A whole-of-society approach to drone counter-measures

Electronic Warfare South Africa 2019 International Conference
05 November 2019

Dr Duarte Gonçalves

CSIR
our future through science

Agenda

- Background
- Risk analysis
- Technical aspects of drones
- Integrative approach to drone counter-measures
- Conclusions

Background - Case study 1 of 2

The Gatwick case (21 December 2018):

- Disruption lasted 33h with an estimated cost of £50 million.
- Disruption affected 140 000 people and led to the cancellation of over 1000 flights.
- £4-5m spent on anti-drone technology.
- Policing cost amounted to £900k.
- Couple falsely was arrested and detained for 36 hours with no subsequent arrests, or convictions.
- Finally, Sussex Police admitted - *“there may never have been any drones.”*

Sources and image credit:
https://www.theguardian.com/world/2019/jan/04/gatwick-returns-to-normality-but-drone-threat-remains;
https://fortune.com/2019/01/22/gatwick-drone-closure-cost/

Background - Case study 2 of 2

Damage to the infrastructure at Saudi Aramco's Abaqaiq oil processing facility in Buqyaq, Saudi Arabia, 14 Sep 2019.

- The strikes appear to involve at least 20 drones and several cruise missiles.
- Half of Saudi Arabia's oil production capacity was shutdown or *5% of the world's global daily oil production* .
- At least 17 strikes hit targets:14 storage tanks and three processing trains.

Source: Detailed satellite photos show extent of 'surgical' attack damage to Saudi Aramco oil facilities, CNBC, 17 Sep 2019, https://www.cnbc.com/2019/09/17/satellite-photos-show-extent-of-damage-to-saudi-aramco-plants.html

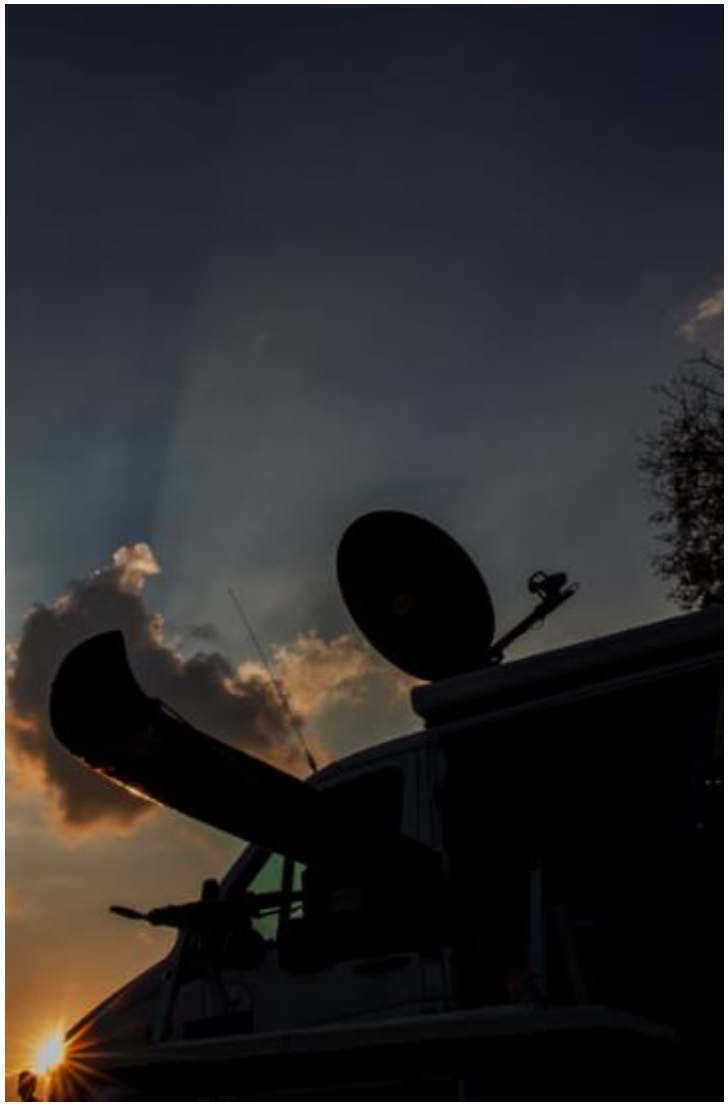
Background - Project

- Over 230 products from 155 companies in more than 30 countries working on counter-drone systems (November 2018, not including military labs and traditional GBADS).
- What sort of drone threats and hazards should we concern ourselves with *in the context of South Africa*?
- What are legislative and organisational constraints in drone counter-measures?
- What counter-measures could be applied, taking into account these constraints *and* cost?

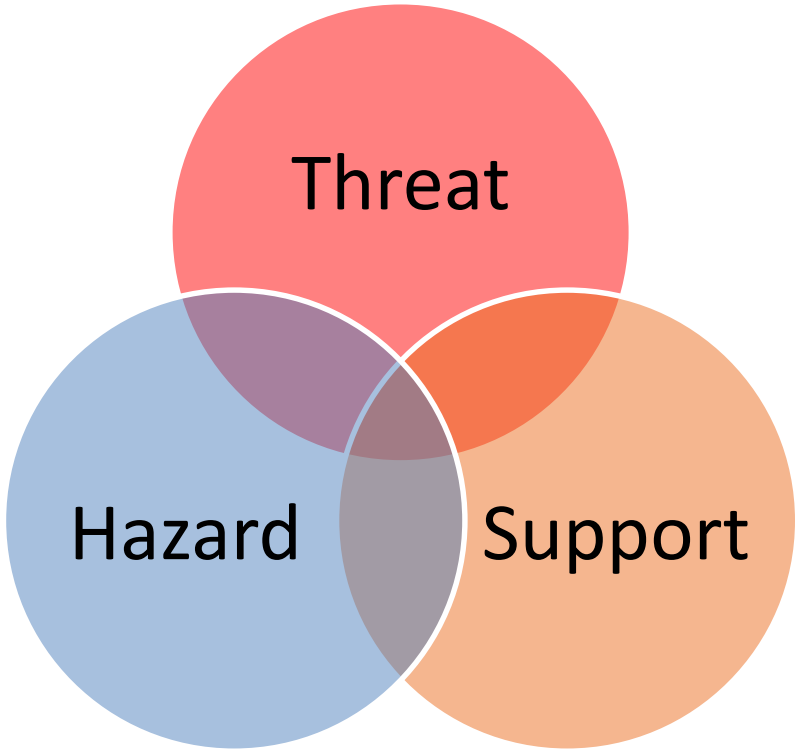
Background - Project

- Scope of the project:
  - Limited to South Africa;
  - Only airborne drones over land;
  - Non-proliferation is excluded;
- This presentation is based on selected aspects of an ongoing, CSIR funded project.

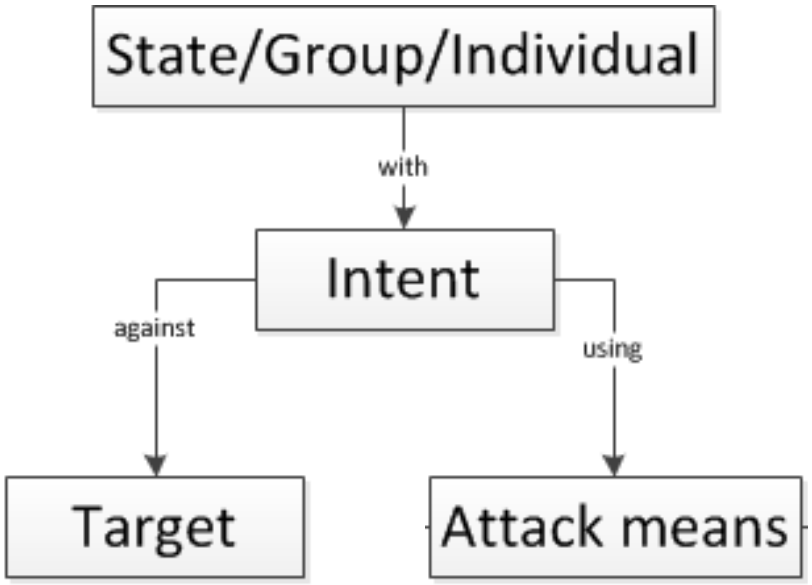
The nature of the drone risk



- Framework for threat analysis;
- Two emerging drone risks.



Framework for threat analysis



Principles:

1. Red alternatives analysis
2. Analysis of competing hypothesis

Two Emerging Risks

Two drone risks are highlighted in this presentation:

- **Extracting economic value** - smuggling, theft of intellectual property or other information and blackmail. Organised criminal groups have the resources. Drones provide new opportunities to expand their operations using methods less familiar to law enforcement.
- **Hazards** caused by collision of drones into other (airborne) vehicles, infrastructure or people.

  Illegal, irresponsible use, negligence, incompetence or technical issues. Technical issues includes loss of control of a drone through design errors, drone malfunction or operator has lost communications with the drone.
- The consequences of these hazards are related to the total energy.
- Commercial demand for drone based services with many commercially available drones and an increasing demand to fly drones within civil society.

Quick overview - Technical aspects of drones

- Drones categories;
- Drone flight and control categories;
- Drone payloads, and
- Drone swarms.

Drone categories

- Multirotor, fixed wing or hybrid systems;
- Electric, internal combustion, turbine;
- Huge variation in size, speed, endurance and payload capacity;
- Generalisations:
  - Multirotor – Low endurance, lower speed, low payload capacity
  - Fixed wing – High endurance, higher speeds, larger payloads, but have a higher logistical footprint.
  - Hybrids – combine best of both.

Drone flight and control categories (1/3)

- The drone flight may be carried out by the remote pilot completely manually, or with different levels of automation.
- Drone flight and control categories:
  - Direct Control;
  - Mode Control;
  - Flight Plan Control; and
  - Autonomous Control.
- Direct control requires highly skilled remote pilot. Remote pilot controls flight trajectory.

vs

- Autonomous control requires the least skilled remote pilot of all control categories. Drone controls flight trajectory.

Drone payloads

- Surveillance payload: Visual, infra-red and voice;
- “Conventional” explosive payloads;
- “Unconventional” explosive payloads:
  - dirty bombs (nuclear, biological or chemical attack) or
  - pyrophoric devices (materials that ignite spontaneously).
- Cyber payload – Cell phone based;
- Jammer (not very likely in civilian cases);
- Contraband and
- Combinations of these payloads.

Drone swarms

Two swarm approaches:

- **Homogeneous swarm:** relies on the advantage of numbers to attack a single target or multiple near-simultaneous targets.
  - Overload counter-measures at targets.
  - Example: Attack on the Russian bases in Syria 2018.

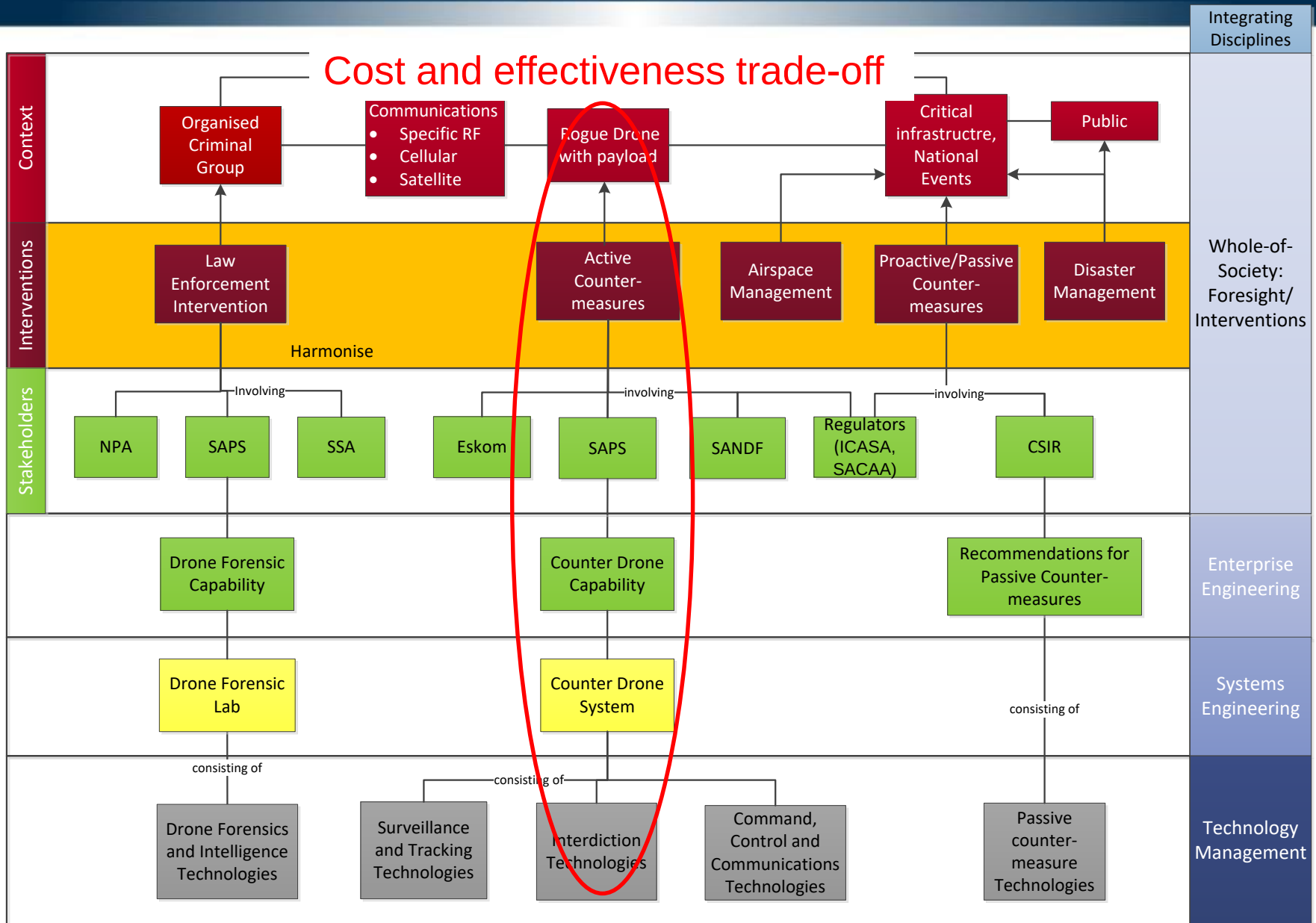
- **Functionally specialised drones** used together, for example:
  - Decoys,
  - Jammer (stand-off now becomes stand-in);
  - Surveillance (audio-visual), and
  - Explosive payload.

Daniels, J., 12 Jan 2018. Russia says it killed rebels behind swarm drone attack in Syria, but experts see more such strikes ahead. *CNBC.*

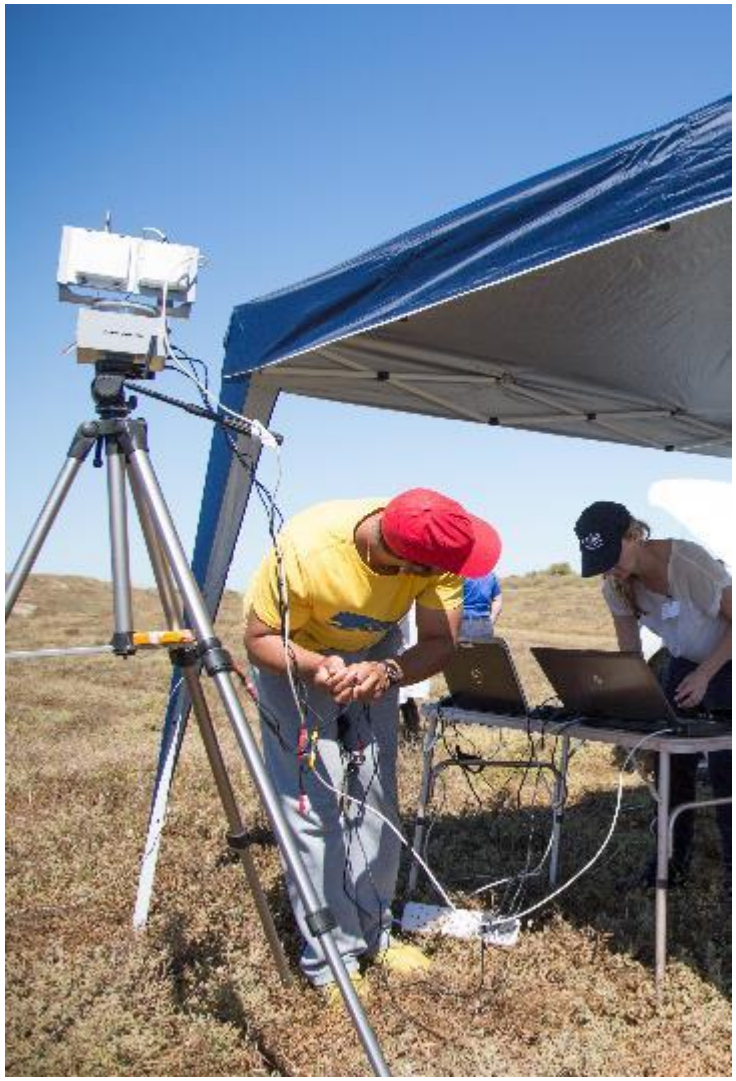
An integrated approach to drone counter-measures

- In South Africa there are approximately 18 government stakeholders with applicable legislation, private stakeholders, NGOs and the public.
- The following is a *vertically and horizontally* integrated framework for developing drone counter-measures.
- It serves to *illustrate* the some of the interventions and how these might flow down. It also does not reflect stakeholder consensus or agreement. It is a work in progress.

An integrated approach to drone counter-measures



Intervention: Law enforcement



Drone forensics and intelligence:

- Combination of airframes, Electronic Warfare capabilities, and digital forensics (which includes cyber forensics and mobile device forensics);
- Paradigm shift:
  - With national/international events, the offence starts with rogue drone entering restricted or prohibited airspace (assuming this is an offence);
  - Geolocation of operators (if this is possible) and
  - Intragroup (criminals) communications.

Intervention: Active counter measures

- Active counter measures (examples):
  - Detection is based on combinations of radar; electro-optical; Infra-red and acoustic and additional information such as a recognised air picture.
  - Interdiction: Kinetic means (Gun, needles); net; RF jamming; GNSS jamming; spoofing; laser; electromagnetic pulse and raptor (bird).
  - Some of these interdictions can be conducted from a drone.
  - There are potential consequences to using each of these in a civilian context.
  - The challenge of active counter measures: Probability of successfully neutralising rogue drone = Probability of detecting the drone x Probability of successful interdiction.

Intervention: Airspace management, Passive/proactive counter measures, Disaster management

- Airspace management:
  - Secure identification of drones (especially for high energy drones), including position (Automatic Dependent Surveillance - Broadcast).
- Passive/proactive counter measures:
  - Policy, regulations;
  - Deception, camouflage, cover, concealment;
  - Identification of drones (as discussed);
  - Processes and operating procedures and
  - Detection of anomalies (e.g. Wi-Fi anomaly detector).
- Disaster management:
  - Rogue drone preparedness to be incorporated into Disaster Management.
  - If all else fails….

Conclusions

- Rogue drones are not an “overseas” problem. South Africa has a specific risk profile which may be different from other countries.
- There is no single stakeholder that can deal with the rogue drone problem- it extends beyond the mandate of a single government department.
- Shared understanding of the rogue drone issue and preparedness are key.
- Stakeholders need capabilities, not just technical systems, while maturing various technologies for the future.
- A strategic mix of capabilities can be identified from strategic interventions highlighted.
- Each of these interventions is necessary, but not sufficient to address the rogue drone problem.
- An increase in counter-measures will lead to a response from adversaries resulting in an escalation and unpredictability of drone counter-measure effectiveness.

Questions?

Dr Duarte Gonçalves
dgoncalv@csir.co.za
012 841 3963