DRONEDEFENCE

Richard Gill

DRONEDEFENCE
4X-UST

CAUTION KEEP CLEAR OF FAN

DRONEDEFENCE

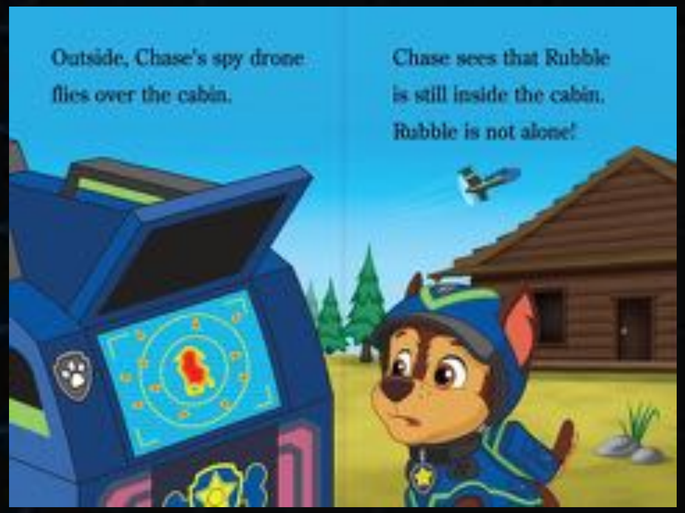
Unmanned Aerial Vehicles (UAVs) or Drones:

- UAVs Have Been Around For 100 Years
- ‘Drone’ First Used In The 1930s
- Military Drones Came First
- Negative Public Perception
- The Narrative Needs to Change
- Develop Supportive Framework While Addressing Legitimate Security Concerns
- Legislation needs to Catch Up

DRONEDEFENCE

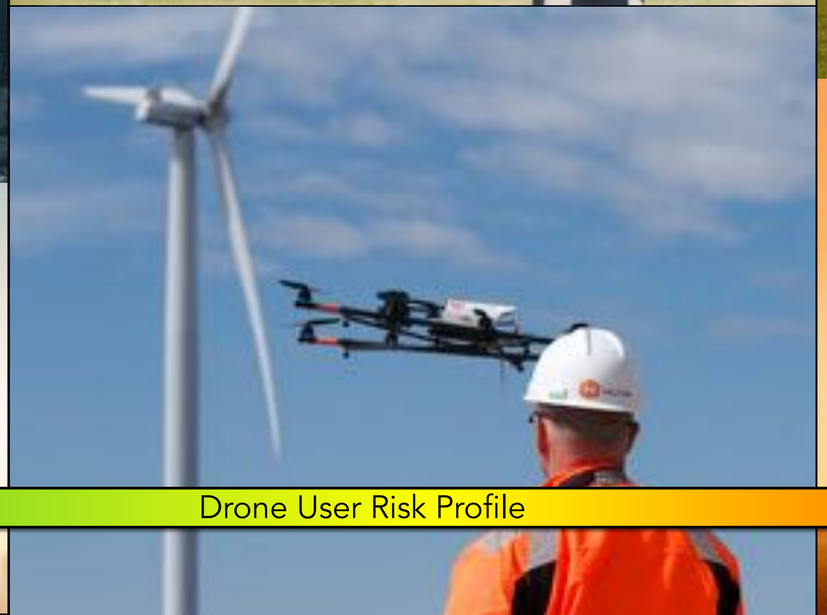
Overcoming Adoption Barriers:

- Develop Supportive Framework
- Current Legislation
- A Human, Not a Technology Problem



DRONEDEFENCE

The Ecosystem, Now and the Future



Low Risk — Drone User Risk Profile — High Risk

PAST

NOW

FUTURE

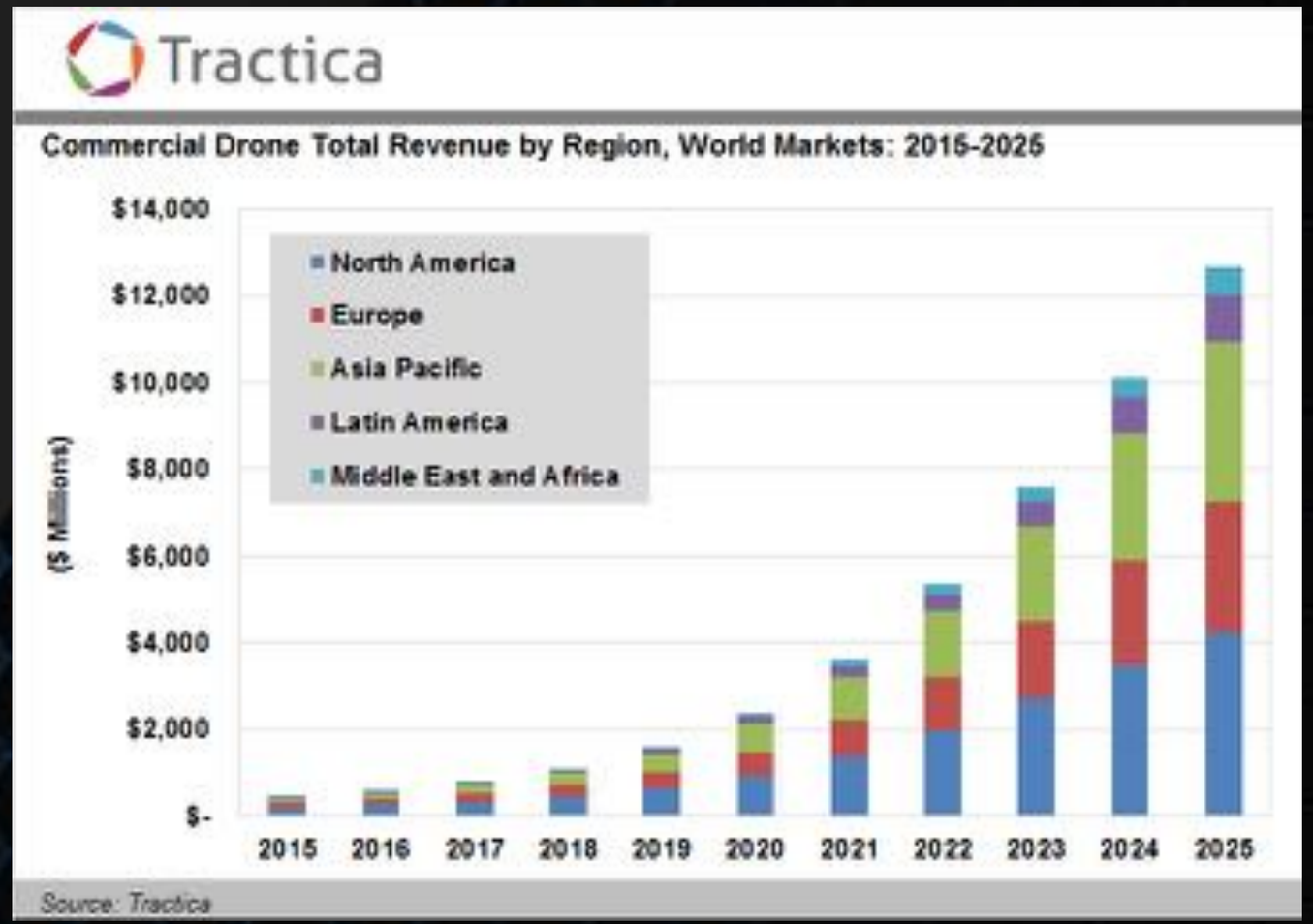
DRONEDEFENCE

Technology Enablers:

- Declassification of Technology
- Production Advancements (microprocessors, chipsets, gyroscopes & GPS)
- Battery Technology

Reasons For Drone Sales:

- GPS Assisted – Easy to Fly
- Readily Available – Can be bought online
- Relatively Cheap – Outstanding 4K cameras



DRONEDEFENCE

Drones – Key Capabilities:

- Access – Overcome Physical Barriers
- First Person View – See What the Camera Can See & Capture Images
- Real Time Control – Steer Onto Target
- Ability to Carry Payload

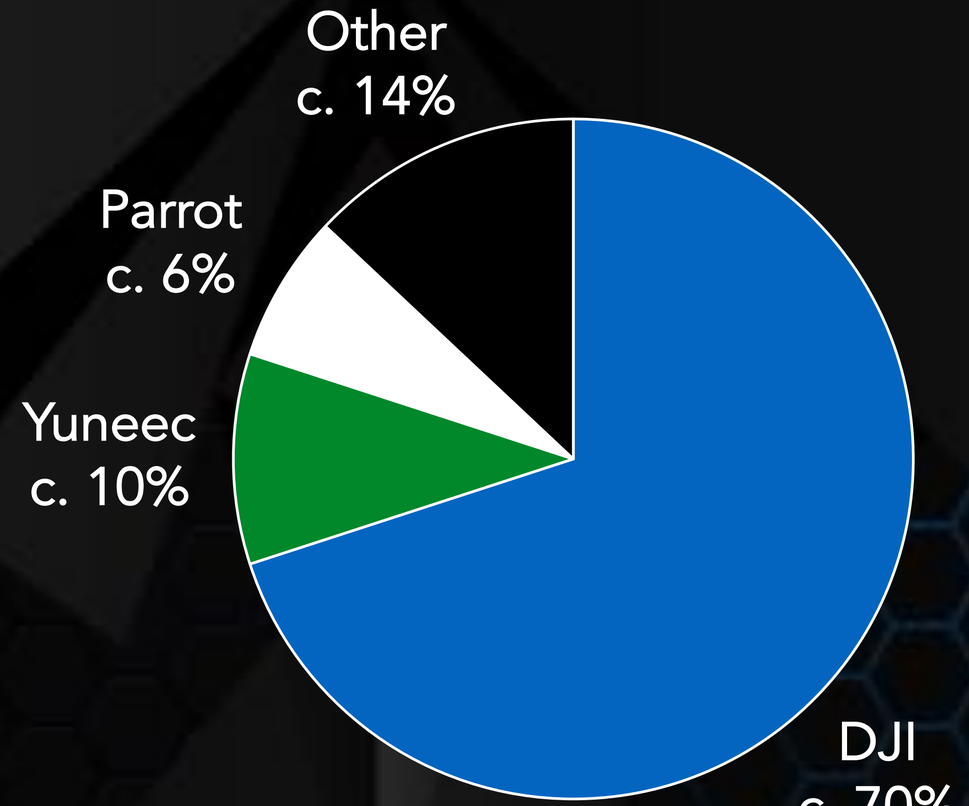
DRONEDEFENCE

Worse Case:

- Dirty Blood
- Crop Spraying Drone
- Programmed Flight
- Major Public Event

DRONEDEFENCE

Common Commercial Drones:

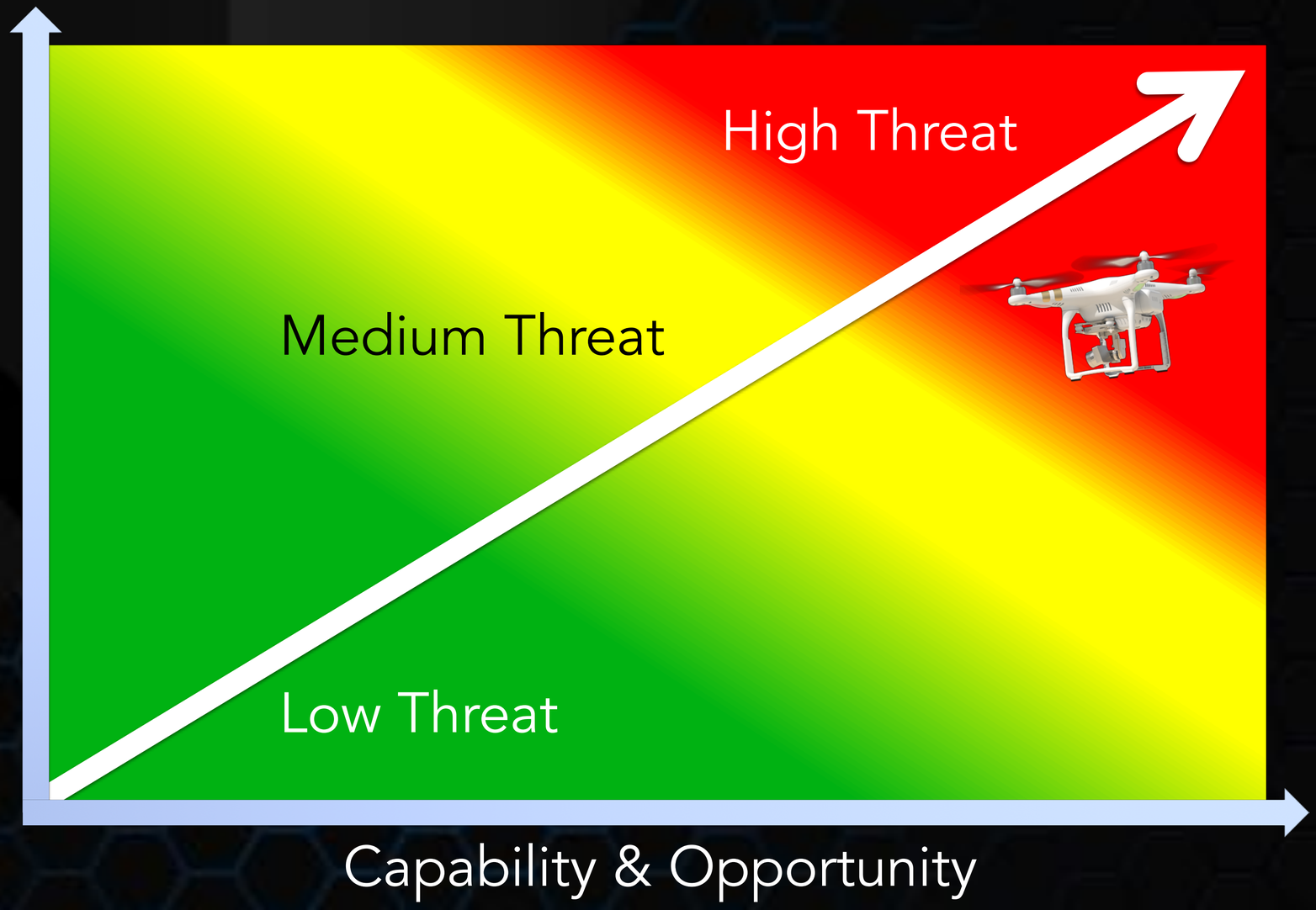


DRONEDEFENCE

The Continuum of Tolerable Risk:

- Organisations Face Nefarious Actors
- Drones Offer New Opportunities

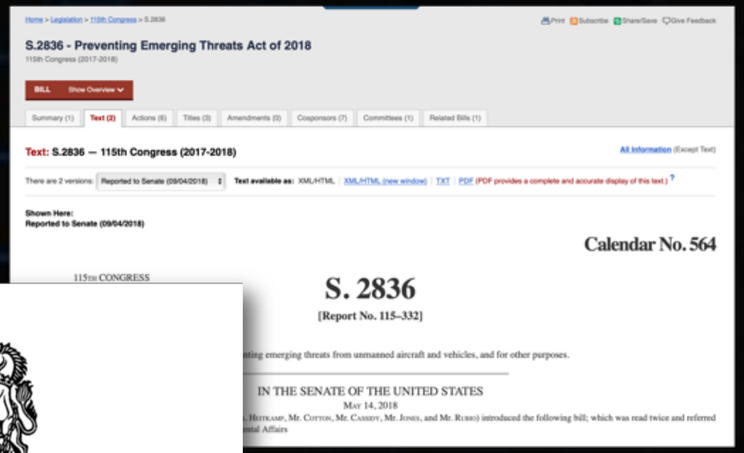
- Are the Risks worth the Reward?



DRONEDEFENCE

Applicable Legislation:

- Preventing Emerging Threats 2018 (US)
- Federal Aviation Authority (FAA)
- Civil Aviation Authority (CAA)
- Police Act 1997 (Part 3 Sect 92-95)
- Prisons Act (2018)
- National Decision Model
- Air Navigation Order
- European Convention on Human Rights (Article 2)
- Wireless Telegraphy Act
- Right to Self Defence
- Aviation Security Act 82


S.2836 - Preventing Emerging Threats Act of 2018

115th Congress (2017-2018)

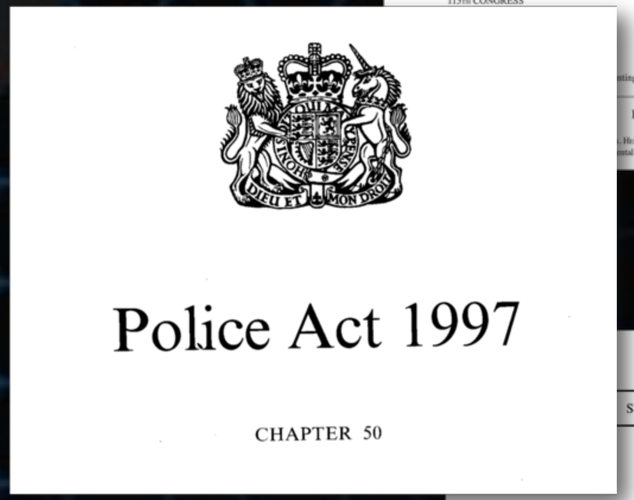
Text: S.2836 — 115th Congress (2017-2018)

Calendar No. 564

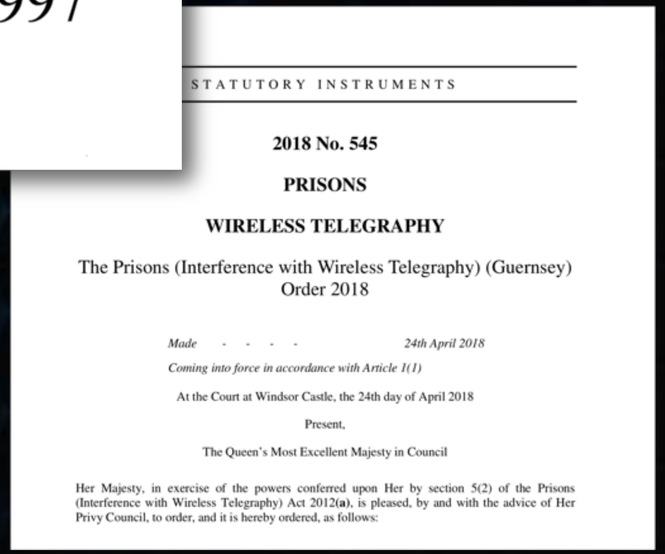
S. 2836

[Report No. 115–332]

IN THE SENATE OF THE UNITED STATES


Police Act 1997

CHAPTER 50


STATUTORY INSTRUMENTS

2018 No. 545

PRISONS

WIRELESS TELEGRAPHY

The Prisons (Interference with Wireless Telegraphy) (Guernsey) Order 2018

Made - - - - 24th April 2018

Coming into force in accordance with Article 1(1)

At the Court at Windsor Castle, the 24th day of April 2018

Present,

The Queen's Most Excellent Majesty in Council

Her Majesty, in exercise of the powers conferred upon Her by section 5(2) of the Prisons (Interference with Wireless Telegraphy) Act 2012(**a**), is pleased, by and with the advice of Her Privy Council, to order, and it is hereby ordered, as follows:

Hello Tower, Permission To Launch?
There is a Better Way: DRONEDEFENCE

DRONEDEFENCE

What Needs Protecting & From Who?

What Needs Protecting:

- Assets From Damage
- Reputation from Damage
- People From Harm
- Knowledge From Theft
- Activity From Observation
- Locations From Incursions
- High Value Items From Exfiltration/Theft

Severity	Extreme
Likelihood	Unlikely

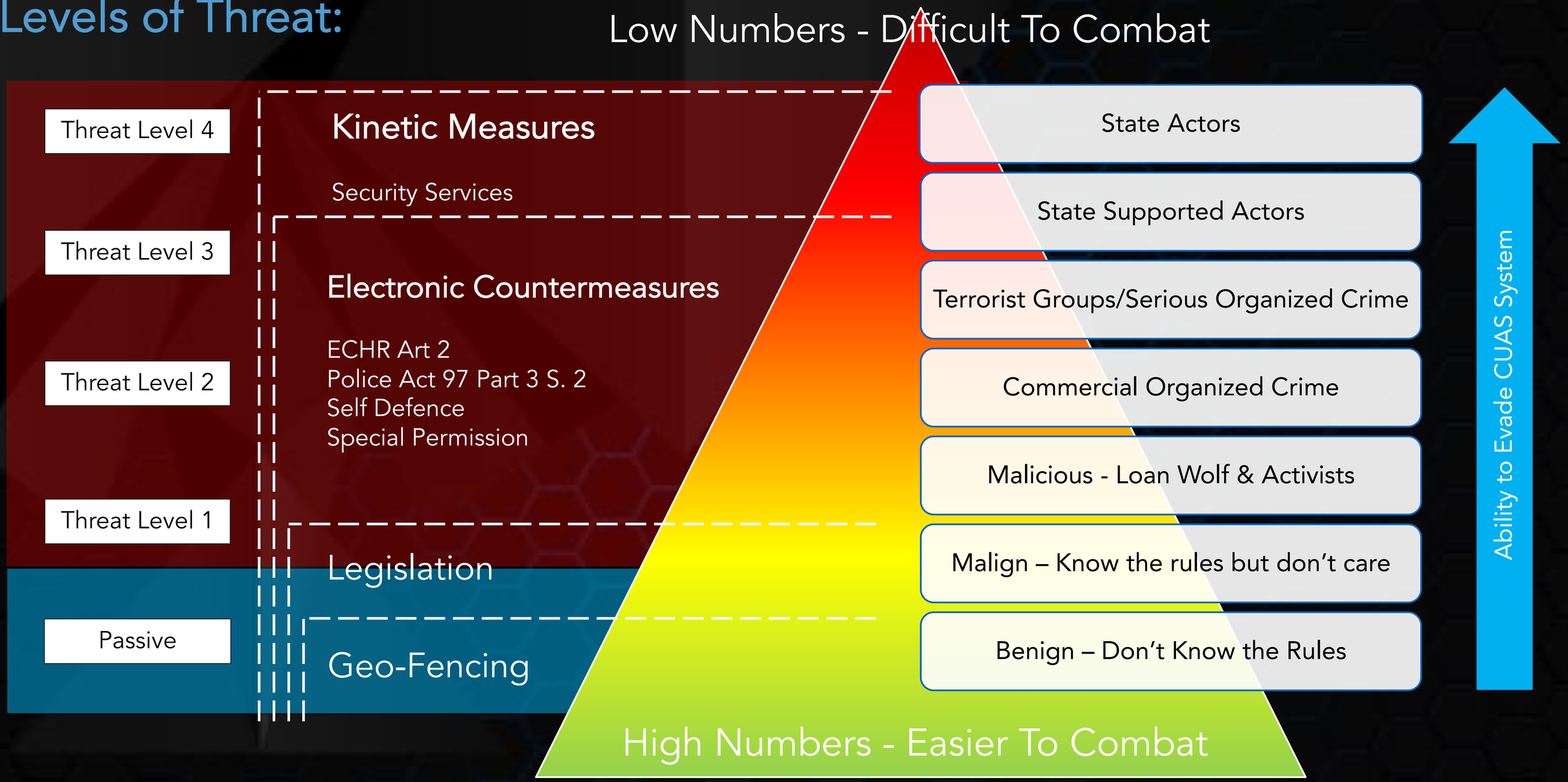
4

DRONEDEFENCE

Drone Flight Planning Cycle

DRONEDEFENCE

Levels of Threat:



Drones Threat Levels:

	Threat Level 1	Threat Level 2	Threat Level 3	Threat Level 4
Actor	Lone nuisance drone user including paparazzi.	Lone activist, terrorist or drone operator with limited criminal intent.	Terrorist group(s), determined activists or drone operators with advanced organized criminal intent.	Medium to high technical ability conducted well supported terrorist groups, advanced criminal networks and state actors.
Intent	Deliberate invasion of privacy.	Hostile surveillance and transport of illicit substances.	Severe economic disruption, mass transport of illicit substances and harm to the population.	Severe economic impact, a 'spectacular' event and multiple casualties.
Technical ability	Low	Low	Medium	High
Evasion Ability	No awareness of drone countermeasures, no defensive measures or actions taken.	No awareness of drone countermeasures, no defensive measures or actions taken.	Some awareness, obscured launch points, RF precautions and autonomous flights.	Extensive awareness, obscured launch points at greater distances, RF precautions and high use of autonomous flights.
Type of Drone	Multi-rotor (commercial with no modifications)	Multi-rotor (commercial with no modifications) Fixed wing (commercial with no modifications)	Multi-rotor (commercial with some modifications) Fixed wing (commercial with some modifications)	Multi-rotor (bespoke systems) Fixed wing (bespoke systems)
Numbers of drones	Single	Single	Two	More than two
Control Method	Real time command and video no autonomous flight	Real time command and video no autonomous flight	Real time command and video with GPS assisted autonomous flight	Real time command and video with advanced autonomous flight (not reliant on GPS)

Which Applies To You?

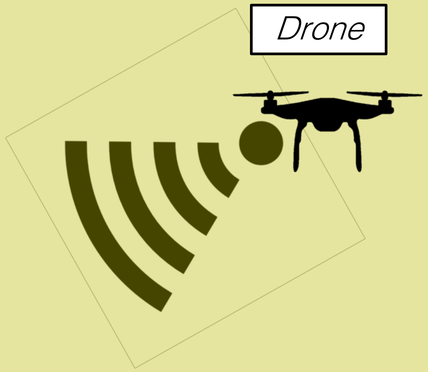
DRONEDEFENCE

Detection Solutions

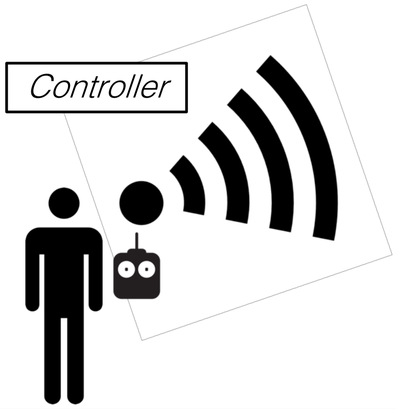
DRONEDEFENCE

GPS

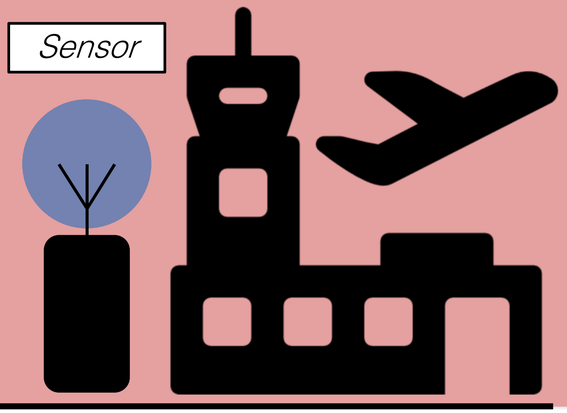
Drone



Controller



Sensor



Detect

Identify

Track

Drone Detection

DRONEDEFENCE

Detection Technology	Threat Level	Range	Pros	Cons
Radar (Detect & Track)	3-4	750m To 5km	Can detect RF silent drones Established Tech	Struggles with ground clutter High False Alarm Rates High Costs 'Active Device' Requires Permission
Cameras (Detect & Identify)	3-4	Up to 1000m (depending on weather)	Capture Image of Drone	Poor Weather Performance High False Alarm Rates Poor against multi targets
Acoustics (Detect)	4	Up to 200m (depending on	Can act as last line of detection	Very poor in built up areas Can't identify or locate
Radio Frequency Analysis (Detect, Track & Identify)	1-2	Up to 5km	Single – Detect & Range & Bearing Multi – Geo-location	Cannot detect a drone when not transmitting Updates Needed

DRONEDEFENCE

Defeat the Device
Mitigation Solutions

Drone Mitigation

DRONEDEFENCE

Technology	Threat Level	Pros	Cons
Directed Energy	4	Can destroy drones Low 'Cost per Kill' Multiple Drone Capable	High capital cost Military Only Export Barriers Limited Suppliers
Kinetic	4	Can destroy drones	High capital cost High 'Cost Per Kill' Export Barriers Limited Suppliers
Physical Capture	4	Last line of Defence Medium 'Cost Per Kill' Can capture all drones	No RF interference Lower barriers for deployment Unable to cope with Multi Drone Attack
Radio Frequency Jamming	1-3	Highly Effective Low to no impact on drone No Cost for Kill	Can interfere with other systems Legislation Barriers

Observe
Sensors

Orientate
Analysis

Decide
GUI

Act
Response

Large Radar
5km +

Radio Frequency
c. 2km

Camera – Visual
Up to 1km

Small Radar
c. 1km

Person – Visual
300m

Acoustic
Up to 200m

Hard

Soft

Kinetic

Spoofing

Jamming

Directed Energy

Subversion

Communications/ Media

Patrolling

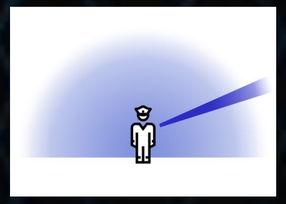
Arrests

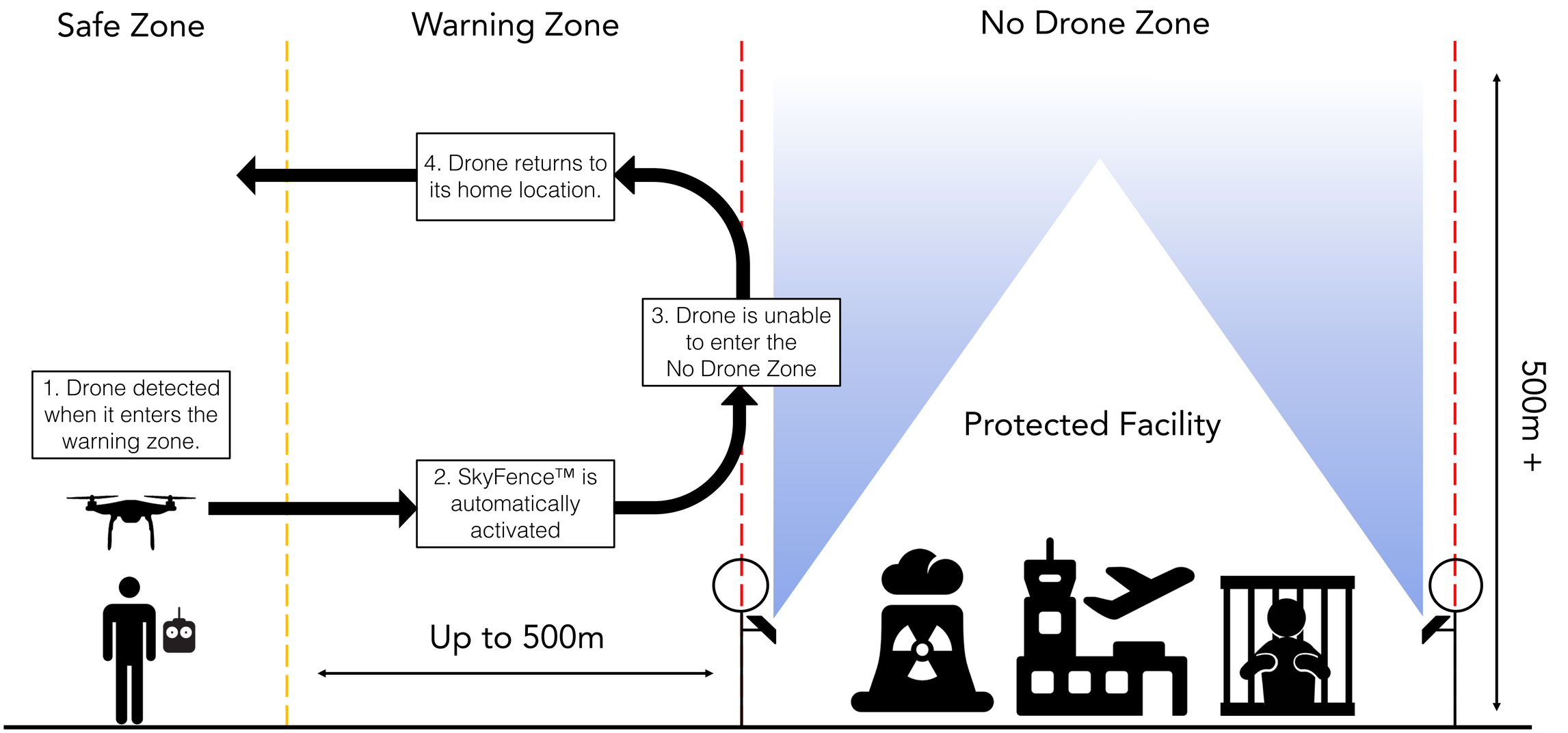
IPE

Legislation

DRONEDEFENCE

Our Mitigation Solutions





© Copyright 2019 – Drone Defence Services Ltd

DRONEDEFENCE

Industry Challenges:

- No industry standards
- Lots of New Entrants
- Early Market
- Legislation yet to catch up
  - Aviation Security Act
  - Wireless Telegraphy Act
  - Prisons Act
  - Police Act
- Develop understanding of drone capabilities and impacts

DRONEDEFENCE

Q & A