Panel 5: Assessing, Detecting and Responding to RAS Threats

Moderator: Professor Stéfanie von Hlatky, CIDP, Queen's University

Dr. Guy Vézina, Director General S&T Army, Defence R&D Canada
Col Richard Dickson, Commander Canadian Army Land Warfare Centre
Questions

Q. How RAS adversary systems, either non-lethal or lethal, will affect our own tactical operations;
Q. Whether these threats should be anticipated given technical, legal, moral and ethical constraints of state, non-state and individual actors;
Q. How will unstructured/complex environments and unpredictable/evolving scenarios affect our abilities to respond; and
Q. How should Canada approach the development of capabilities to counter such systems?
Q. How RAS adversary systems, either non-lethal or lethal, will affect our own tactical operations;

- *multiplier, distance, 24/7, multi-roles, disruptive ...*

- *lethal vs non-lethal - rules? who said rules?*

- *friend or foe – behaviour predictability?*
Q. Whether these threats should be anticipated given technical, legal, moral and ethical constraints of state, non-state and individual actors;

- technical - really!
- legal - really.
- moral - really?
- ethical - really...
Q. How will unstructured/complex environments and unpredictable/evolving scenarios affect our abilities to respond; and

- “more places to hide, more places to fail”;
- “military objective or not” - interpretation of location/purpose/use;
- rules on “distinction, proportionality, and precautions in attack”;  
- “predicting adversarial behavior” accounting for tech limits/strenghts;

- **challenge**: coding & decoding behavior (resilience and performance) of platforms as well as human-system trust and confidence in complex environments.
Q. How should Canada approach the development of capabilities to counter such systems? <<OODA cyber-physical-human>>

1. **Threat Modeling & Assessment**
   - Range, payload, manoeuverability, signature, navigation, comms, platform, weaponization, level of autonomy/intelligence, human control interface, red teaming, conops, operational effectiveness against blue force / adversarial mission effect assessment, swarm/saturation;

2. **Threat Detection & Behavior Prediction**
   - Sensor modeling, sensor performance assessment with respect to threats/conops/weather/day-night, intelligence, red intent assessment

3. **Threat Counter-measure**
   - hard kill, soft kill, comms/navwar override, decoy, shadowing, legal and policy aspects.

4. **Experimentation** (virtual, live and constructive)
   - Build surrogates, use decoy, validate detection, prove counter-measures, embed in field exercise, inject in iterative procurement