Israeli Aviation Cybersecurity Framework

ICAO EUR/NAT DGCA Meeting

DG CAAI – Joel Feldschuh

10 May 2022

Israeli Arena

- Small aviation industry
- Legislation applies to critical systems operators only (IAA - ANSP & Aerodrome operator)
- Increase in cyber attacks on Israeli organizations
- Cyber-security industry with $8.8billion funds raised in 2021 **(40% of global private investment)**
- Advanced National Cyber Directorate (INCD)

Aviation Cybersecurity Evolvement

Building oversight capacity within CAAI

Drafting Regulations

INCD Threat Intelligence Desk

National Transport SOC
(Ministry of Transport)

Establishment of National Steering Committee for Aviation Cybersecurity
(governmental decision)

Establishment of Israeli National Cyber Directorate

National Risk Survey 'Hercules'

2018

2019

CAAI INCD

Cooperation Agreement (MOU)

First audit of air carrier

2020

2021

Drafting National Policy

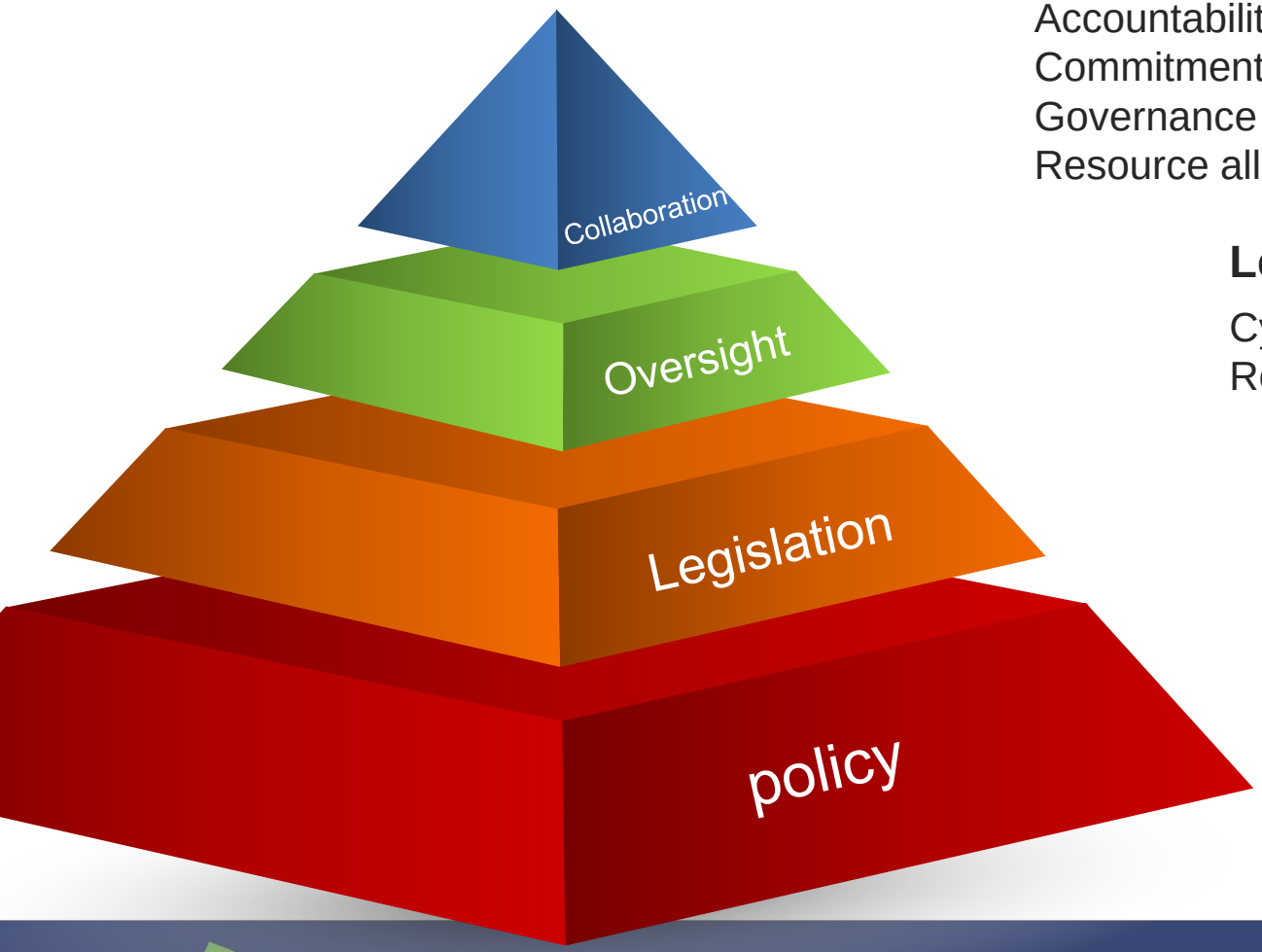
Establishment of Sub-committees
(Regulation, Risk management and Int'l cooperation)

2022

Risk-Based Approach

- Focus on aircraft
- Threat analysis (‘Hercules’)
  - Based on publicly available information
- Who is the potential attacker? What are their capabilities? What is their motivation?
  - Not a binary game (aircraft shot down or nothing)
  - Non-state players might harm safety and cause damage
- Basic layer of protection – initial and continuous airworthiness
- Aircrew training

Establishment of oversight capacity – essential components



Policy

WHY?
Accountabilities & responsibilities of national entities
Commitment of government
Governance at the national level
Resource allocation

Legislation

Cyber – new “technical area”
Regulations – balanced, risk-based

Oversight

Oversight approach
Experts – internal & external
Training – initial and recurrent

Collaboration

National & International

Main Conclusions & Recommendations

- **Act now, even If regulations are not in place yet**
  - Operational and safety consequences as a result of cyber attacks are realistic
  - Raise awareness among organizations' senior management
  - Nomination of information security manager within each organization is a mandatory, first step
- **Learn from others who did it / on process**
  - Policy, regulations, risk-management, oversight approach, personnel
- **Resources**
  - Political will is a cornerstone
  - What is the alternative cost?
- **Recruitment of technical personnel – thinking out of the box**
  - Recruitment of IT experts and provision of tailored training program in collaboration with Cyber authority
  - Using external experts is power multiplier. Attention to heterogenic expertise in your experts team

Thank you!