Weapons (DEW), discussed in more detail below.
- **DEW** – DEW can be subdivided into HEL and HPM weapon systems. Current practical HEL systems are all solid-state, transforming electrical power into focused laser energy. While the system itself can be expensive, the cost per shot is low, requiring only electrical power. Drones tend to be vulnerable for laser engagements, especially when targeted at a critical part of its structure or another essential element, such as its control electronics. Pre-knowledge of vulnerable parts can help to shorten engagement times. HPM systems convert electrical power into electromagnetic radiation, also resulting in low costs per engagement. An HPM weapon system may very well be one of the few options at hand to simultaneously engage multiple targets, such as a swarm of UAs. Developments for HPM and HEL weapon systems are ongoing in order to increase power and effective range. Both concepts are promising for defeating LSS air threats and are still maturing. Meanwhile, the first operational HEL weapons systems capable of engaging LSS air threats have been delivered and HPM-based systems are expected to follow soon. DEW-based effectors should therefore be considered for second generation C-UAS systems.
- **Saturation** – Every C-UAS system has a limit of the amount of targets it can detect, track, identify and engage at the same time. Some first generation C-UAS systems are easily saturated, either by system limitations or by the human operators being overwhelmed by the number of threats they need to deal with concurrently. Second generation systems should have less system limitations and reduce the workload on the operators by means of automation to a maximum extent possible.
- **Point defence, defence at range and area defence** – Many present-day C-UAS systems are limited in range for both their detection capability and applying their effectors. Since LSS air vehicles can move relatively fast, these range limitations are the culprit for the short timelines between initial detection and the drone posing an immediate threat. Deploying a system having limited range essentially results in a point defence at that position. To cover a larger area requires multiple of these systems to be deployed. A next generation of C-UAS systems would therefore benefit from sensors providing more detection range. This can be achieved by using advanced radars and/or by elevating

sensors on a mast or on a (tethered) UA. To also provide protection at range, effectors are needed that cover more distance. Effectors well-suited for this are HEL weapon systems and larger calibre (smart) munitions, although the latter have difficulties with targets manoeuvring during their time of flight, which can be several seconds at longer ranges. Missiles are known to be able to intercept their targets at significant ranges, however they tend to be expensive. Area defence requires mobility of the effector platform, possibly provided by a hunter-killer drone as discussed below.

- **Hunter-killer drones** – A hunter-killer drone is an unmanned platform designed to engage other drones. By getting nearer to its target than fixed installations are able to do, a hunter-killer drone can observe its target from shorter distances, thereby enhancing identification and potentially determining the intent. In addition, raising sensors to a higher elevation will boost detection ranges of some sensors and will also increase the chance of locating the operator of the target drone. The information thus obtained enables better informed decision making. Some effectors, such as nets, can only be effectively deployed from short range, thus requiring a moving launch platform if more than just point defence is needed. Other effectors, such as HPMs and jammers, can cover more range, but may create unwanted effects on other (non-target) systems in the vicinity when they are employed with the power levels necessary to bridge that distance. Getting close to their targets enables applying these effectors at modest power levels, thus creating only a local effect. A hunter-killer drone may additionally be equipped with kinetic means to intercept their targets, such as small hit-to-kill projectiles. Alternatively, the hunter killer-drone may intentionally collide with its target in order to take down an imminent threat. In addition to intervening with their targets, hunter-killer drones can be used to follow their targets and to monitor where it will be recovered. This may assist in localising the operator. The level of autonomy of a hunter-killer drone can range from tight human-in-the-loop control to fully autonomous and everything in between. The first operational hunter-killer drones are now appearing on the market, although most are still in the development and demonstration phase. Therefore, this concept is second generation C-UAS and is assessed as promising for both detection and intervention by the SCI-301 RTG.
- **Training** – For any military unit, realistic training is of paramount importance to operational readiness. For first generation systems, this can be provided by dedicated “red air” drone operators. However, this is manpower intensive and limits the scenarios to the type and number of drones which are available. It is desired that next generation C-UAS systems are equipped with build-in Live-Virtual-Constructive (LVC) capabilities to further enhance realistic training opportunities. This requires Modelling and Simulation (M&S) of LSS air vehicles and their corresponding signatures.
- **Upgradability** – Many first generation C-UAS systems suffer from a lack of upgradability. While the threat is developing very rapidly, the C-UAS systems are not able to keep pace with the increased capabilities of the threat. Any future C-UAS system would therefore be easily expanded with more and different sensors and effectors. In addition, enhancements to the user interface, decision support tools and autonomy should be incorporated when available or be developed when desired.
- **Research, development and production** – While LSS air vehicles as a threat develop very rapidly, it is felt that operational C-UAS systems are unable to keep pace. Dedicated research programs must be encouraged, as well as the production and testing of demonstrators, in order to enable faster development of more and better capabilities against LSS air threats. Industry is yet to find a good format for producing operational C-UAS systems, as large industrial defence companies are geared towards designing complex and expensive weapon systems. Since C-UAS systems will have to be produced in large numbers and need to have a justifiable cost-ratio with respect to the threat they are designed to engage, these larger companies need to find new business models. Smaller companies on the other hand often lack the financial resources to significantly invest in research and development and are inapt to manufacture their products in large numbers or have little experience in making products according to the required military standards.

- **Acquisition processes** – It is observed that many of the NATO nation's acquisition processes are inadequate for the rapid developments in C-UAS systems. The time it takes from initial expression of need of a weapon system until its first operational introduction takes several years in most defence organisations. While this process fits for the acquisition of large weapon systems such as tanks, naval vessels or fighter aircraft, it is too slow to keep up with the progress of LSS air threats and the C-UAS systems developed in response. A change of these processes is required to effectively and timely acquire C-UAS systems and to maintain an operational capability against newly emerging LSS air threats.

The conclusion of the work performed by the SCI-301 RTG is that there is no silver bullet against the LSS air threat, nor will there be one in the foreseeable future. Effective means of countering drones will consist of a system of C-UAS systems. Development is needed in several areas to arrive at a next level of capabilities, as identified by the RTG and indicated above.

6.0 THE ULTIMATE GOAL: DETERRENCE

A second generation of C-UAS systems will undoubtedly be more capable and more efficient in dealing with current LSS air threats and will be better prepared for the rapid development of these threats in the future. However, being able to better detect, track, identify and to neutralise drones in itself may not be enough to stop potential adversaries from using drones. The ultimate goal is to break the will of the adversary to use its drones against NATO's interests by means of applying deterrence.

Deterrence might keep an adversary from operating UAs in the following cases:

- When operators fear that their personal lives or that of others within their organisation are in danger or otherwise negatively affected when the operators will start to operate the UA.
- When operators feel that operating the UA is futile and/or there is a high chance of losing valuable assets such as the UA itself or ground stations.

In order for deterrence to be successful, the threat or warning to the targeted adversary must be communicated, it must be credible, it must be effective when executed and it must be plausible that refraining from operating the drone will improve the outlook of the target of the deterrence.

In order to achieve the first objective, it is important to locate where the drone is operated from and to identify who operates it. C-UAS systems may contribute to this by the ability to detect and track at long range, enabling to backtrack where the detected drone was launched from or to witness its recovery. Alternatively, it is possible to locate the control signals from the operator to the UA. Forensics on captured or crashed drones might reveal who modifies, constructs or operates the LSS air vehicles. Other ways of locating the operators outside the C-UAS system is for example possible by means of intelligence, or traditional reconnaissance missions.

The second objective can be attained by having extremely effective C-UAS systems that will capture or destroy nearly all LSS air vehicles that a potential adversary launches. Since drones are typically inexpensive and easily operated in large numbers, the effectiveness of the C-UAS system must indeed be very high before it has a deterring effect.

Both objectives can contribute to effective deterrence. It is advised by the SCI-301 RTG that C-UAS systems beyond the second generation will focus on achieving this type of deterrence. However, it is also felt that it will take a significant effort before that goal is reached.

ACKNOWLEDGEMENTS

The author wishes to thank all members of the SCI-301 RTG, past and present, for their contribution in that study. It has been an exciting endeavour in turbulent times and it was a privilege to be working alongside inspiring personalities from so many different nations and having such diverse backgrounds.

A special thank you goes out to George Matich, team lead of Team A, who sadly passed away in January 2021. George was an extremely knowledgeable person who contributed significantly to this task group, both professionally and as a person. He will be remembered and missed by all SCI-301 members.

REFERENCES

[1] Bushey, D.E., NATO S&T SCI-241 ET Technical Activity Proposal (TAP), "Defence against UAV Attacks", (2010).

[2] Bookham, R.P., NATO S&T SCI-301 RTG Technical Activity Description (TAD), "Defeat of Low, Slow and Small (LSS) Air Threats", (2017).

[3] Dominicus, J.W. & SCI-301 Team, "SCI-301 RTG Defeat of Low, Slow and Small (LSS) Air Threats 2018 Annual Report", (2018).

[4] Willis, M., et al., "A Comprehensive Approach to Countering Unmanned Aircraft Systems", Joint Air Power Competence Centre, (2021).

[5] Alne, S. & NIAG SG-170 Team, "Engagement of low, slow and small aerial targets by GBAD", final report on NATO NIAG Study Group 170, (2013).

[6] Alne, S. & NIAG SG-188 Team, "GBAD sensor mix optimization", final report on NATO NIAG Study Group 188, (2015).

[7] Alne, S. & NIAG SG-200 Team, "Low, slow and small threat effectors", final report on NATO NIAG study group 200, (2017).

[8] Holland Michel, Arthur, "Counter-Drone Systems", 2nd Edition, Center for the Study of the Drone at Bard College, https://dronecenter.bard.edu/projects/counter-drone-systems-project/counter-drone-systems-2nd-edition, (2019).

AUTHOR/SPEAKER BIOGRAPHIES

Jacco Dominicus (Jacco.Dominicus@nlr.nl) holds a Master of Science degree in Aeronautical Engineering obtained from Delft University of Technology. He is currently Principal R&D Manager within the Defence Operations Department of the Royal Netherlands Aerospace Centre NLR. He leads a team on operational deployment and weapon system performance. The department provides technical and operational support to the Netherlands' military for all platforms with an air or space component. Jacco Dominicus was early to identify the importance of countering small UAs and the lack of capabilities to do so in our defence organisations. He currently is the chair of NATO RTG SCI-301 "Defeat of Low, Slow and Small Air Threats".