model futures
www.modelfutures.com

presents:

IntegratedEA

STRATEGY • OPERATIONS • TECHNOLOGY

www: http://www.integrated-ea.com
HashTag: #IEA12
Twitter: @IntegratedEA

VEGA
A Finmeccanica Company

NITEWORKS

Abatis

TEAM ENSURE

de&s

Generic
YOUNG SPIRIT | SENIOR MIND

MooD
SMARTER DECISIONS

Reply
glue

mega

NITEWORKS

Embedding Architecture in the Enterprise

Integrated-EA 2012

Wg Cdr Alex Hicks – Cap ISTAR DPD Lead Planner
Luke Tucker - Niteworks

NITEWORKS

Outline

- Background
- Approach
- Benefits
- Lessons
- Wider Adoption

NITEWORKS

Background

- The ISTAR & IO Enterprise (and Defence more generally) has historically provided specific, bespoke, domain and platform centric solutions to deliver Military Capability.

- The Direct, Process & Disseminate Capability Investigation (DPD CI) sought to identify gaps, overlaps, shortfalls, redundancy and project inter-dependencies in the DPD portfolio in order to support the development of a coherent, affordable and viable DPD Capability Management Plan.

NITEWORKS

Approach

- Developed a Service Taxonomy based upon Doctrine
- Profiled projects within the DPD portfolio against the Service Taxonomy
- Enabling the identification of functional overlaps and inter-dependencies
- Use of differentiators to characterise projects and prioritise further intervention

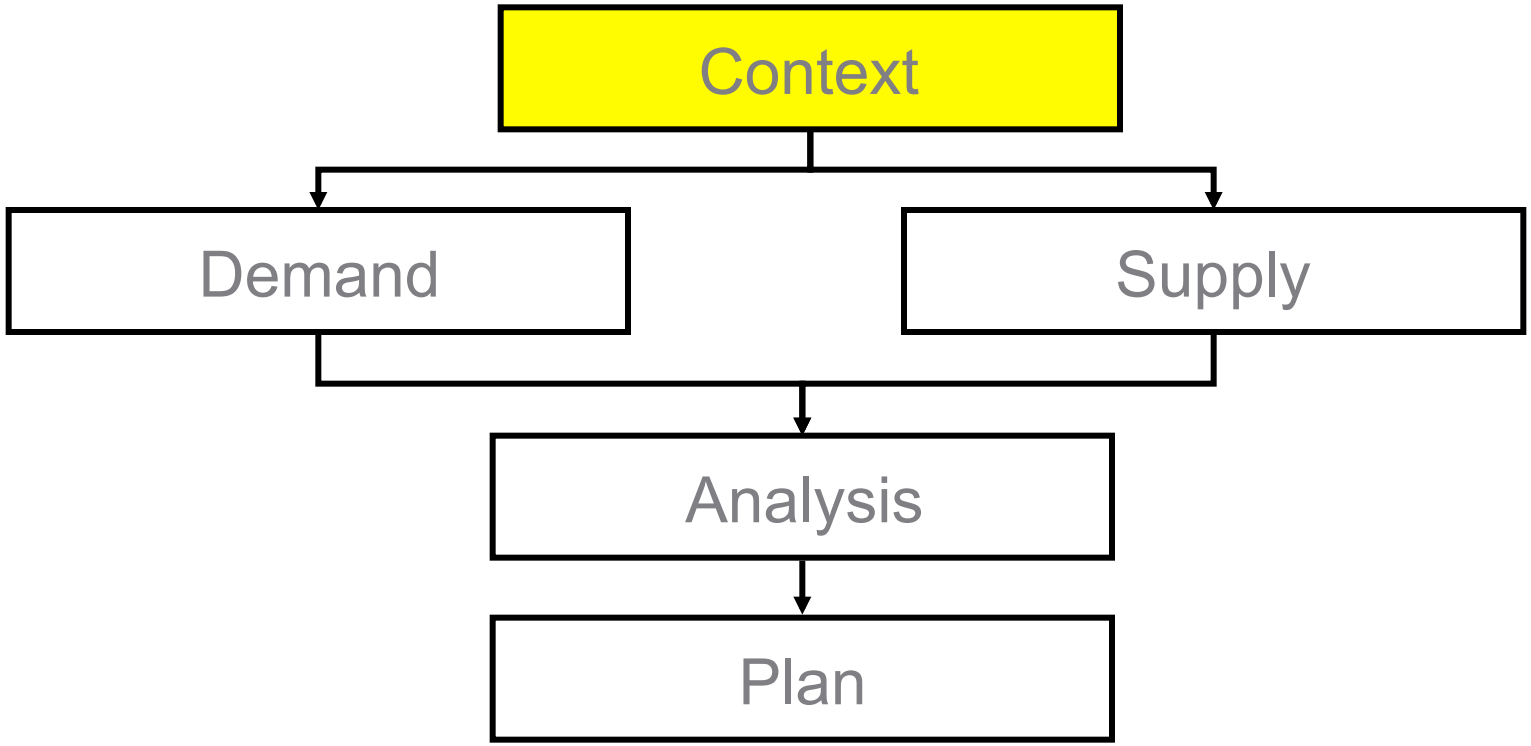
NITEWORKS

Wing Commander Alex Hicks

Direct Process and Disseminate (DPD) Approach

NITEWORKS

Approach - DPD Capability Planning Process



NITEWORKS

SDSR Deductions

SDSR Readout

Intelligence Capabilities

"Our intelligence capabilities will support the increased emphasis on identifying threats and opportunities early, shaping development and preventing threats from emerging. Operating flexibly, we will:
focus intelligence collection and assessment on providing strategic insight and understanding, to inform policy and decision-making
provide early indications and warnings of the intentions of hostile or potentially hostile state and non-state actors, and insights into their capabilities
work to identify the scope and scale of terrorist and weapons proliferation networks, which can inform efforts to disrupt them, including work with allies to interdict illegal shipments
carry out investigations into terrorist activity, from early attempts to radicalise through to detailed attack planning
maintain our ability to provide timely technical assessments of emerging weapons systems and techno…

Information systems, Infrastructure and People

"We will invest further in information systems, infrastructure and people that enable the sharing of intelligence within defence and government and will allies and partners. We will also develop our wider information gathering capabilities such as human and open-source i…

National security tasks and planning guidelines

"National security tasks and planning guidelines. We will identify and monitor national security risks and opportunities. To deliver this we require:
a coordinated approach to early warning and horizon scanning
strategic intelligence on potential threats to national security …
investment in technologies to support the gathering of communications data vital for national security and law enforcement
intelligence assets to support the core military, diplomatic and domestic security and resilience requirements"

Manage Risks

"We will manage … risks by … maintaining our military strategic intelligence capability. We must be able to identify new and emerging military risks as part of our overall approach to intelligence"

Central coordination and strategy

"Central coordination and strategy. Strategic all-source assessment, horizon scanning and early warning are integral parts of the work of several government departments and should feed directly into policy-making, into the annual domestic National Risk Assessment and into the biennial strategic National Security Risk Assessment review process. We need to ensure that the National Security Council has timely, relevant and independent insight to inform its decisions, and that assessment of capabilities are coordinated to support cross-cutting strategic policy work. In order to achieve this priorities will be agreed annually by the National Security Council. These priorities will be used to produce specific requirements for strategic all-source assessment, taking into account assessment capacity and expected volumes of information to be collected. Oversight arrangements will be established to drive performance against these requirements; to deliver improved coordination of prioritisation and allocation of resources across the full range of all-source assessment bodies and functions; and to realise efficiency savings. Cross-departmental cooperation will be further strengthened by closer collaborative working and a common framework for analytical skills and training to promote analytical career development".

Intelligence relationships with overseas partners

"Intelligence relationships with overseas partners, based on shared security interests, will continue to be mutually beneficial. We will:
continue to develop our most significant bilateral intelligence relationship with the US, and the 'Five Eyes' cooperation with the US, Australia, Canada and New Zealand
further expand our relationships with other partners with whom we have shared security interests, through joint operations and intelligence exchange, both in Europe and more widely
share all-source intelligence assessments, terrorism threat assessments and security advice with and through multi-national organisations, including NATO and EU member states
work with newer intelligence partners to help them to develop their capacity and skills, to improve our combined effort."

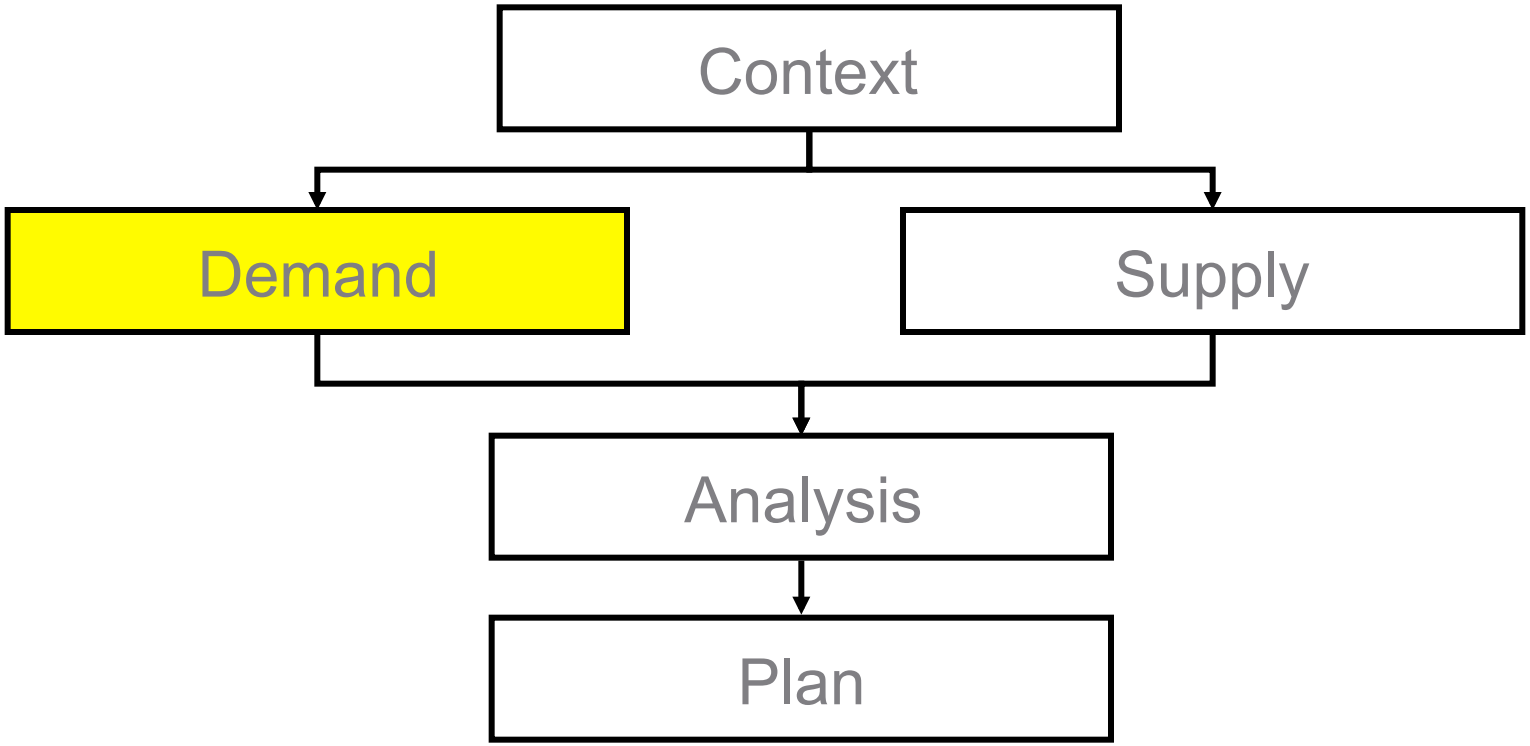
Future character of conflict

The future character of conflict
Globalisation increases the likelihood of conflict involving non-state and failed-state actors. Stateon-state conflict will not disappear, but its character is already changing. Asymmetric tactics such as economic, cyber and proxy actions instead of direct military confrontation will play an increasing part, as both state and non-state adversaries seek an edge over those who overmatch them in conventional military capability. As a result, the differences between state-on-state warfare and irregular conflict are dramatically reducing.
This will add to the pressures on military personnel and the government. It will be more difficult to distinguish our enemies from the civilians, media, non-governmental organisations and allies also present on the battlefield. We must expect intense scrutiny of our operations by a more transparent society, informed by the speed and range of modern global communications.…

The Strategic Defence and Security Review *October 2010, Cm 7948*

NITEWORKS

DPD Capability Planning Process



NITEWORKS

DPD Goals to achieve SIE vision of 2020

Analysis & Assessment - G1
Analysis must at the centre of the Single Intelligence Enterprise providing insight and understanding to the DM, founded on an informed assessment which fulfils their IR. This must be underpinned by effective collaboration within the UK and across coalition environments and requires that processes, tools and outputs are coherent in order to deliver the required quality of assessed intelligence.

D 1 2 5 5 6

Intelligence Coordination - G2
SIE Intelligence Coordination needs to be rationalised and simplified to ensure that Direction, Collection, Analysis and Dissemination of I2 is responsive to the strategic, operational and tactical requirements of Decision Makers. This requires a change in process, governance, culture and development of a common system which enables agile development and prioritisation of IRs and their subsequent tasking in terms of Collection and Analysis. The SIE demands that these processes will need to be matured to ensure coherence with Coalition Partners and key UK institutions in particular the NSC and OGDs.

D 6 9

Collaboration - G3
In order to realise the benefits of burden and information sharing with UK and Coalition Partners the appropriate governance, culture and systems must be developed to provide an environment in which information can be shared.. It is important that these capabilities evolve towards a near real time, single virtual environment to ensure that UK and Coalition partners can react with an appropriate level of agility to fast developing situations given the future character of conflict. This will, where appropriate require the adoption of common standards and processes across the UK and with allies and partners. These new ways of working and information sharing will require cultural changes over time. The SIE must embrace all stakeholders to a greater or lesser extent, irrespective of their location, organisational boundaries and security working levels.

D 6 7 8

Integration of Single Intelligence Sources - G4
The SIE requires to be integrated with the full range of current & future collection capabilities provided organically by the UK and by US, 5 Eyes, NATO, EU and Ad Hoc partners to ensure persistent & the widest possible access to coverage. The SIE must embrace single source initiatives, such as the SSB, DI/GEOINT and ICG visions. This requires the development of rigorous standards which enables the seamless sharing of raw data and analysed product to underpin further analysis, assessment and dissemination.

D 6 6 9 1

Interoperability - G5
The SIE should be interoperable with US and other 5 Eyes architectures and technologies. Arrangements and interfaces need to be in place in order to operate seamlessly with the intelligence systems of NATO nations while also being interoperable to the greatest extent possible with EU nations and other coalition partners.

D 7 8

Information Integration and Sharing - G6
The SIE requires that a coherent approach to IM structures, policies and processes is implemented to enable I2 to be collected, processed and disseminated , in order to enhance understanding. It will be important to balance the imperatives of information sharing with security and information assurance measures. This requires confidence and respect for each others' products and outputs. It requires risk assessment and preparedness. Also, in the context of a networked approach, appropriate policy and technological solutions must be developed which are robust and agile enough to counter the growing cyber threat.

D 6 9

Knowledge Management - G7
The information that fuels the SIE is diverse and has the potential to support government and military functions . Defence should aim to link the resources & information capabilities of many organisations to enable the effective search, retrieval and visualisation of networked I2, within a framework of 'collect once, use often'. A networked approach requires people with the systems, tools, skills, individual and collective behaviours, who can manage, make sense of and exploit rising volumes of information and intelligence. Communities of expertise and knowledge will also need to be more fully exploited. Collection, storage, manipulation and rapid dissemination of information and intelligence will need underpinning by enhanced, distributed data basing and carefully managed bandwidth connectivity.

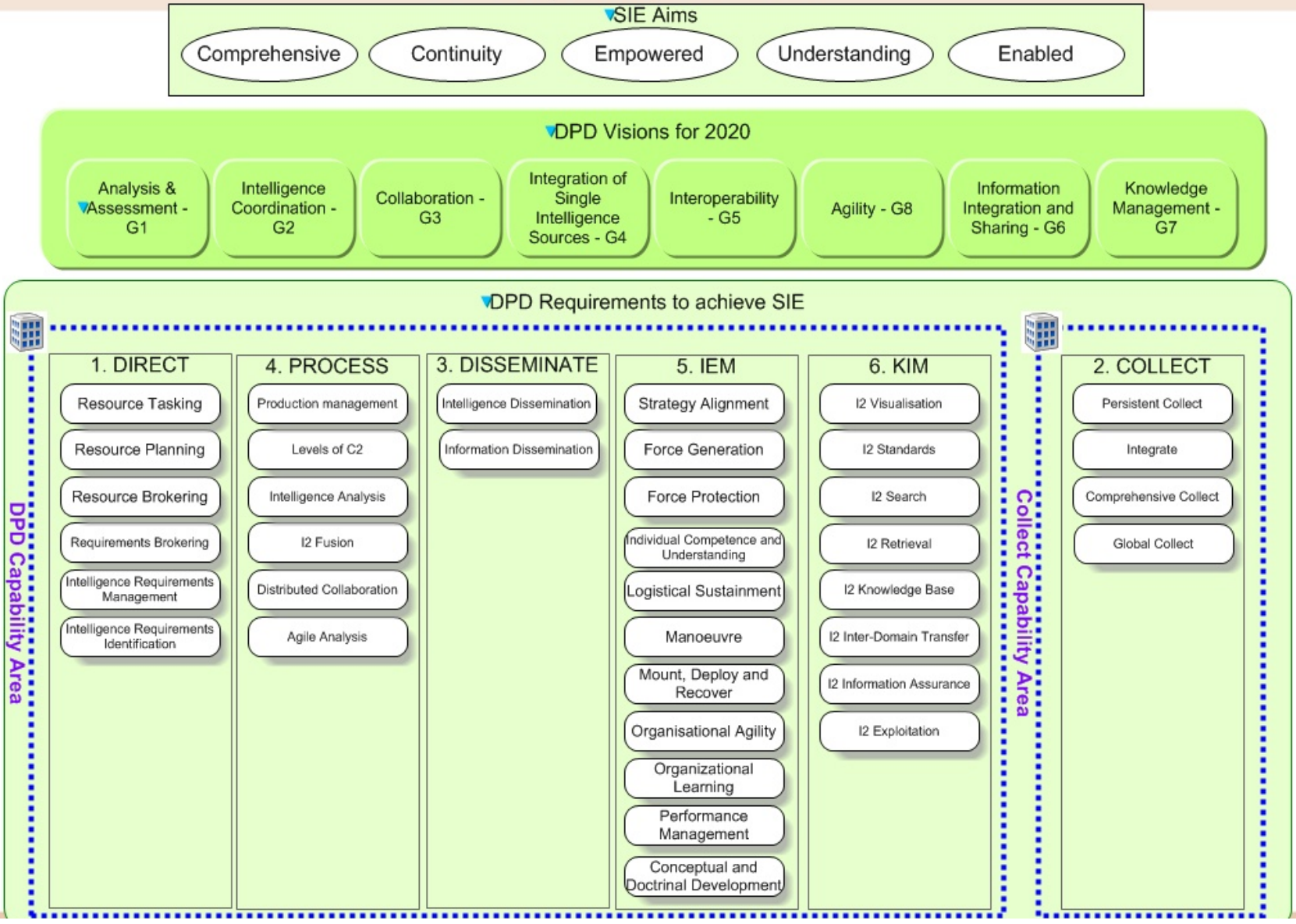
D 9 1

Agility - G8
SIE requires the capacity to adapt and develop appropriate combinations of people, structures, processes and technologies to react to changes in strategic and operational and tactical requirements.

D 4 5 1

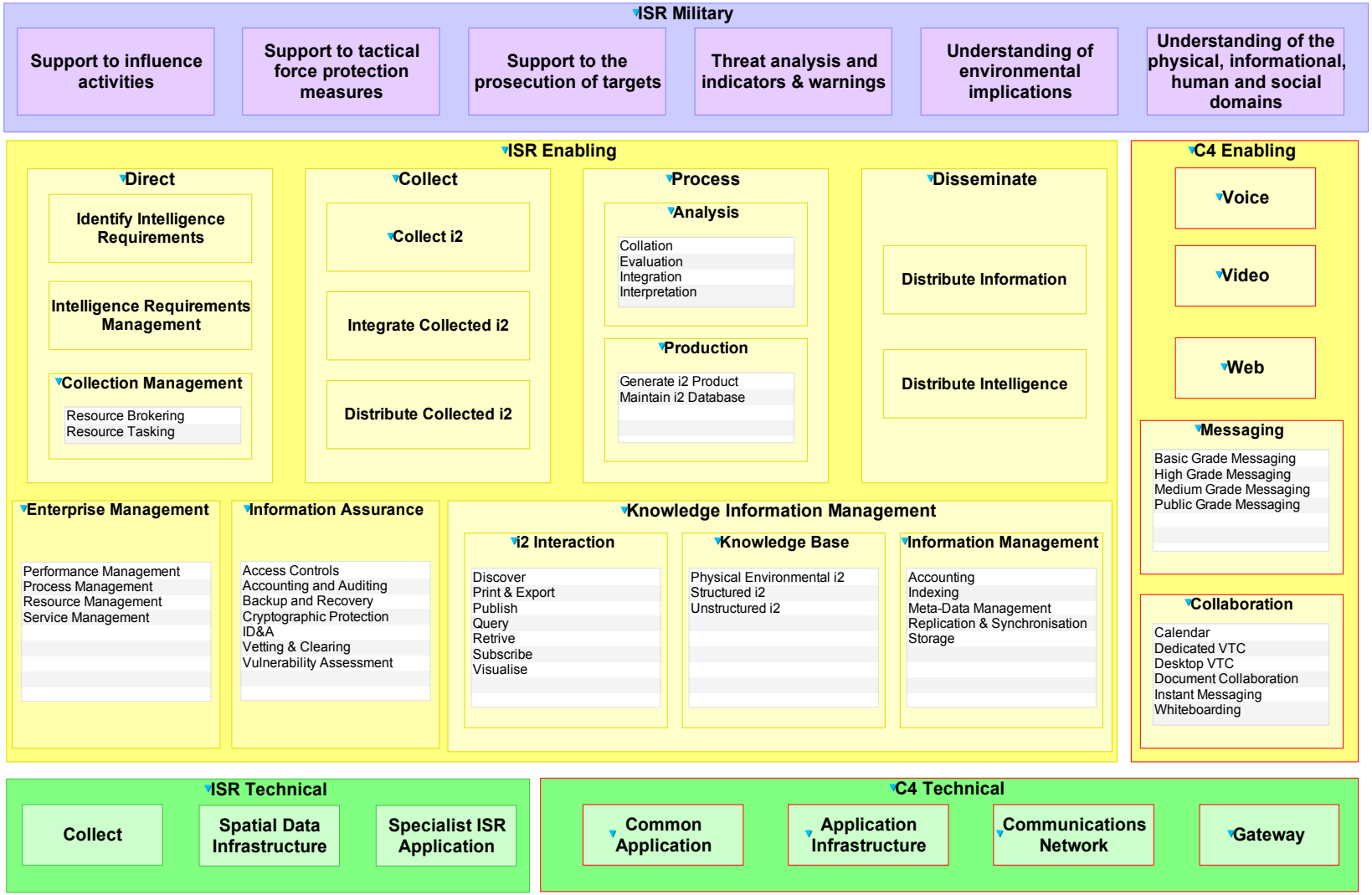
NITEWORKS

DPD Capability Overview



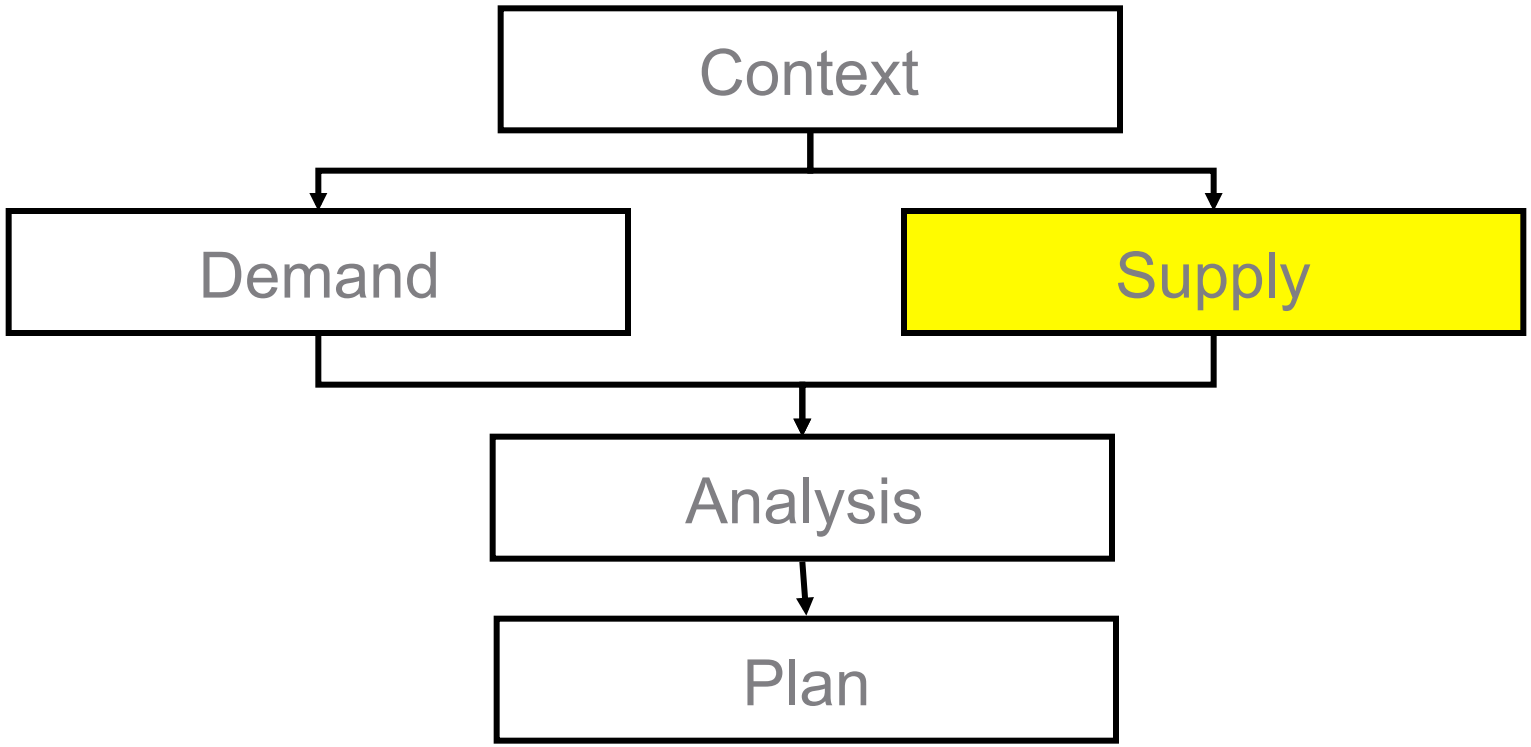
NITEWORKS

ISR Service Taxonomy



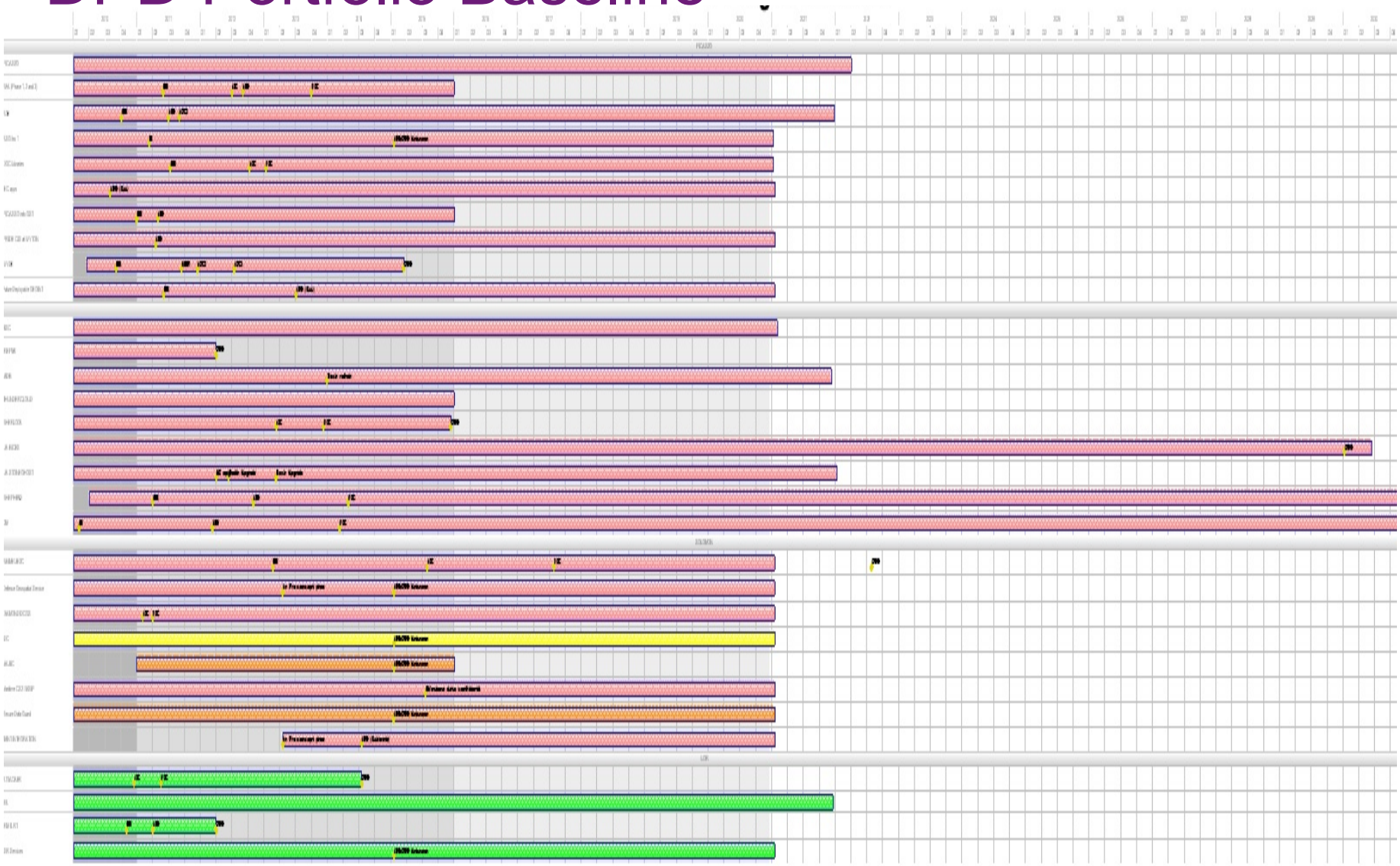
NITEWORKS

DPD Capability Planning Process



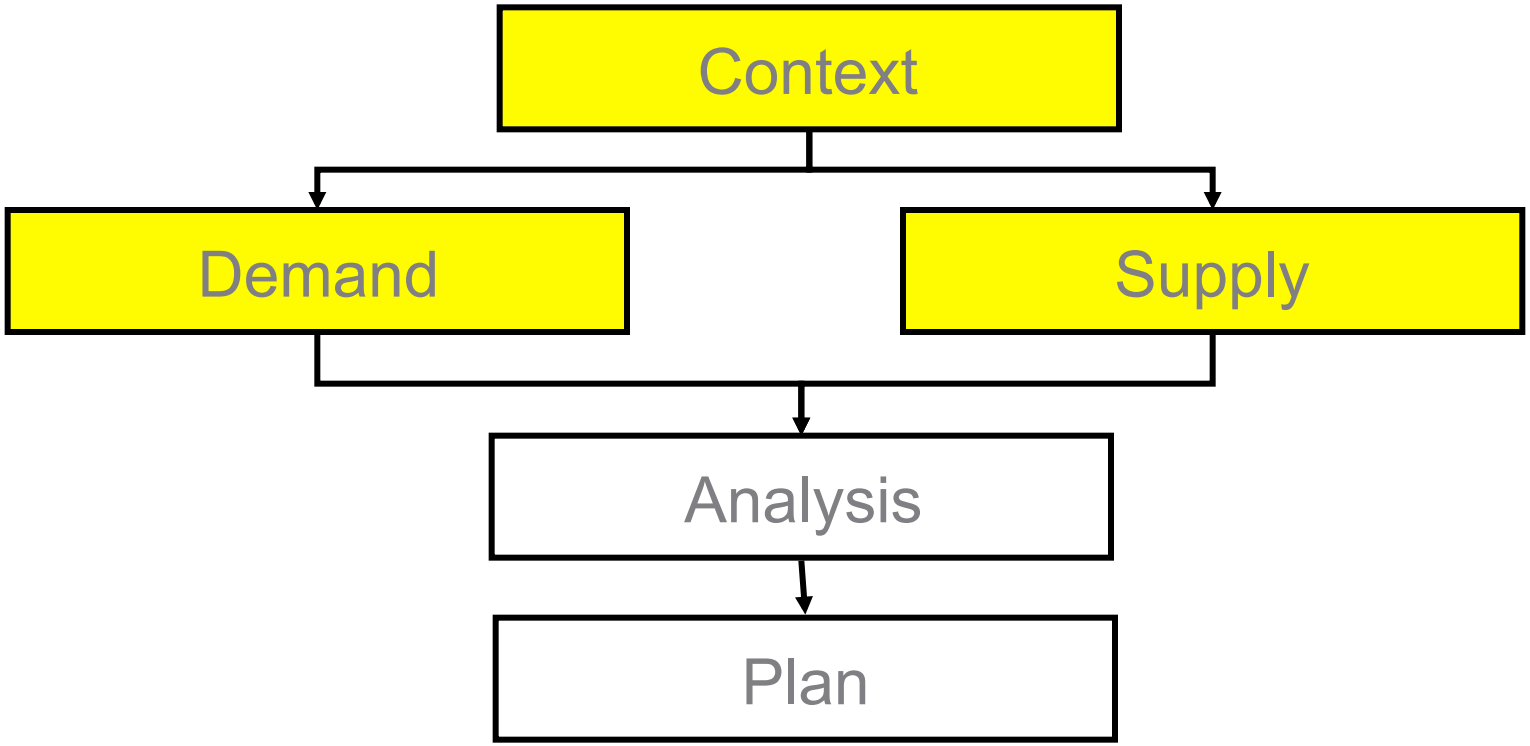
NITEWORKS

DPD Portfolio Baseline



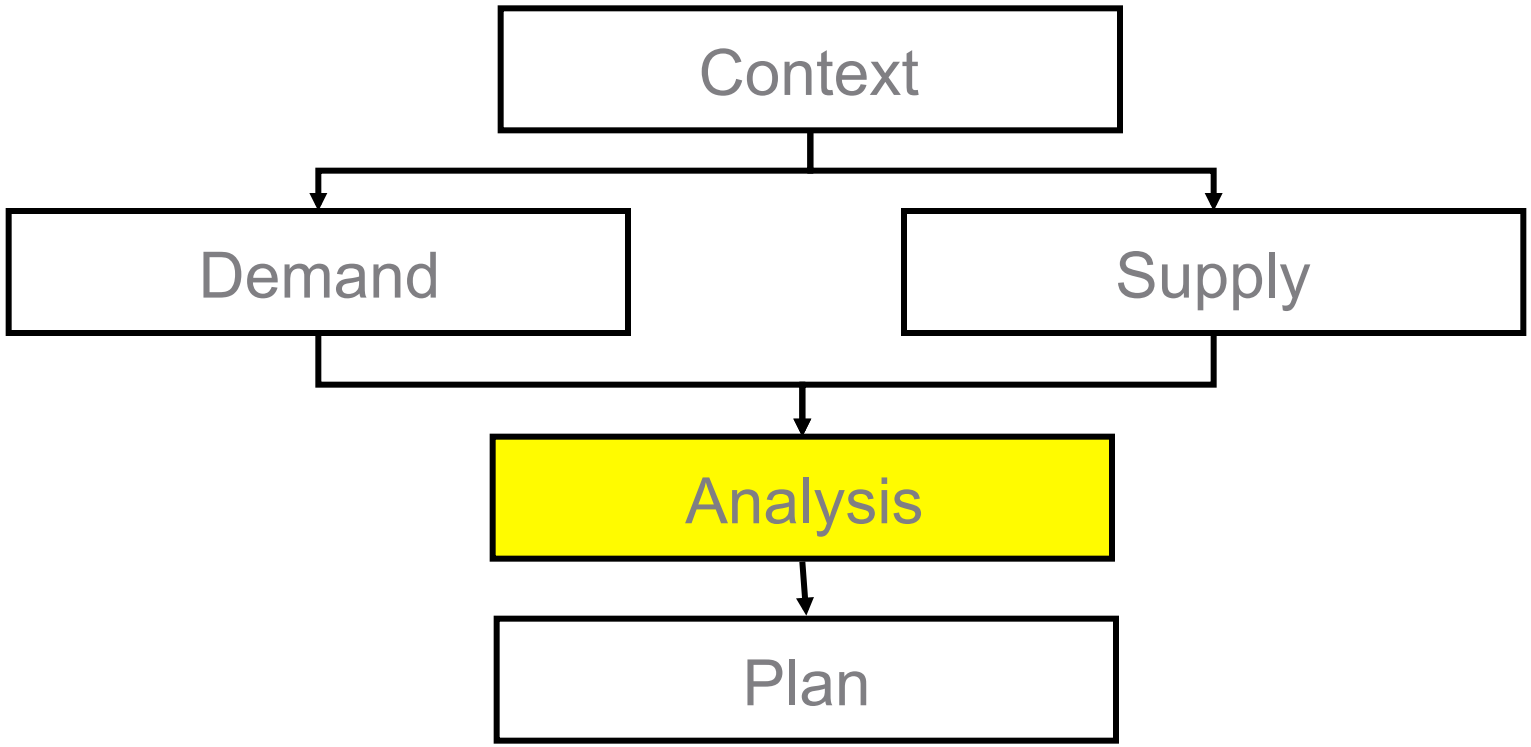
NITEWORKS

Supply Vs Demand View



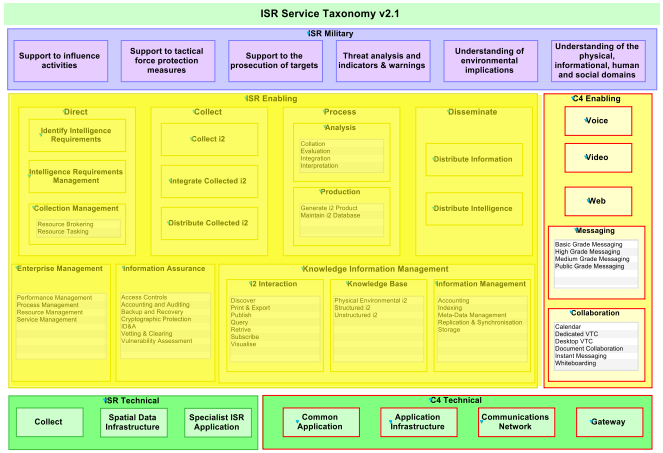
NITEWORKS

DPD Capability Planning Process



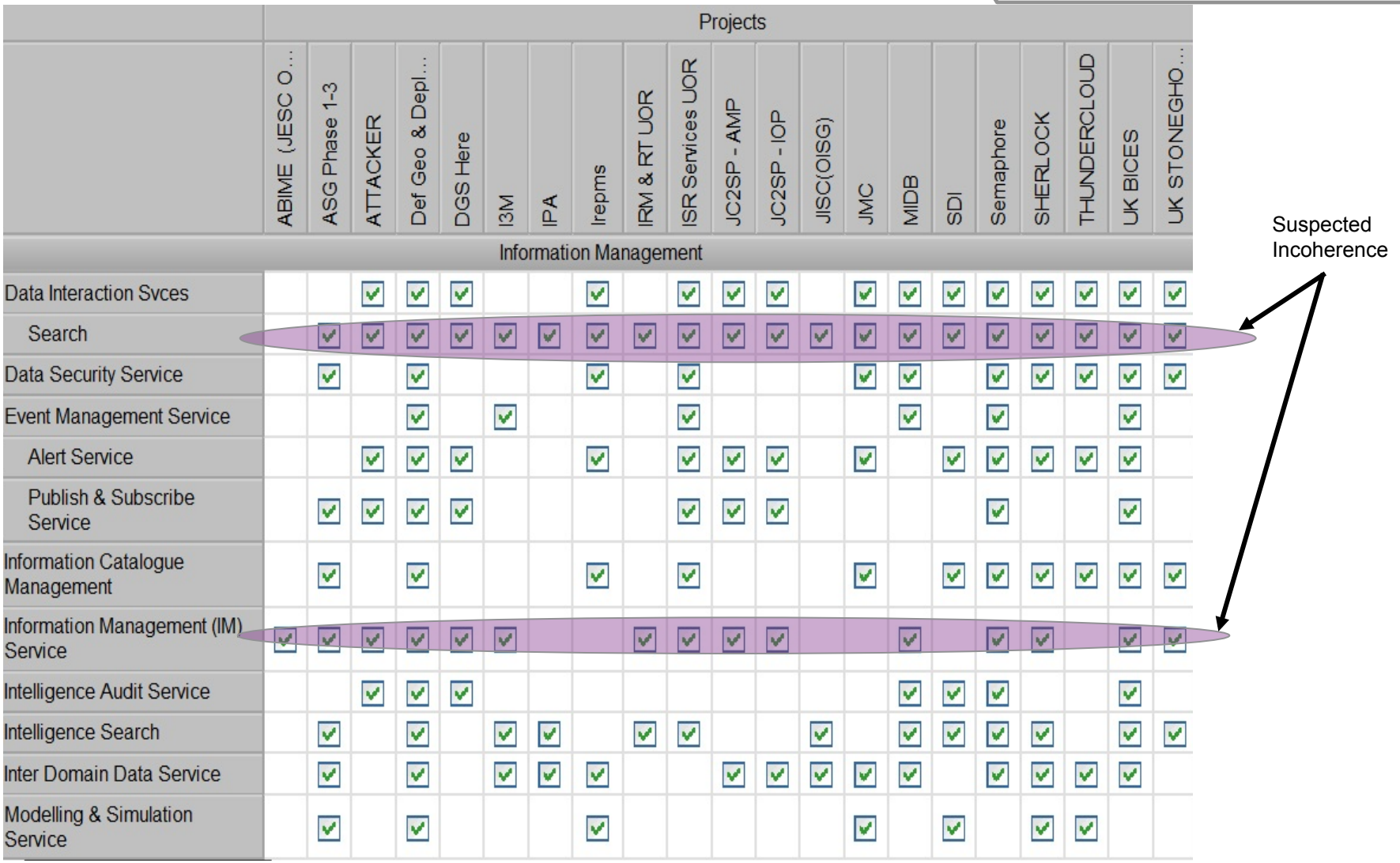
NITEWORKS

	Projects																				
	ABIME (JESC O…	ASG Phase 1-3	ATTACKER	Def Geo & Depl…	DGS Here	I3M	IPA	Irepms	IRM & RT UOR	ISR Services UOR	JC2SP - AMP	JC2SP - IOP	JISC(OISG)	JMC	MIDB	SDI	Semaphore	SHERLOCK	THUNDERCLOUD	UK BICES	UK STONEGHO…
Information Management																					
Data Interaction Svces																					
Search																					
Data Security Service																					
Event Management Service																					
Alert Service																					
Publish & Subscribe Service																					
Information Catalogue Management																					
Information Management (IM) Service																					
Intelligence Audit Service																					
Intelligence Search																					
Inter Domain Data Service																					
Modelling & Simulation Service																					



SO1 Sponsor	Desk Officer	P9 Line	Project in architecture	Sub Projects	Lead User
Steve Massetti	Steve Massetti	P900184900	PICASSO	AFA (Phase 1, 2 and 3)	ICG
				AOE	ICG
				ASG Inc 1	ICG
				OGC Libraries	ICG
				EC apps	ICG
				PICASSO into GST	ICG
				PRIDE CIS at WYTON	ICG
				WYDE	ICG
				Future Deployable GEOINT	ICG
	Ed Ackland	P900369000	JISC		ICG
	Riyaz	P900092900	iREPMS / THUNDERCLOUD		PJHQ
	Riyaz	P900269600	MIDB		Fleet
	Riyaz	P900253800	SHERLOCK		DIS
	Riyaz	P900089900	UK BICES		DIS
	Riyaz	P900270900	UK STONEGHOST		ICSP
Alex Hicks	Alex Hicks	P900529000	SHEPHERD	SHEPHERD Stage 1	Jt Cap
				SHEPHERD Stage 2	Jt Cap
				SHEPHERD Stage 3	Jt Cap
	Monty	P900764000	I3M		ICSP
	Steve Massetti	P900271400	SOLOMON	Defence Geospatial Service	ICG
	Alex Hicks			IDC	ICSP
				IMINT INTEGRATION	ICSP
	Monty			MAJIIC	ICSP
	Ed Ackland			ABIME/JESC	ICG
	Alex Hicks			Secure Data Guard	ICSP
	Ed Ackland			DIAMOND/DOGS	Air
	Mark Minell			Maritime CS2 / MSIP	DIS/Fleet
	Reggie	P980058600	ATTACKER		PJHQ
		P900522200 P980086500	IRM&RT		PJHQ
		P980004000	ISR Services UOR		PJHQ
		P980056200	IPA UOR		PJHQ

NITEWORKS



NITEWORKS

Benefits

- Identification of £83M savings
- Common and improved understanding of the enterprise
- Ability to express the contribution of projects in terms of Capability
- Ability to make decisions holistically across the enterprise
- Capability Gaps easily identified and impact articulated
- Ability to drive out capability overlaps
- Leverage latent capability to best effect
- Ability to clearly articulate Capability Requirements to the Delivery Organisation

NITEWORKS

Lessons

- Cannot manage enterprise based on services alone
  - Understanding of the operational context
  - Appropriate governance needs to be implemented
  - Brownfield constraints is key
- Services need to be the common language by which the ISR Enterprise is described
- Importance of seeking stakeholder buy-in
- Significant commonality between C4 & ISTAR domains
- Very painful process, requiring very strong leadership

NITEWORKS

Wider Adoption

- Information Superiority Reference Architecture (ISRA)
- MOD Transformation
- ISR Services UOR
- Used in-theatre to articulate, issues, constraints and bottlenecks
- Dstl Research Goal/Programme Mapping
- High- Level ISTAR & IO Reference Architecture (HIRA)

NITEWORKS

Questions?

Wg Cdr Alex Hicks – Cap ISTAR DPD Plans

Luke Tucker - Niteworks