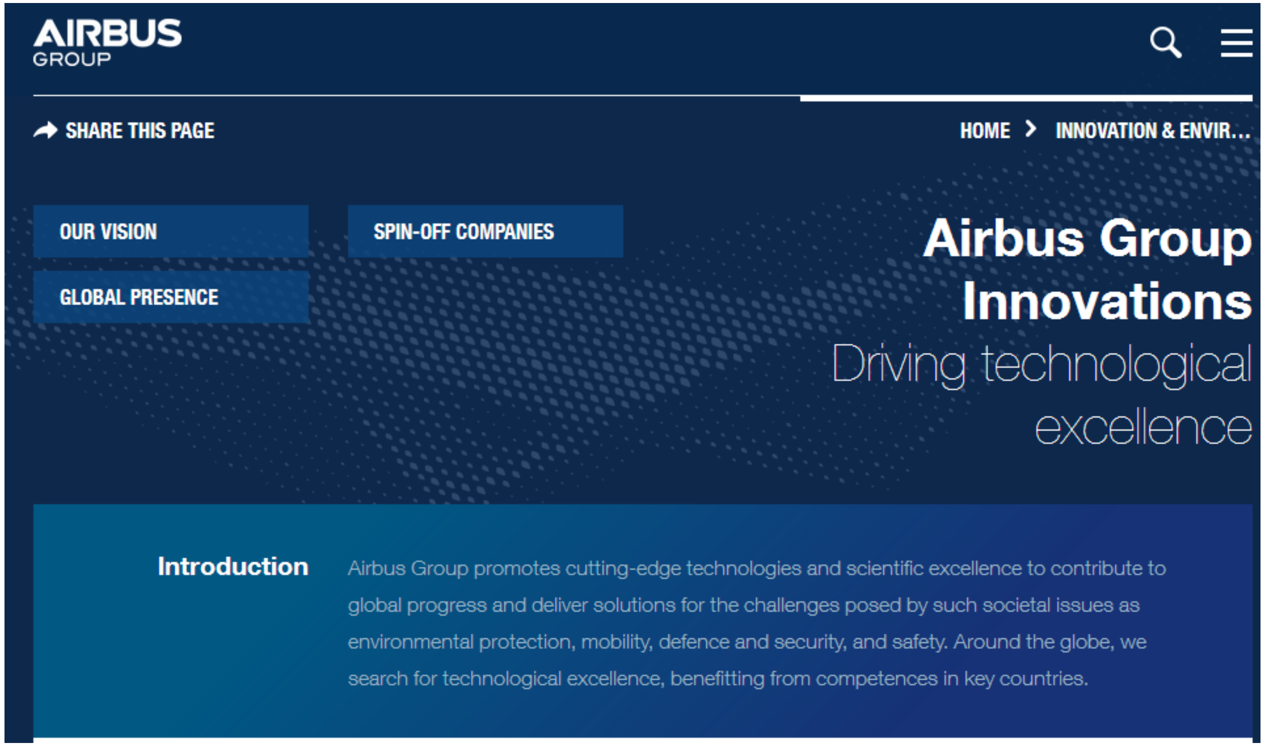
Cross-Domain Situational Awareness and Collaborative Working for Cyber Security

Devon Hansen, Mark Hall, Kevin Jones

8 June 2015

Airbus Group Innovations



Airbus Group Innovations
Driving technological excellence

Introduction Airbus Group promotes cutting-edge technologies and scientific excellence to contribute to global progress and deliver solutions for the challenges posed by such societal issues as environmental protection, mobility, defence and security, and safety. Around the globe, we search for technological excellence, benefitting from competences in key countries.

Mark Hall: *Research Engineer for Visual Analytics & Knowledge Capture*
Devon David Hansen: *Research Engineer for Games Technologies*
Kevin Jones: *Research Team Leader - Cyber Operations*

This work is sponsored by Defence Science and Technology Laboratory (DSTL) as part of the Cyber Situational Awareness programme

Introduction

The Problem

- Increasing complexity of organisations

- Critical operational decisions need to be taken in situations which require collaboration within multi-disciplinary organisations

- Improved situational awareness for collaboration will lead to better decisions and improved operations

Introduction

Research Question

- How can we improve our understanding of cross-domain situational awareness to influence the design of future collaborative systems?

Contribution

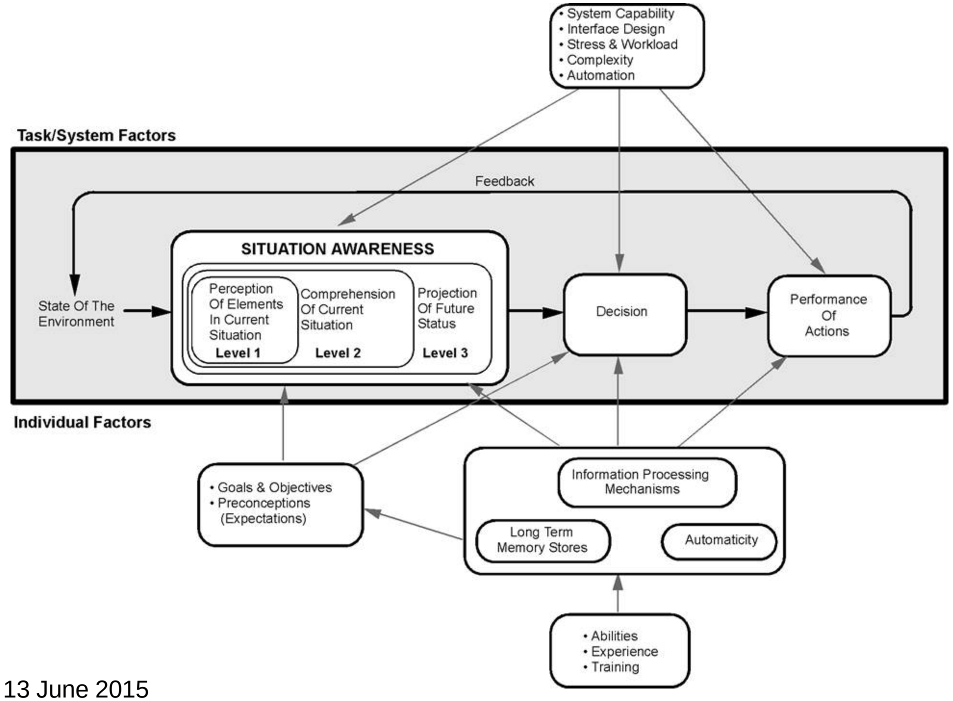
- This paper presents and discusses a theoretical model for situational awareness for cross-domain working, aimed to improve understanding and impact the future development of collaborative systems.

- A use-case is discussed within a military context of the use of this model for cross-domain working between an operational-domain and cyber security-domain.

Background

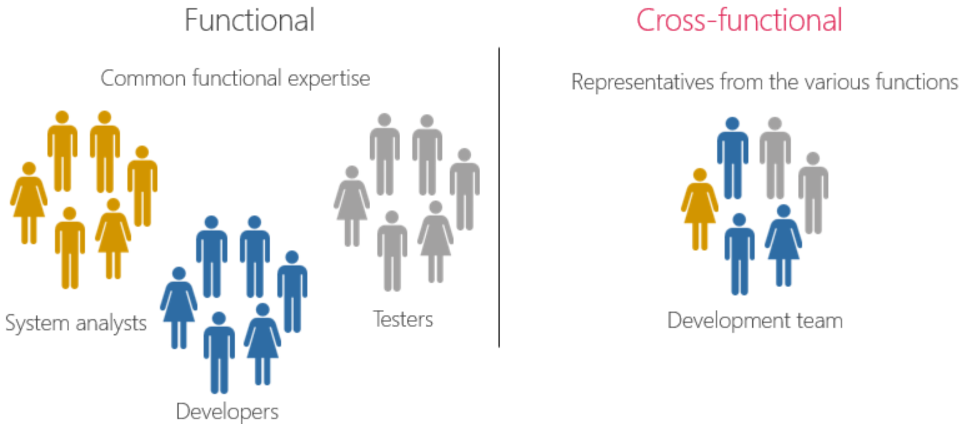
Situational Awareness

SA can be described as ‘*the perception of the elements in the environment within a volume of time and space (level I), the comprehension of their meaning (level II), and the projection of their status in the near future (level III)’* (Endsley, 2000)



Cross-Domain/Functional Working

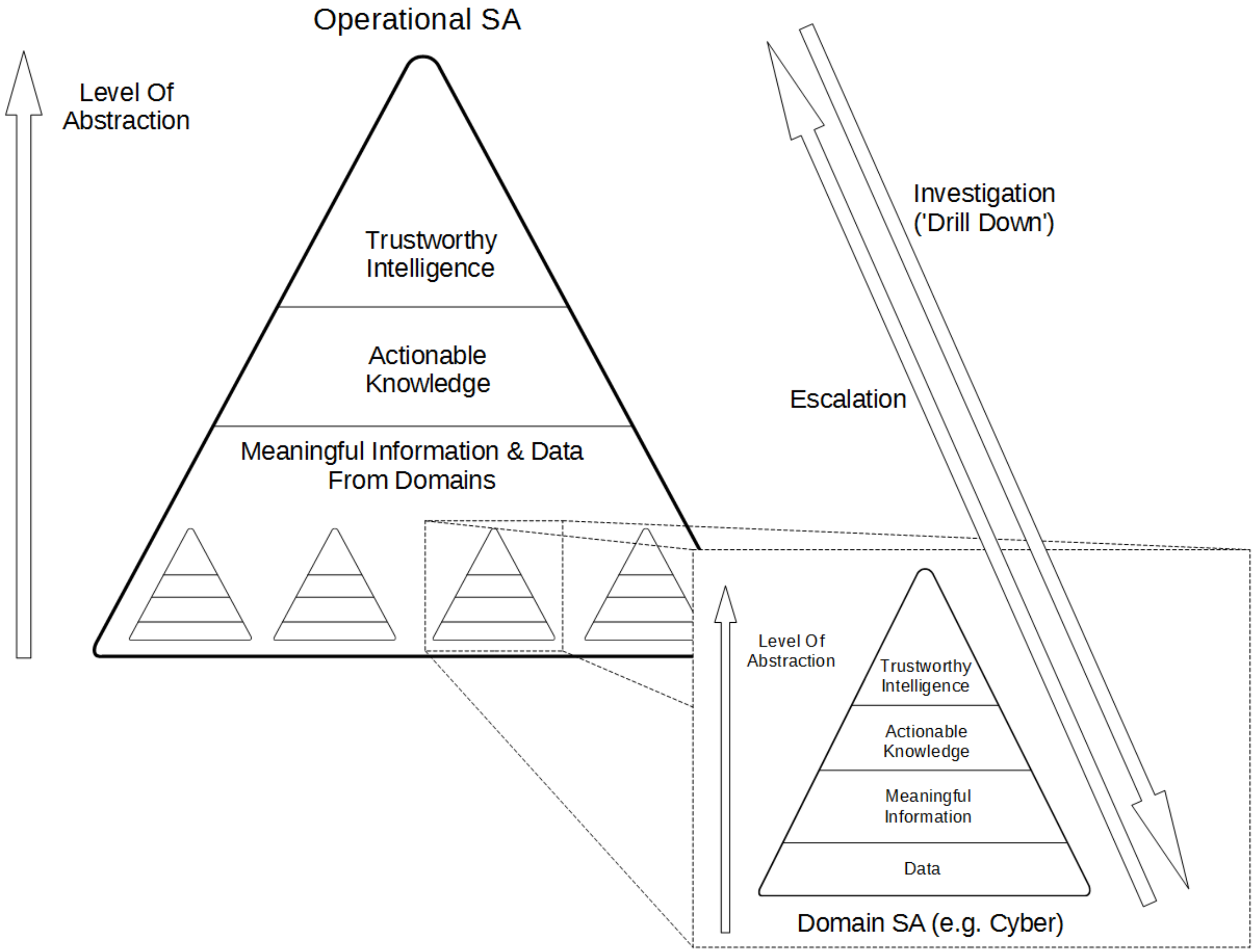
Group of people with different expertise working towards a common goal (Krajewski et al., 2006). This is often seen in Cyber with multiple different areas worked in (e.g. hardware, software, policies, logistics, etc)



Source: http://www.bebetterleader.com/how-do-i-form-teams/

Cross-Domain Situational Awareness for Cyber Security

- Cyber SA can be seen as a subset of an organisation's overall SA

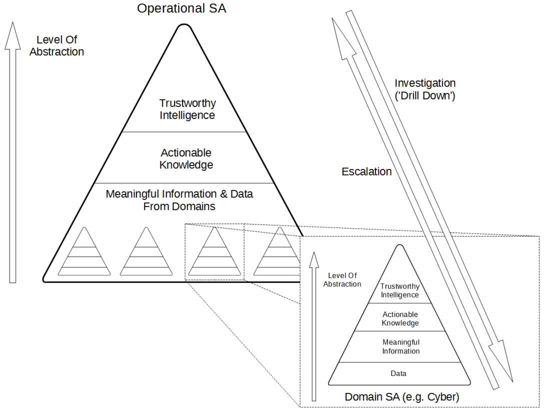


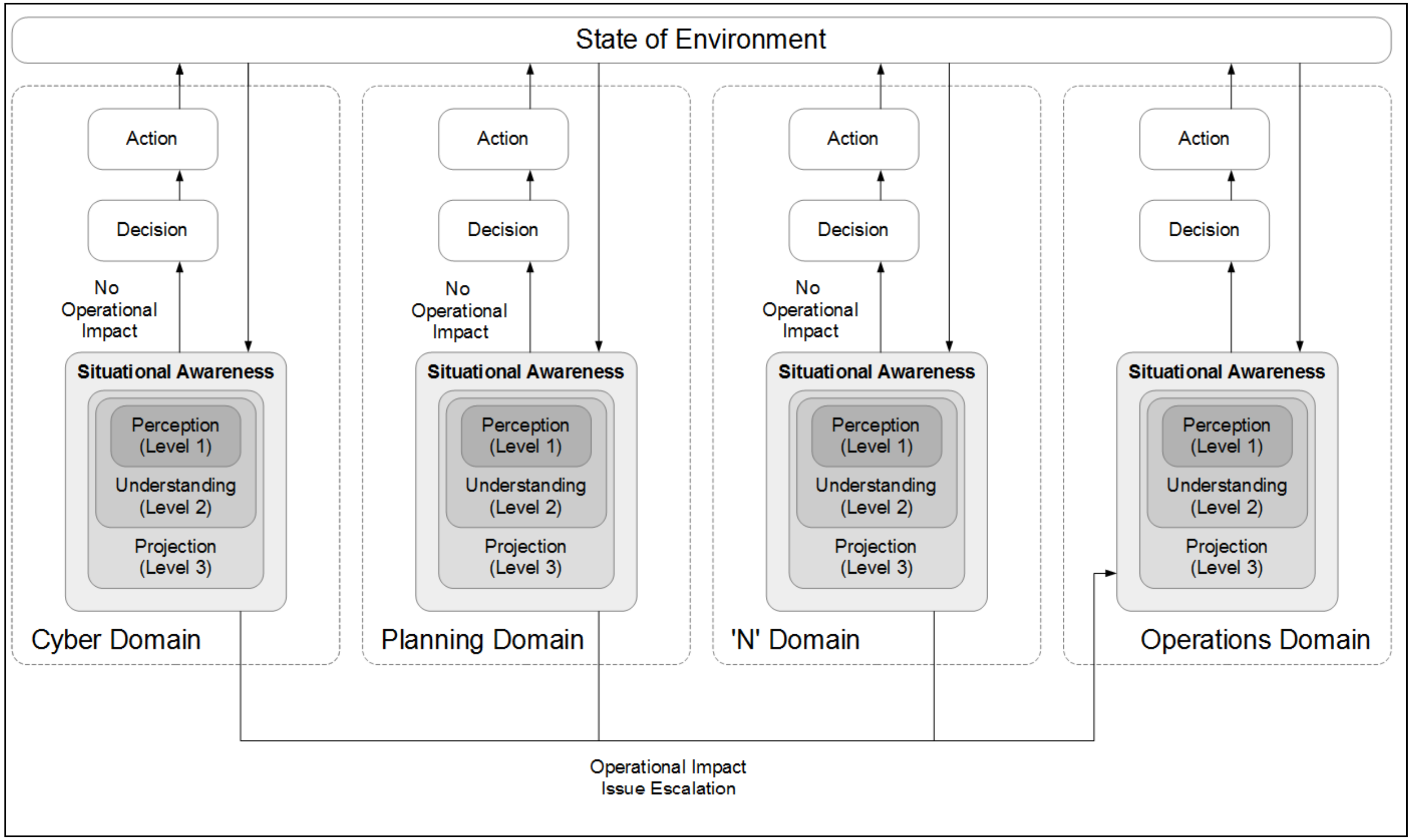
Knowledge – *i.e. the internal belief state of a person...it may be created by integrating information with one's existing knowledge (McAlpine, 2010)*

Information – *i.e. the data plus the meaning connected to it (Wilson, 1987)*

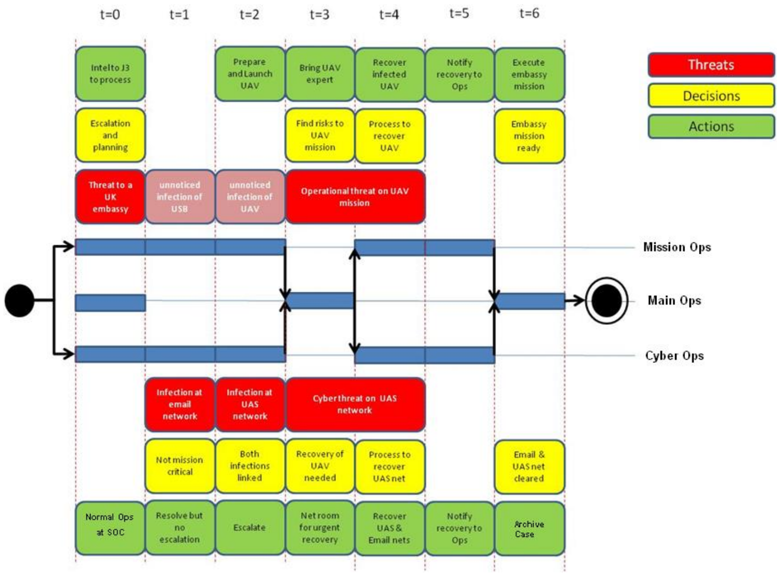
Data – *i.e. unprocessed facts, without discernible meaning to the observer (Fosket, 1996) (McAlpine, 2010)*

Cross-Domain Situational Awareness for Cyber Security





Model in Action: Use Case Walkthrough



t=0	t=1	t=2	t=3	t=4	t=5	t=6
Intel to J3 to process		Prepare and Launch UAV	Bring UAV expert	Recover infected UAV	Notify recovery to Ops	Execute embassy mission
Escalation and planning			Find risks to UAV mission	Process to recover UAV		Embassy mission ready
Threat to a UK embassy	unnoticed infection of USB	unnoticed infection of UAV	Operational threat on UAV mission			
	Infection at email network	Infection at UAS network	Cyberthreat on UAS network			
	Not mission critical	Both infections linked	Recovery of UAV needed	Process to recover UAS net		Email & UAS net cleared
Normal Ops at SOC	Resolve but no escalation	Escalate	Net room for urgent recovery	Recover UAS & Email nets	Notify recovery to Ops	Archive Case

Major Events

Spear Phishing Attack Leads to Malware Infection

USB Stick Used to Transfer UAV Intelligence Data from UAV Network – USB Stick Infected

USB Stick Used on UAV Network Infecting Devices (Bridged Airgap)

UAV Infection Detected and Incident Response Required

Ben Birchall/PA Wire

GOSCC

- Head of Cyber
- Cyber Analyst #1
- Cyber Analyst #2

Airbus Defence & Space

- Expert

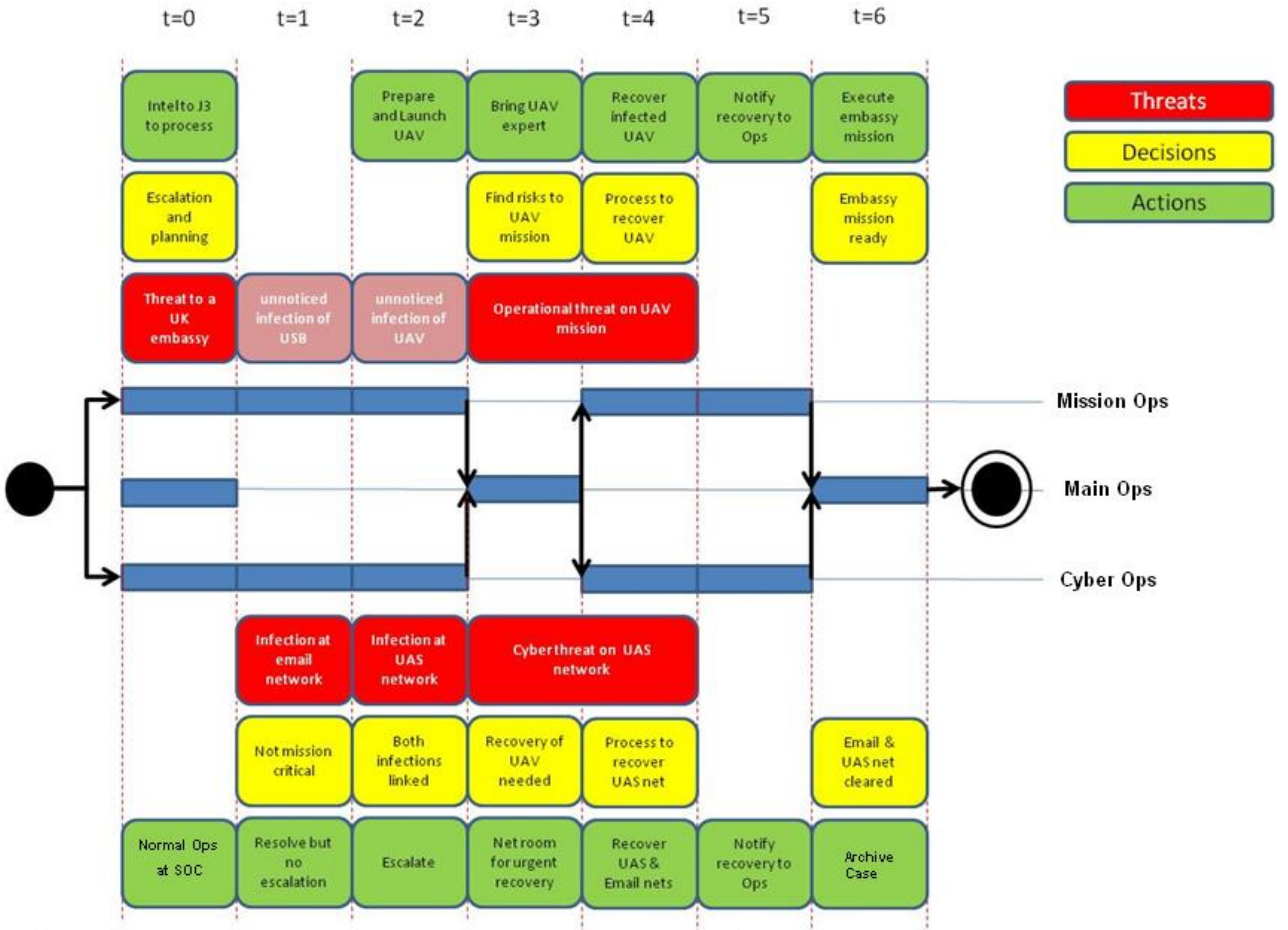
London

- J2

Afghanistan

- J3
- Email User
- UAV Operative

Use Case Walkthrough



t=0	t=1	t=2	t=3	t=4	t=5	t=6
Intel to J3 to process		Prepare and Launch UAV	Bring UAV expert	Recover infected UAV	Notify recovery to Ops	Execute embassy mission
Escalation and planning			Find risks to UAV mission	Process to recover UAV		Embassy mission ready
Threat to a UK embassy	unnoticed infection of USB	unnoticed infection of UAV	Operational threat on UAV mission			
Infection at email network						
	Infection at email network	Infection at UAS network	Cyber threat on UAS network			
	Not mission critical	Both infections linked	Recovery of UAV needed	Process to recover UAS net		Email & UAS net cleared
Normal Ops at SOC	Resolve but no escalation	Escalate	Net room for urgent recovery	Recover UAS & Email nets	Notify recovery to Ops	Archive Case

🟥 Threats

🟨 Decisions

🟩 Actions

Conclusion

Future collaborative systems should:

- Facilitate the appropriate escalation of issues that are likely to have an operational impact based on operating constraints
- Empower personnel lower in the organisational hierarchy to make decisions if the operational impact falls within operating constraints
- Facilitate issues to be investigated when necessary to the appropriate suitable level of abstraction
- Address collaboration issues to facilitate the following capabilities (Saarani, 2012)
    1. Communication
    2. Information sharing
    3. Co-ordination

Future Work

- Formally validate the model and understand limitations
- Improve any future iterations