

Data Policy – UK & international security perspective

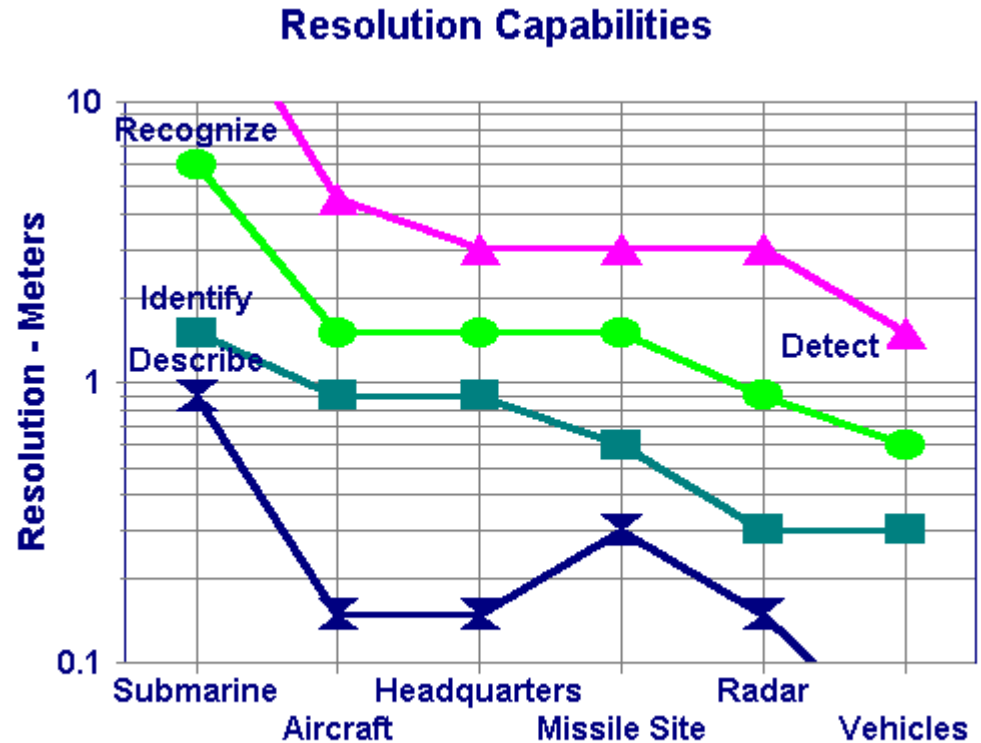
Pat Norris*

Space & Defence Strategy Manager

* author of *Spies in the Sky*

Security – protecting our troops

- Satellite-based remote sensing data can put UK military forces at risk
 - especially as the image resolution improves
 - and imaging radar overcomes cloudy & night-time conditions
- US licensing regime for <1 metre imagery attempts to address this:
 - 24 hour hold on the data
 - licensing of data exports
- Similar Euro regimes emerging
 - need for coherence/coordination of these various arrangements
- There is also a need to educate our forces concerning the risks presented by satellite imagery
 - and train them in counteractions, both active (deception) and passive
 - very little experience of interpreting hi-res SAR imagery in military contexts



Privacy

- We often forget that members of the armed forces are also UK citizens
- Their privacy is often more sensitive than that of their civilian fellow citizens because invasions of their privacy may result in death or injury
- As images become available with sub-metre resolution are we reaching the point where individual privacy is being infringed?
 - e.g.: individual vehicles can be detected and some elements of vehicle identification are possible

Security – rights of the sensed state

- The UN remote sensing principles* may not be legally binding but have some status as a statement of best practice
- They establish the concept of the country being imaged by a satellite (the “sensed state”) and give it certain rights, including:
 - Principle XII: the sensed state shall have access to primary and processed data at reasonable cost
 - Principle XIII: the country that owns the satellite shall cooperate with the sensed state to “enhance the mutual benefits to be derived therefrom”
 - Principle IV: the remote sensing “shall not be conducted in a manner detrimental to the legitimate rights and interests of the sensed state”
- On the face of it these Principles give a sensed state quite a lot of rights and should enable our forces in, say, Iraq (through the Iraqi government) to delay the publication of compromising imagery from satellites of a third party

* Principles Relating to Remote Sensing of the Earth from Outer Space

The proactive option

- The options for a sensed state in the event of a sensing country being in breach of the UN Principles are not defined
 - nor are they explicitly limited
- There is anecdotal evidence of actions being taken by sensed states to deceive the satellite imagery of another state
 - certain forms of deception are explicitly forbidden in various arms limitation and reduction treaties
 - by implication deception is not forbidden in other agreements where it is not mentioned
 - such deception can be active, e.g.: heaters to simulate operating equipment and people
- It seems not excluded therefore that a sensed state could extend this use of electromagnetic transmitters as a form of active deception:
 - radio, against imaging radars
 - optical/IR against optical/IR
 - Open Skies Treaty seems too narrowly focused to exclude such actions

Nuclear Non-Proliferation Treaty (NPT)

- As a signatory of the NPT, the UK is committed:
 - (Article VI) to “seek effective measures relating to cessation of the nuclear arms race”
 - (Article I) “not to induce any non-nuclear weapon State to acquire nuclear weapons”
- This has historically been taken to mean that the UK should reduce its nuclear arsenal and delivery platforms
- An additional activity that UK could undertake is to help create an assured source of satellite surveillance data that can't be blocked by “cheque book” or political shutter control
 - give non-nuclear State assurance of early warning of major military actions by a potential adversary
 - reduce need for that State to have a nuclear deterrent
 - defuse tension and demonstrate good faith by the major powers
- Such an initiative would open up new areas of data policy to address
 - who has access to which assured data, e.g.: UN Forces would be exempt

International exchange of sensitive data

- Exchange of classified satellite imagery between European countries has proved difficult:
 - statements by French and German officials attest to this for Helios-2 & SAR-Lupe
 - complex ground facilities are required to ensure access to imagery is compatible with data policy and other legal restrictions in each country
- Introduction of the European Union into the equation is not always a positive step:
 - the EUSC (Torrejon) does not yet have access to classified Helios imagery whereas the WEUSC (its precursor) did
 - the status of the EU institutions in relation to classified data of Member States is complex
- ESA is slightly more advanced (thanks to Galileo) in establishing its legal status as concerns classified data, information and systems

QUESTIONS?