MSG-151

Cyber Effects in Campaign and Mission Simulations

and

IST-156

Modelling and Simulation S&T: Critical Enabler for Cyber Defence

Bharat Patel
UK National Lead Member
NATO MSG & SCI Panel
DSTL, UK MoD

Background

NATO M&S Master Plan:

“M&S, which has traditionally concentrated on the kinetic effects of warfare, must now also focus on… human behaviour, asymmetric threats, [and] information superiority”

- **Modelling and simulation of manoeuvre warfare is much more mature than M&S for cyber and information operations**
- **MSG-117 on M&S for Cyber Defence, 2012 – 2015**
- **MSG-151 was stood up as a result to address MSG-117’s findings. 2017**
  - Cooperated with IST-156 to bring the M&S and IST communities together

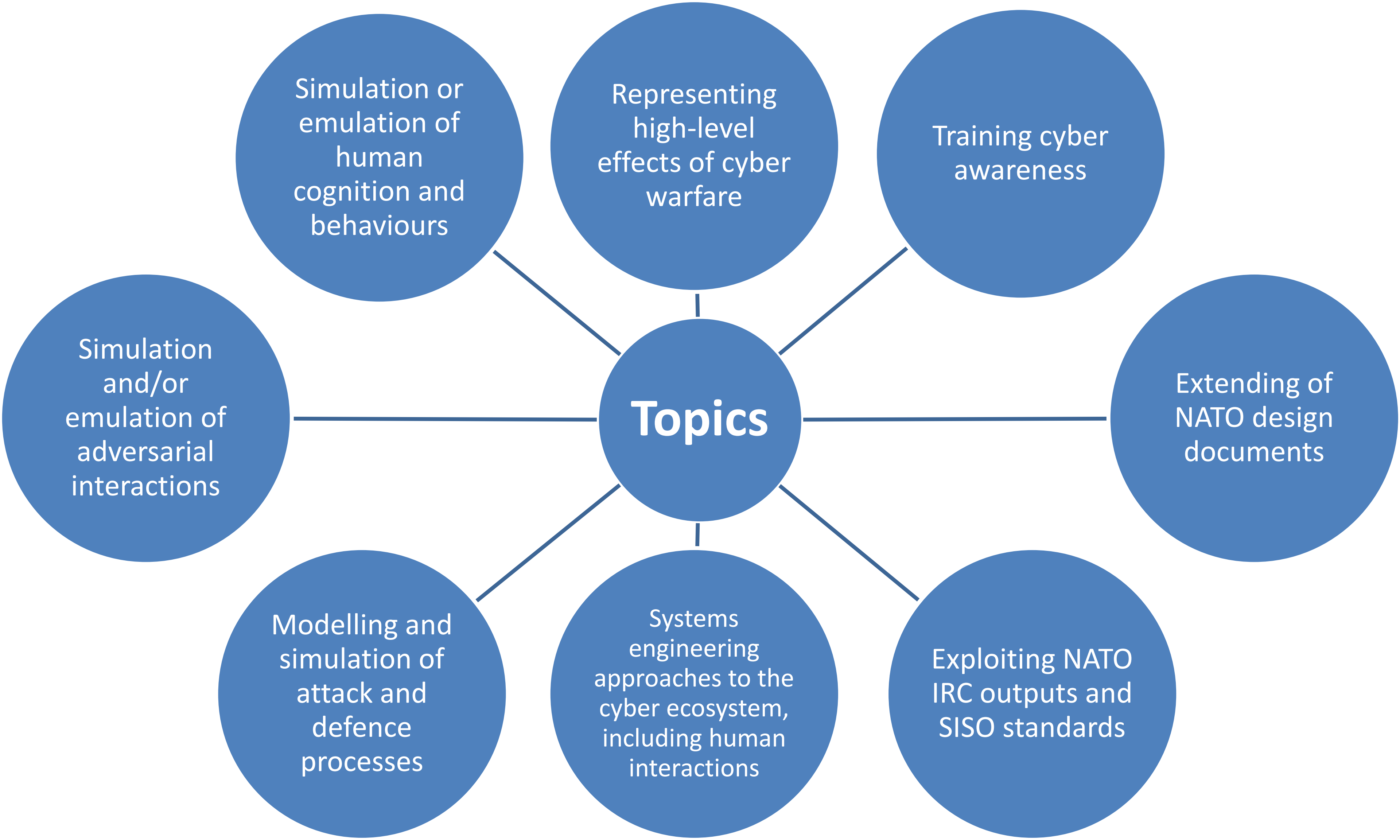
Objectives

MSG

- Provide collective insight into the art of the possible regarding M&S techniques in the cyber domain
- A list of specific challenges that need to be addressed to maximise the benefit of M&S for cyber-related training and mission rehearsal
- Insight on how the M&S and the cyber domain may evolve in the future, and the opportunities and threats this poses

IST

- Provide a forum to discuss the S&T developments that could be leveraged and form an integral part of a model-driven approach, including systems engineering
- To arrive at a better representation, with varying levels of fidelity, of the socio-technical system (of systems) that comprise the cyber ecosystem, their security, and defence against cyber threats



Topics

Simulation or emulation of human cognition and behaviours

Representing high-level effects of cyber warfare

Training cyber awareness

Extending of NATO design documents

Exploiting NATO IRC outputs and SISO standards

Systems engineering approaches to the cyber ecosystem, including human interactions

Modelling and simulation of attack and defence processes

Simulation and/or emulation of adversarial interactions

Attendance

- **Approximately thirty people attended the first two days, with attendance of around twenty on the final day, from 8 nations (BEL, CAN, DEU, ESP, GBR, NLD, SWE, USA)**

- **90-minute slots for presentation and discussion, plus future activity generation**

Presentations

1. **MSG-117 M&S for C2SIM**
   Jack Bramhill (Dstl) on behalf of Bharat Patel (Dstl)

2. **Extending Computer Generated Forces (CGF) Architectures to Support Information Warfare and Cyber Effects**
   Mark Hazen (DRDC)

3. **Extension of NATO design documents to Accommodate Cyber Defence: Position Paper**
   Perri Nejib and Dennis McCallam (Northrop Grumman)

4. **Situational Awareness on the Highest level of the Internet - Consequence Prediction of Events**
   Bert Boltjes (TNO)

5. **Understanding the Mission Impact of a Cyber Attack in a System of Systems Environment**
   Chris Lang and Bob Madahar (Dstl)

6. **Development of a conceptual model to support information and cyber warfare effects in modelling and simulation systems**
   James Kearse (Thales UK)

7. **JUMP: Concept Demonstrator for Cyber Mission Planning**
   Antony Waldock (BMT Defence Services)

8. **C2-Simulation interoperability and its applications for cyber simulation**
   Mark Pullen (GMU)

Discussions Topics addressed by 4 Groups

1. How will the cyber operating environment change in the future?

2. What key elements must we model to represent cyber effects?

3. Where can M&S have the greatest impact in cyber decision making?

4. Representation of human effects in cyber M&S

How will the cyber operating environment change in the future? (1)

- Increased liaison by hostile state actors
- Effect on procurement: Improve Resilience (Cost?)
- integration between cyber operators and other personnel
- Increase in internet of things
- Generate distrust of colleagues, systems and messages received
- Inducing panic

How will the cyber operating environment change in the future? (2)

- Cyber to become an increasingly dominant part of warfare
- Increased numbers of dark nets, back doors, non-attribution, unknown/distributed locations
  - Detecting cyber operations challenging
- Increased conflict between government and corporate security and personal data privacy
- Increase in autonomy; tendency to keep the human out of the loop (not only commercial drones or self-driving cars)
- Machine learning can detect suspicious cyber activity, as long as systems are monitored

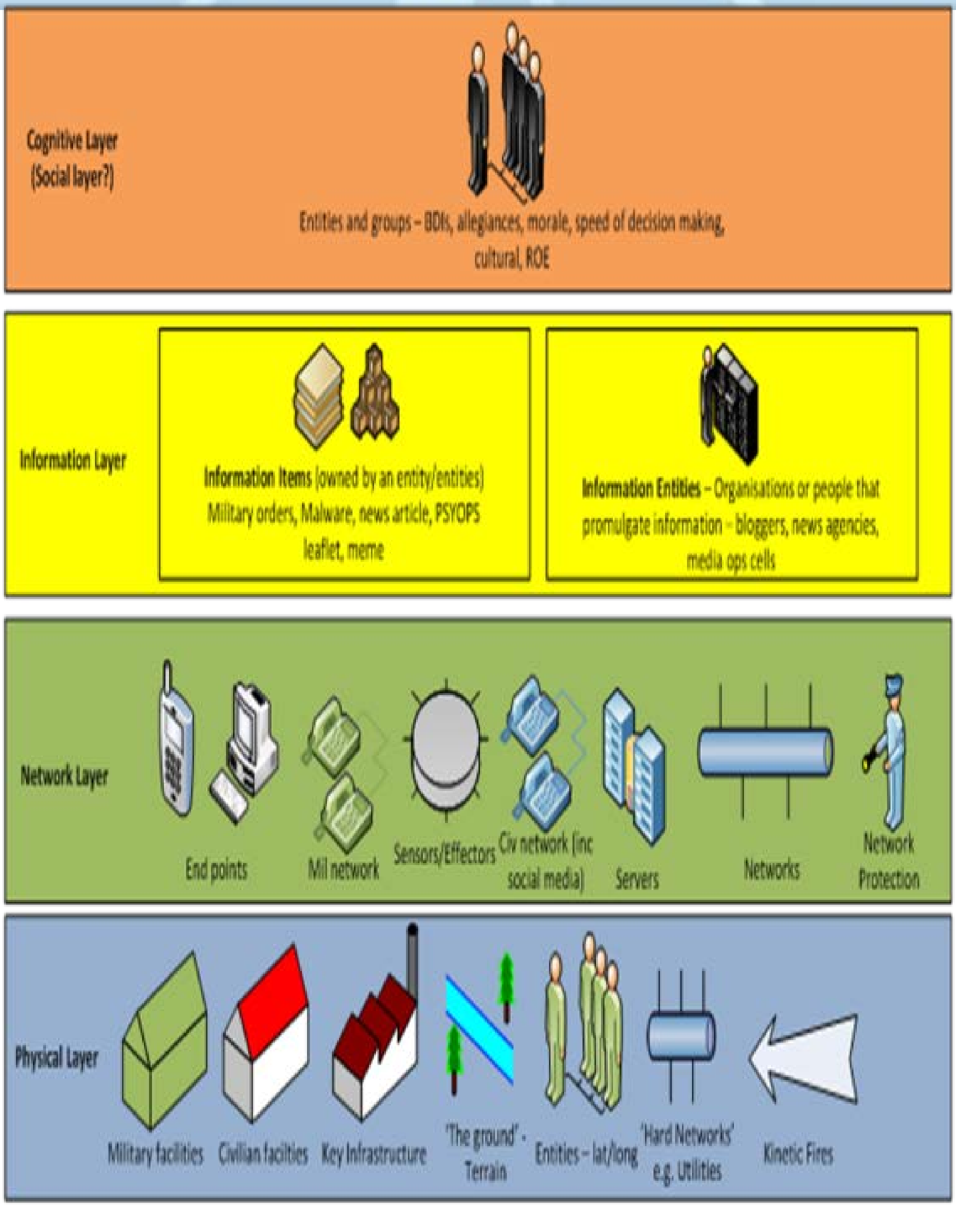
How will the cyber operating environment change in the future? (3)

- Increase in amount of Data and Digitisation
- Ability to validate information: Reality vs fake news
- Increased access to processing power (Cloud to Quantum Computing)
- Massive increase in physical sensors – data availability and derivation
- Backups and sophisticated “lay-low” attacks
- Increase in wearables which may be targeted

How will the cyber operating environment change in the future? (4)

- Quantum encryption/decryption
- Augmented reality interfaces are ubiquitous
- Quick speed of evolution
- Legal framework/rules of engagement agreed for global cyber operations/targeting
- Improved classification of threats and threat actors
- Increased military participation in cyber and electromagnetic activity (CEMA)
- Greater awareness of threat by the general public and military users alike leading to better security.

Proposed UK/CAN IW Layer Model



Cognitive Layer
(Social layer?)

Entities and groups – BDIs, allegiances, morale, speed of decision making, cultural, ROE

Information Layer

Information Items (owned by an entity/entities) Military orders, Malware, news article, PSYOPS leaflet, meme

Information Entities – Organisations or people that promulgate information – bloggers, news agencies, media ops cells

Network Layer

End points

Mil network

Sensors/Effectors

Civ network (inc social media)

Servers

Networks

Network Protection

Physical Layer

Military facilities

Civilian facilities

Key Infrastructure

'The ground' - Terrain

Entities – lat/long

'Hard Networks' e.g. Utilities

Kinetic Fires

What key elements must we model to represent cyber effects?

- Need a range of fidelity, from very high level down to engineering level modelling
- Higher-level effects tend to be more straightforward to implement and more reusable than engineering-level
- Generate a list of cyber effects that must be represented
- Model of defences against attacks
- Layered model of Information Warfare (UK/CA Model).

Where can M&S have the greatest impact in cyber decision making?

- **Use of (commercial) games in conjunction with cyber and information models to support training of senior leaders**
- **Supporting software for operations to take decisions in the cyber domain.**
  - Physical effects
  - Influence effect
- **Supporting software for cyber defence for ops**
  - Situational awareness for your own systems
  - Model mission impact of cyber attack in system of systems.

Representation of human effects in cyber M&S (1)

- The effects of human interaction are the predominant contributors to system of systems complexity
- Understanding ambiguous communication to fully represent social media
- Symbology for cyber assets and events
- Different levels of human behaviour: strategic, tactical, operational, learning/training

Representation of human effects in cyber M&S (2)

- Topology / Architecture
  - Partition into a few high level attributes: psychological, physiological, cultural, sociological
  - Breaking behaviours into discrete actions that can be modelled
  - Humans cause disruption; Model assumptions as well as uncertainty
- Review/Baseline existing knowledge and expertise
  - Related work going in in nations, human factors work in IINCOSE
  - Look at interactive gaming to aid in understanding of human representation
  - Look at key elements that marketing use to represent human elements?

Activity recommendations

- An exploratory team to produce a “top ten” list of effects/attacks/countermeasures and counter-effects that are most worth modelling. (see new TAP led by NLD)
- Exploratory teams on the applicability of international law to cyberspace, and how current trends are likely to complicate the future cyber landscape. This may be supported by a lecture series on the Tallinn manual.
- An exploratory team to study the applicability of modifying commercial-off-the-shelf software and games techniques to improve strategic decision support. It may also investigate any gaps in the ability of CGF software to model cyber attackers/defenders.
- A task group for identifying ways to improve situational awareness of friendly assets vulnerable to cyber attack.
- A workshop to focus on producing a coherent taxonomy and symbology for cyber events, working across NATO HFM, MSG and IST panels.

Finding effective ways to defend against cyber attacks relies not only on applying security and assurance systems, but also having trained and educated staff who are aware of those systems, the risks involved, and the actions to take to defend against cyber intrusions and attacks.