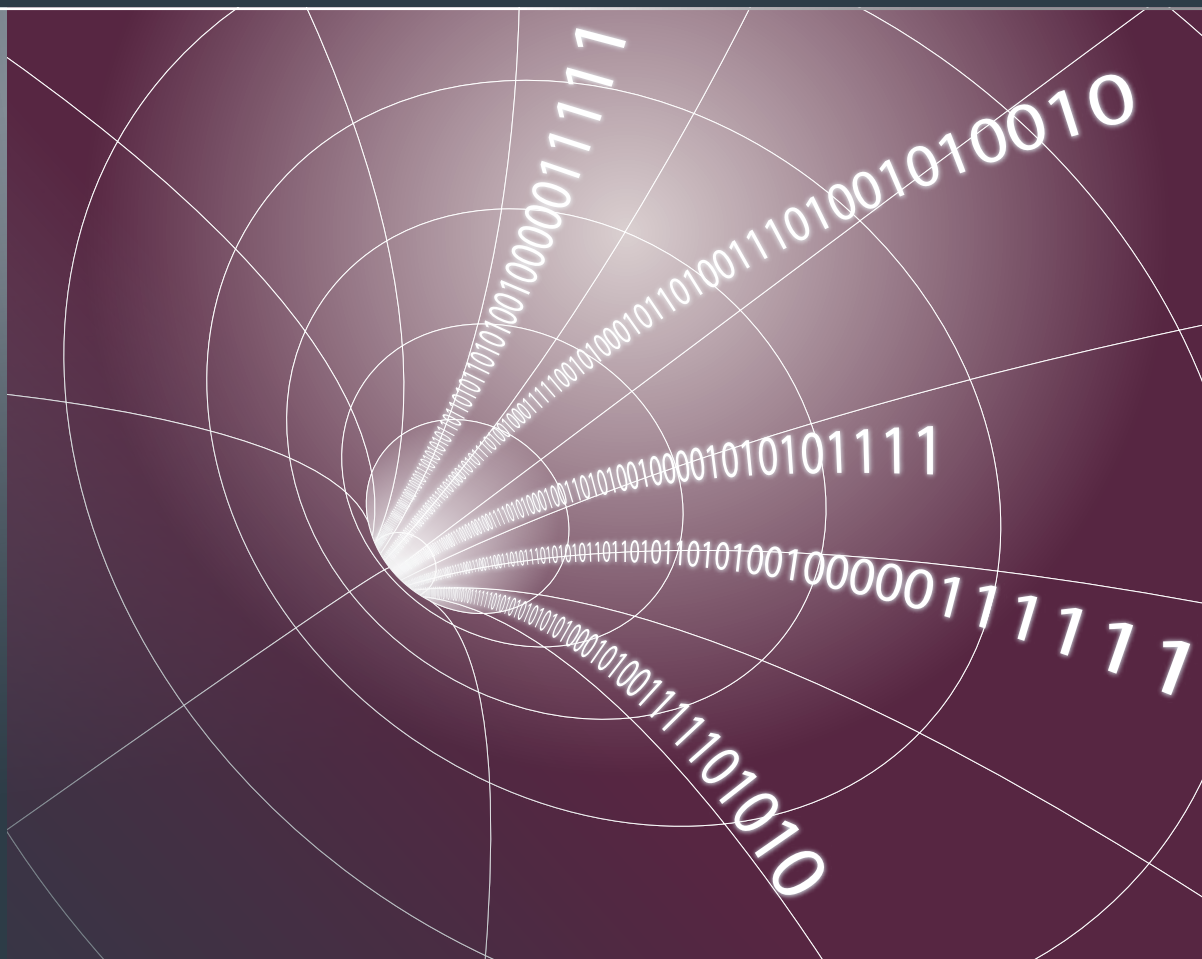
MINISTRY OF DEFENCE

Ministry of Defence

MOD Information Strategy 2011

Better Informed, Better Defence



Defence Information Vision

MINISTRY OF DEFENCE

To achieve the Defence Vision we need to transform the way we exploit the value and power inherent in our information. The Defence Information Vision sets the context for this transformation:

Agile exploitation of our information capabilities to improve effectiveness and efficiency on operations and in support areas through access to, and sharing of timely, accurate and trusted information.

We all have a part to play in realising the Defence Information Vision through our collective pursuit of better decisions through better use of Information, today and in the future.

The four, enduring, key benefits derived from the Defence Information Vision are:

Improved Effectiveness – Our outputs are better when they are enabled by improved information flows;

Agility – Information can be accessed and manipulated whenever and wherever required, subject to affordability and security constraints;

Efficiency – Operational and their supporting processes are more efficient, both because information flows through them better, and Management Information is available to govern them;

Compliance – We comply with our legal and cross-Government obligations, so that we can focus our resources on supporting operations, while maintaining the Departmental reputation.

Foreword by 2nd PUS & VCDS

The Defence Reform Review recognised that Information is a strategic asset and is crucial to success in the business and battle space. It is required for the cost-effective delivery of military capability, and the efficient performance of the MOD's business and support functions. To drive our information transformation this MOD Information Strategy, complemented by the Defence ICT Strategy, aims to provide a corporate framework from which the Chief Information Officer (CIO) sets the information requirements that TLBs, Commands and Process Owners should enforce through their Plans.

This Strategy sets the high-level context for our continuing transformation of the way we use and manage information, a transformation that underpins successful Defence reform and effective and efficient achievement of our objectives. The significant investment in the Defence Information Infrastructure (DII) and other Information Systems has provided the tools for this transformation to provide exploitable and trusted information at the right place and time, to enable the right decision, in order to deliver the right effect and achieve the right outcome.

We commend this MOD Information Strategy to you, and look to all in Defence to play their part in supporting the transformation of our information capability.

John Day

JNR Houghton

Introduction by the Defence Chief Information Officer

John C T Taylor

Transforming the way we manage, share, present and exploit our information is critical to achieving Defence outputs; this transformation is being led by the CIO organisation. The MOD Information Strategy (MODIS) published in 2009 set the agenda and provided a framework to support the reform of Defence information capability, establishing the conditions to achieve the Defence Information Vision. Recognising the many changes in Defence, MODIS has been refreshed to reflect current business and operational priorities.

The information landscape has changed significantly over the last ten years. This has included our engagement in enduring, high-tempo operations in Afghanistan and Iraq; contingent operations such as those in North Africa; an increasing focus on Allied and expeditionary operations; the need to be more joined-up internally and externally with Other Government Departments (OGDs), allies and industry; the development of cyber warfare; and the constant need to deliver resource efficiencies. Part of the changing landscape is a renewed drive by the Government, supported by the MOD, to commoditise ICT services and seek better value for money across the public sector. Owing to the increasing role that ICT plays in delivering Defence and wider-Government outcomes, the ICT elements of MODIS 2009 were developed into a separate Defence ICT Strategy, published in October 2010. By directing our investment in and use of ICT, it complements MODIS 2011 and between them we have a path to delivering the Defence Information Vision.

The Strategic Defence and Security Review (SDSR) recognised that our core information remains haphazardly defined, inconsistently gathered and poorly archived. It is difficult to discover and reuse valuable information to achieve our goals. Apart from the negative impact on operations, we open ourselves to criticism at a time of increasing external scrutiny. We have sufficient information policy; however, there remains too much individual licence and too little compliance. We must do better at adopting Information Management (IM) good practice and exploiting the new tools being rolled-out. DII has begun to address the challenge of joining up Defence internally; however, we face many new challenges and as a result our strategies have evolved to reflect these new realities.

MODIS 2009 articulated the Defence Information Vision. Achievement of the Vision was through the delivery of four Strategic Effects: Strategic Alignment; Information Exploitation; Accessibility & Trust; and Value for Money. MODIS 2011 has expanded these four Effects into seven Information Themes with the aim to provide the right information, to the right people, in the right place, at the right time, to enable the right decision, in order to deliver the right effect and achieve the right outcome - Information Superiority. Key to achieving the Vision is to treat information as a valued asset; only then will we achieve better-informed decision-making. This requires Defence personnel to become appropriately skilled in IM and Information Exploitation (IX). We must also improve the connections between business process, information flows and the supporting information systems. Finally, we must continue to innovate if we are to reform and retain the information advantage we have created.

As CIO, and Information Management Process Owner, I will drive the Information Agenda forward. I look to all stakeholders and information champions in Defence to help deliver the strategic intent of MODIS 2011.

Governance

The Defence Board, through Defence Strategic Direction (DSD), has delegated authority to the Defence CIO to set the conditions to achieve the Defence Information Vision. With delivery responsibility spread across Defence, the CIO relies upon the support and commitment of TLBs, Process Owners, Agencies and Trading Funds. The required direction to the senior information staff within these organisations is provided via the CIO Forum, chaired by the Defence CIO.

The co-ordination of the delivery activities is delegated to the MODIS Executive Group (MODIS EG), which governs the portfolio of information-related programmes captured in the MODIS Strategic Implementation Plan (SIP). The MODIS EG is chaired by the Defence CIO with stakeholders drawn from across Defence. It measures progress towards achieving the Vision and balances conflicting priorities so that the best collective set of benefits are realised for Defence. Taking the priorities set by the DSD, it also considers emerging cross-Government policy and the changing needs of our allies and industry partners. Current priorities are:

- Success in Afghanistan and on other operations;
- Implementing SDSR and delivering Defence Reform;
- Delivering Defence outputs in the most effective, efficient and sustainable way.

Managing Change

In order to promote effective IM/IX across their organisations **TLBs, Trading Funds and Agencies are** required to publish their own IM Directive[1] and ensure that the approach to information is set out, managed and enforced through their Plans. The **CIO will** lead on examining how OGDs, our allies and industry can support this change by promoting more common Ways of Working (WOWs), information sharing and interoperability.

Process Owners (POs) are to more effectively exploit the information that flows through their processes to deliver better VfM for Defence. As part of their role, **POs should define their information requirements, and must**:

- Identify information needed in relation to, or generated by, their process, including Management Information;
- Require that information is managed throughout its lifecycle in accordance with information policies set by the CIO;
- Set any additional policy, standards and rules needed to govern the management of process-specific information, consulting other Process Owners who may be affected;
- Monitor compliance with such policies, standards and rules by Information Asset Owners;
- Ensure that their processes enable best use to be made of the information, including by TLBs and other stakeholders such as industry and Other Government Departments;
- In their annual reports to the Defence Audit Committee, provide assurance that there is an effective compliance regime and identify any high-level risks relating to the information;
- Provide the necessary functional expertise and guidance to assist the CIO in formulating information policies and procedures.

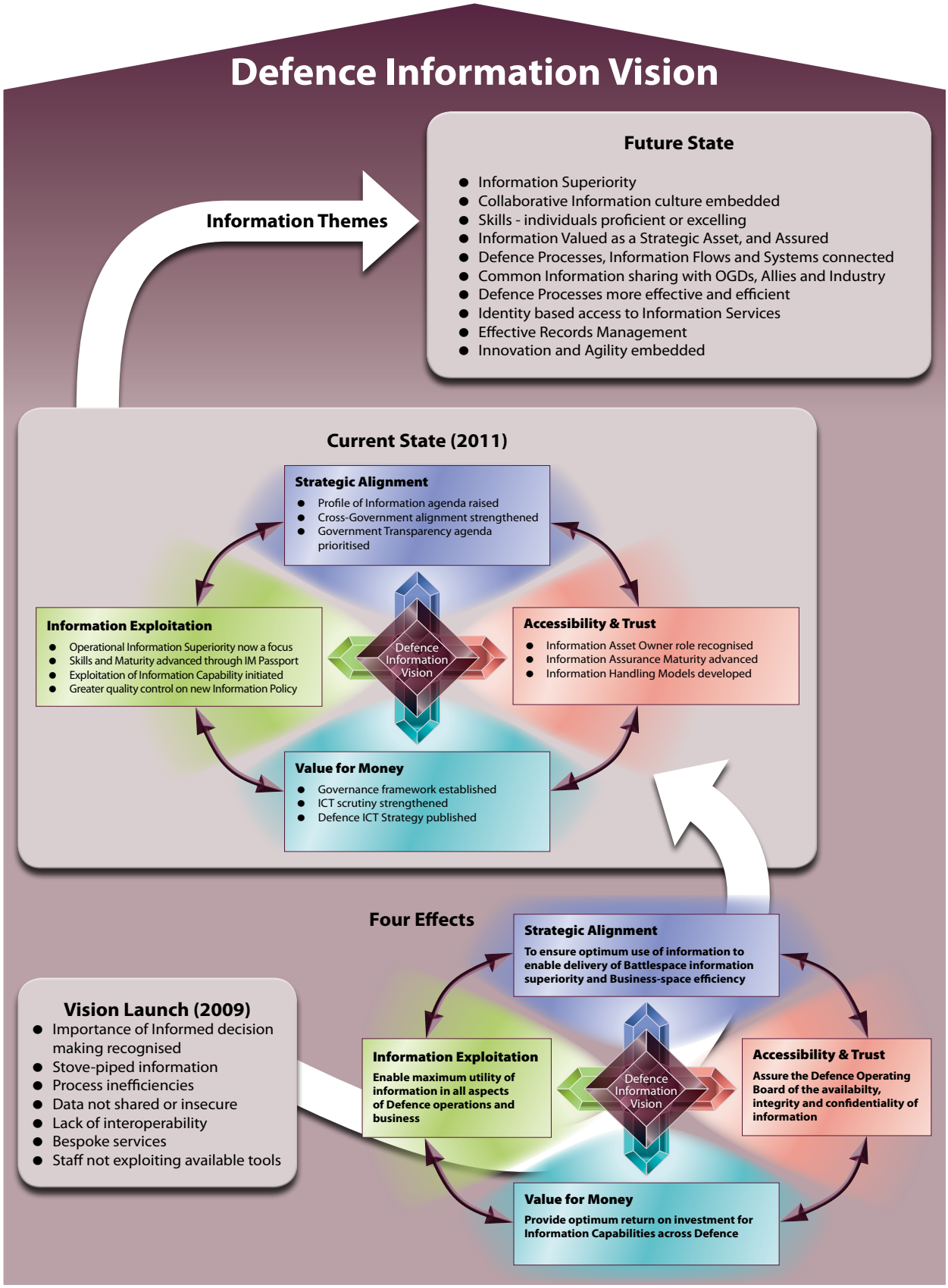
1 IM Directives will be issued by CIOs/SIOs to direct how IM/IX will be delivered in their respective organisations in support of MODIS.

Delivering Change

In the decade following the publication of the 2000 Defence Information Strategy there has been an increasing recognition of the importance of information, particularly in support of informed decision-making. Recognising this, MODIS 2009 articulated for the first time a Defence Information Vision and a roadmap for Defence organised around four Effects: Strategic Alignment, Information Exploitation, Accessibility and Trust and Value for Money. These Effects have proved to be a relevant and useful tool for directing information activities and investment. An assessment of the progress made so far is shown in Figure 1.

However, the Defence landscape has changed and the CIO took a decision to rationalise the existing information related strategies and sub-strategies into MODIS 2011 and the Defence ICT Strategy. The seven Information Themes were developed from the four Effects and shaped by the information related sub-strategies; the intent being to re-focus ongoing or planned activities in support of the information agenda to ensure we remain on track to deliver the Defence Information Vision.

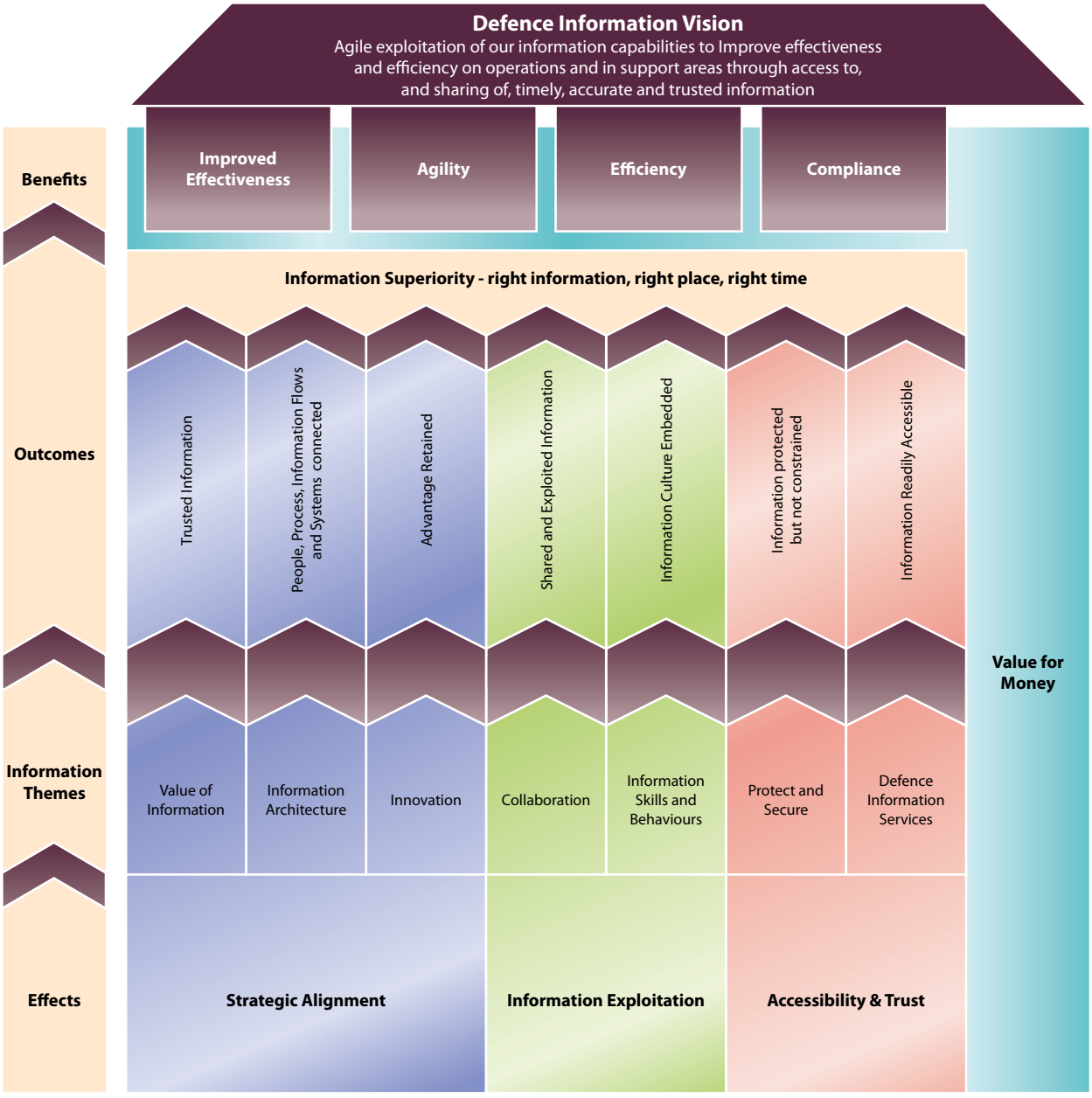
Figure 1 – Defence Information Transformation



To direct and co-ordinate the actions required by MODIS 2011 it is important to understand how Defence will achieve the Defence Information Vision. Figure 2 represents the model used by the MODIS EG to understand how the Information Themes will contribute to the delivery of the desired outcomes and describes what Defence will look like and how it will operate to exploit information in the future.

Building upon the roadmap, defined by the four Effects in MODIS 2009, we will update the MODIS SIP to reflect those activities required by the Information Themes. The SIP also contains the metrics and key performance questions used to measure progress. This, in turn, permits the MODIS EG to co-ordinate the tasks and shape the prioritisation and direction of information change activities.

Figure 2 – Information Benefits Model



Information Themes and Outcomes

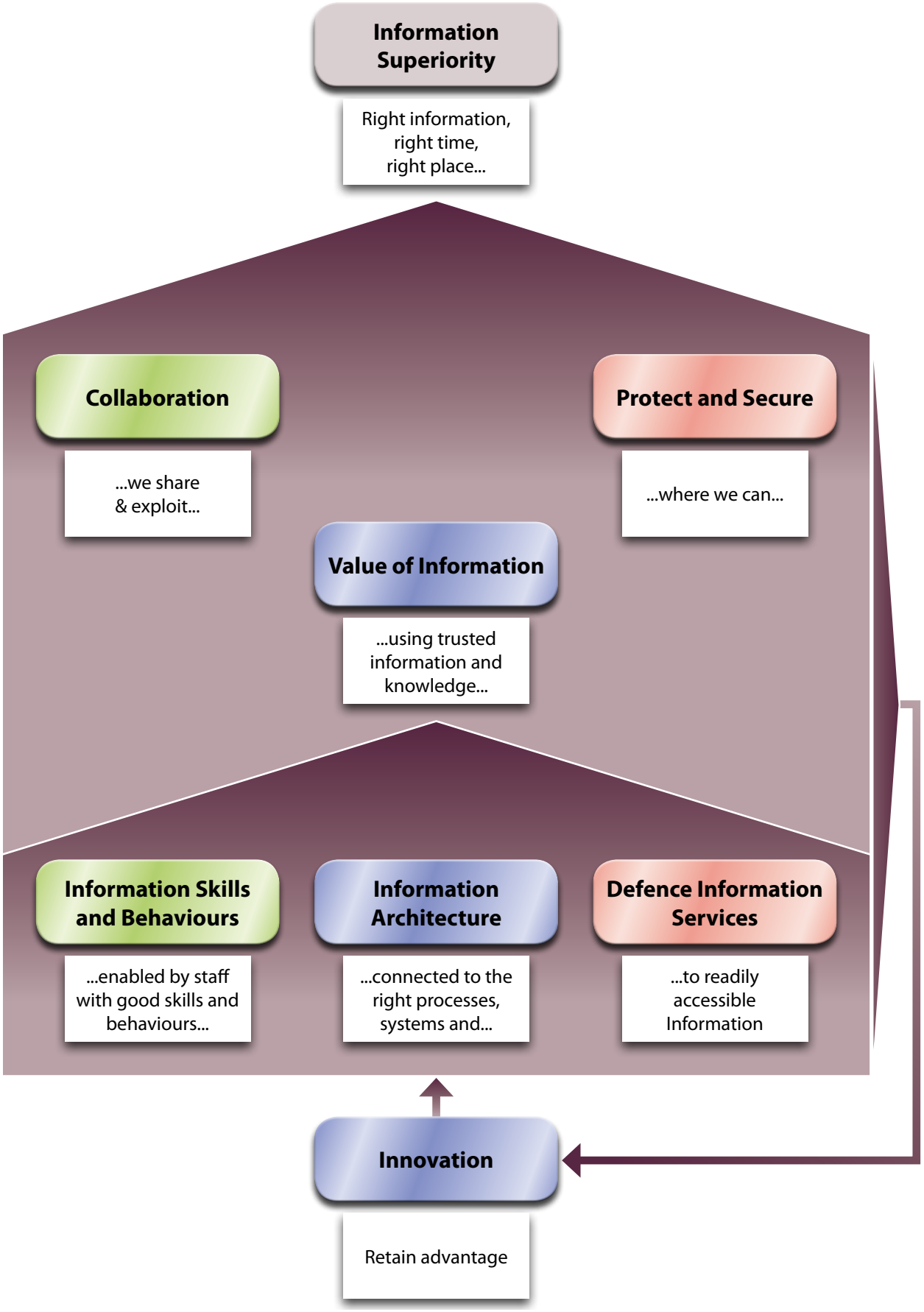
The right information provided in a timely manner enables the right decisions to be made, which is critical to success. The drive to achieve **Information Superiority** and enable better decisions demands that we all improve our information management and exploitation skills.

Collaboration is key to enabling Information Superiority and the ability to make better decisions. By collaborating across organisational and national boundaries we will achieve improved shared awareness, which in turn will contribute to more effective and agile outcomes. Collaboration means creating, sharing and exploiting information with our allies, industry partners and OGDs, which is appropriately **protected and secured**. This can only happen if our information is assured, including the application of the right cyber practices and skills. Only then will users have the confidence that the information can be trusted, while being safe from malicious acts or misuse.

Defence must change behaviours, to recognise the **value of information**, and treat it as an asset. However, not all information is valuable. Information must be regarded as a collective not a personal asset, as its value is often increased through sharing. Equally, sensitive information must be appropriately protected in recognition of its particular value. The value of information is also in part derived from the quality of the available data. Therefore, data must also be recognised and treated as a valuable asset, to be managed in a disciplined way. Timely, relevant, consistent and accurate data are the fundamental attributes of quality information in support of decision-making processes.

Information is only valuable if it is available to the right person, who has the necessary **skills and behaviours** to manage and exploit it. To support better decision-making, information needs to be assessed, analysed, combined with other information and knowledge, and presented in a meaningful way to the decision-maker. In order to achieve the right information flows an **information architecture** approach will be used to identify what **information services** are required. The architecture will describe how information flows along and between processes, where it is used and how it is transformed; this will help determine what information systems we need and how they should be connected to deliver better outcomes.

In order for Defence to retain and improve its information advantage, particularly in austere times, we must be **innovative** in how we use and develop our information systems and processes. Innovation is about using and exploiting existing and new capabilities to deliver more from less. Without effective innovation our capabilities will be reduced and Defence will not realise its goal of better, timelier decisions.


Information Superiority
Right information, right time, right place...
Collaboration
...we share & exploit...
Protect and Secure
...where we can...
Value of Information
...using trusted information and knowledge...
Information Skills and Behaviours
...enabled by staff with good skills and behaviours...
Information Architecture
...connected to the right processes, systems and...
Defence Information Services
...to readily accessible Information
Innovation
Retain advantage

Information Superiority

Critical to effective decision making, whether on operations or in the office environment, is the ability to access the right information at the right time.

Success in any organisation relies upon decision-makers at all levels taking action to achieve their superiors' intent. Deciding exactly what action to take inevitably involves an assessment of the risks and benefits inherent in the available courses of action and this, in turn, requires both access to information and the ability to exploit it. In this sense there is very little difference between the business space and battlespace; we all need to be able to make timely, informed decisions, maximising the effectiveness of evidence-based policy decisions and the delegated ways of working typified by Mission Command. Information Superiority is a term of relative advantage but it is built upon the same foundation of IM and IX in both Business Space and Battlespace – both ultimately support operations.

Communications and Information Systems Support to Operations in the Middle East

Better IM/IX is one of the fundamental building blocks to achieving Information Superiority. IM/IX has already proved valuable during support to current operations:

"Support to operations in the Middle East is subject to the rapid turnover of personnel. Continuity of information is critical to ensuring that this turnover of personnel does not adversely affect operations. By ensuring information is stored and easy to find, new personnel are able to become effective more quickly, and continuity for longer term projects is maintained."

Commander JFCIS (ME) Mar 2010 – Sep 2010

Experience has shown that information requires the same degree of attention as other, more tangible resources; people, money, equipment and real estate. Moreover, this imperative is equally relevant in all support areas across Defence. Information must be valued and viewed as a vital asset in its own right; only then will Information Superiority be truly realised. From a commander's perspective, Information Superiority reduces operational risk by enabling more timely and informed decisions to be made than adversaries can achieve (i.e. decision superiority).

Importance of IX to operations

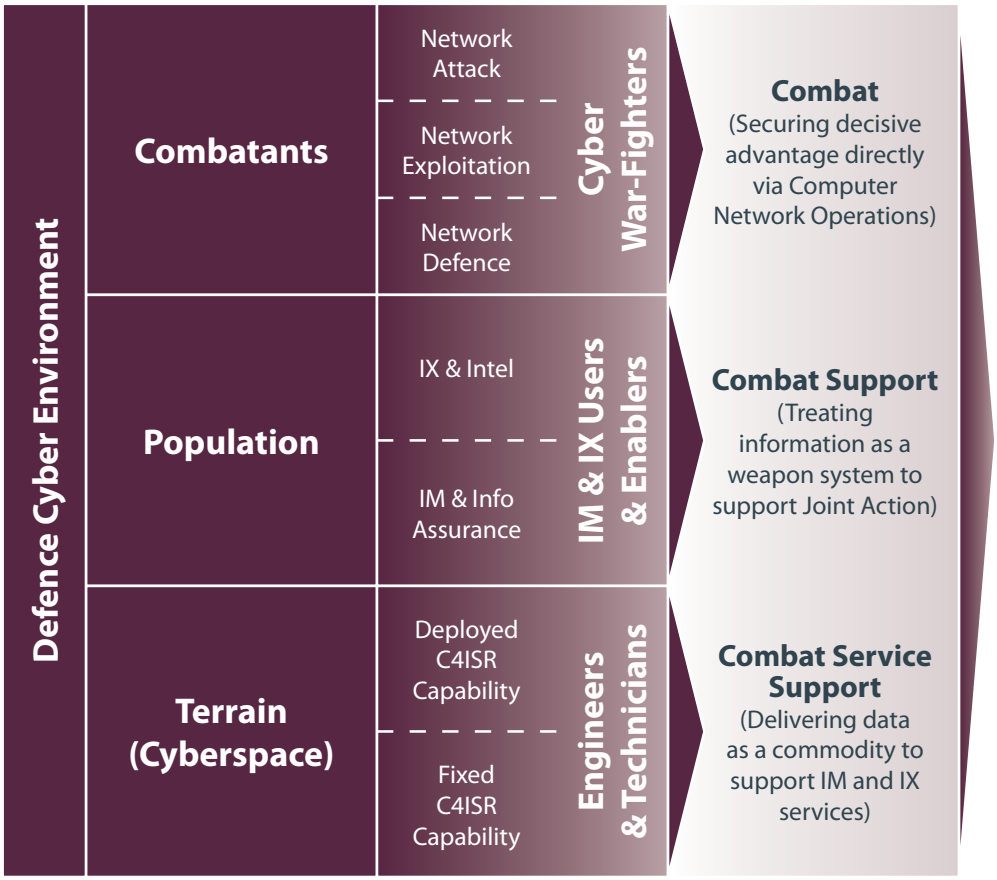
"Limited capability to deliver Intelligence Surveillance and Reconnaissance, and exploit information is a significant risk to the successful conduct of operations"

CJO – Mar 2011

Everyone, from the Chief of Defence Staff down will, by their action, contribute to the achievement of Information Superiority. Understanding

where you fit into the Defence Cyber Environment is key to our Commanders achieving Information Superiority:

Where do I fit in?



Information Superiority is a state of relative advantage achieved through:

Information Superiority
'Possessing a greater degree of information about the battlespace, being able to exploit that information more rapidly and preventing the adversary from obtaining or exploiting information which would give combat advantage.'
JDP 0.01.01

Looking to the future, success in Afghanistan will, in the short to medium term, remain critically dependent upon both situational awareness and intelligence. As a consequence, considerable effort is still being invested to continue developing IM, IX and the underpinning Command Control and Information Infrastructure (CCII) capability on Op HERRICK. To achieve this, **Defence is** using the Operational Information Superiority Programme Board to veer and haul the Equipment Programme, using a range of Urgent Operational Requirement (UOR), Equipment Programme Plan and other interventions to maintain Information Superiority on current operations. As events in the Middle East and North Africa have also recently demonstrated, we clearly need agility and responsiveness in our Information Superiority capabilities so that we can react to short-notice operations which run concurrent with our commitment to Afghanistan.

For operations beyond Afghanistan, the Middle East and North Africa, Defence's Information Superiority capabilities post-SDSR will be re-baselined to ensure that we have a fully coherent and affordable plan,

across all Lines of Development. This revision to the capability baseline by **Director Information Superiority is intended** to see us through the conclusion of current operations, the reconstitution of contingent operations capability for Interim Force 2015 and then on towards Future Force 2020 – all against the backdrop of intense resource pressures and competing joint priorities.

Finally, MOD's approach to Information Superiority is also maturing. When Network Enabled Capability (NEC) was first conceived, its implementation required a revolutionary approach. Since that time, Through Life Capability Management (TLCM) and NEC governance structures have matured to the point where the concept could now be delivered as evolutionary change by Defence. As a consequence, **Defence intends** to update and simplify NEC (including its Handbook, JSP 777) and embed it as 'daily business' within Defence, alongside SDSR and Defence Reform Review changes. This intent was encapsulated in the NEC Executive Group's deliberations in Nov 2010 and VCDS's Joint Command Group for Information Superiority in Jan 2011.

Information Superiority enables decision-makers at all levels in all environments to make timely and informed decisions. It therefore contributes to the Defence Information Vision by delivering benefits in agility, effectiveness and efficiency.

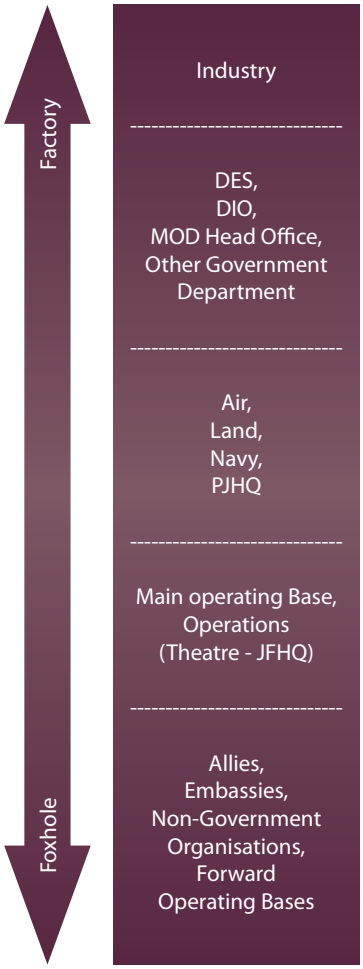
Collaboration

Collaboration is working together. It connects people, information, data and processes across organisational and national boundaries. The ultimate aim is increased end-to-end operational effectiveness - i.e. from "factory to foxhole" – so that information can be exploited to its full extent.

Collaboration is a human process; people working together to achieve common goals. In Defence, the scope of collaboration extends from factory (industry partners) to foxhole (Deployed environment including our allies and OGDs), and thus information, processes and data must flow across these organisational, multinational and industry boundaries. Making these connections presents real challenges and needs common standards and practices to be effective and coherent.

Effective collaboration addresses a number of drivers and challenges that face Defence, including:

- Operational effectiveness. Operations involve complex information environments requiring collaboration between Fixed and Deployed domains, with allies, industry partners , OGDs and NGOs;
- Defence reform. **Defence staff will** have to change the way they work to focus priorities and deliver more with fewer resources. Inherently Defence will need to improve and streamline processes to allow staff to focus on important tasks;
- Supply chain agility. The nature of working with industry, and the requirement for more rapid product development times, requires Government and industry to work together in a more agile and cost effective manner;
- Compliance to regulatory and cross-Government requirements. Defence must embrace cross-Government initiatives (e.g. Sustainability, the Transparency agenda, etc).



The benefit of MOD/industry supply chain integration

The RB199 Operational Contract for Engine Transformation (ROCET) is an exemplar of the savings that can be achieved. Rolls-Royce is contracted for Tornado engine availability. By providing Rolls-Royce with direct electronic access to engine usage data, such as flying hours, Defence has enabled maintenance of engines to be optimised with significant saving in the number of spare engines in the supply pipeline and improved availability of aircraft. This effective bi-lateral exchange of information is a key enabler for Contractor Logistics Support style of operation.

The CIO is setting out policy and direction for Collaborative Working within Defence, and providing the appropriate tools to support this where it can. **The CIO is** working with TLBs and Process Owners to capture best practice and promote re-use to drive consistent WoW and exploitation across Defence. Coherence between Fixed and Deployed environments remains a priority, as does the need for mission-configurable ICT.

The CIO will lead on including collaboration best practices in the training

courses targeted at both information specialists and information users. Furthermore, **Defence needs** to ensure that identity based access to information is enabled so that the creation of a trusted collaboration environment is supported.

Collaborative Working Environments (CWEs) have already been established. **Defence needs** to continue to work with industry to define common standards, practices and mechanisms to allow collaboration across organisational boundaries. This integrated collaboration needs to be driven across the Fixed and Deployed environments.

Collaboration within Defence

Defence has made considerable progress in the development and roll-out of the DII ALAMEIN Microsoft Office SharePoint Server (MOSS) 2007 capabilities and an adoption toolkit that will provide a Defence-wide platform for collaboration over the next 18-24 months. Work is ongoing to accelerate the realisation of benefits from ALAMEIN through developing a toolkit to help identify opportunities to enable information flows (processes) using the delivered capabilities.

As collaboration opportunities evolve, we need to drive coherence in practices and standards across platforms to provide the same quick and easy collaboration that social networks and social media services offer on the web. However **Defence needs** to combine these qualities with the requisite high levels of security, availability and quality of service.

Process Owners and TLBs need to embrace new collaboration tools and techniques to improve and simplify their processes, where possible. This in turn will lead to better-informed and more agile decision-making.

Protect and Secure

Information is a critical asset and needs to be assured, protected and shared securely; the aim being to protect the information without inhibiting its use.

As stated in the Information Superiority and Collaboration themes there is a need to share information with an increasingly diverse audience. As well as the need to share, Defence needs to understand its critical information assets and ensure they are suitably protected. Achieving the balance between sharing and protecting will be dependent on many factors, but it must be an informed decision based on managing risk.

Our information needs to be protected from a diverse number of threats including: accidental data loss; deliberate leaking of data and the challenging range of cyber threats intent on accessing or disrupting our information. We need to ensure that digital information remains accessible and useable over time. In a time when we are increasingly reliant on Information Services, our behaviours and defences need to be dynamic and agile to mitigate the ever challenging and diverse threats the UK faces.

Defence is committed to building and maintaining a robust Information Assurance (IA) regime that allows information risks to be understood and managed across the Department; driving through behavioural change. The Defence Board has directed that CESG Information Assurance Maturity Model (IAMM) Level 3 will be achieved by April 2012 and a programme is in place to deliver this.

This cyber threat comes not only from traditional operational adversaries and state actors, including foreign intelligence services, but also the less traditional non-state actors including computer hackers and criminal elements. These threats not only affect MOD owned systems but those operated by OGDs, industry and allies.

In line with Defence Strategic Direction, a Defence Cyber Operations Group (DCOG) is being established. **The DCOG will** provide Defence with a significantly more focused approach to cyber ensuring that it is at the heart of Defence operations. **The CIO will support** the DCOG in developing skills framework, training and evaluation.

In order to protect our information, **Process Owners, Information Assets Owners and individuals need to** be aware of the risks and to understand their responsibilities when handling information. This needs to be in concert with continued capability development and investment in specialist skills, whilst maintaining close partnerships with OGDs, allies, industry and academia. This will allow the Department to manage its information risk effectively.

By ensuring our information remains assured, protected and secure **Defence will** benefit from relevant, high quality information, available for use by those who need it, when required. Our personnel and processes can exploit information fully and with confidence. **Defence will** have established a trusted environment within which information can reliably be handled in the Department and with our allies, across Government and throughout our supply chain.

This trusted environment, supported by an effective compliance regime, will reduce Departmental risk; we will continue to comply with, and contribute to, the cross-Government IA agenda. The agility, efficiency and effectiveness of our working practices will be enhanced, including those practices that involve our national and international partners. Individual productivity, enhanced through Identity and Access Management (IdAM) services, will be improved as assured information allows decisions to be made in a trusting environment. We will be able to collaborate with ease and confidence.

To enable assured information sharing the use of IdAM services will enable trusted access to information within Defence, the rest of Government and external partners.

The CIO will (via IdAM) promote the use of digital identities and information labels to connect individuals with the information they need and control access to information when necessary. Labelling and attribute based access controls enable the information to be stored once, driving towards the ideal of a single version of the truth.

Collaboration with Industry

The Transglobal Secure Collaboration Program (TSCP) is developing standards for collaboration and secure information sharing with industry. Using these standards, MOD is working with industry (through UK Council for Electronic Business) to pilot an approach to enable Small and Medium Enterprises (SMEs) to access an RLI-hosted CWE.

In conjunction with our industry Partners, **Defence needs to** develop robust capabilities, which are designed from the outset to cope with the cyber threat, and ensure that its information is protected and secured. The effectiveness of these capabilities will rely on Defence developing its broader and specialist information related skills and undergoing the associated behavioural and cultural change.

Value of Information

Defence needs authoritative data and quality information; information must be viewed as a valuable asset.

Agile exploitation of information capabilities relies upon the delivery of quality data that is fit for purpose. By exploiting information in context the Defence community is able to improve its knowledge and situational awareness. Timely, relevant, consistent and accurate data are the fundamental attributes of trusted, quality information in support of decision-making processes.

Information Rights

Each year the department receives some three thousand Requests for Information (RFI) under the Freedom of Information Act, and some 25,000 Subject Access Requests (SAR) in accordance with the Data Protection Act. Moreover, the number of requests covered by the Environmental Information Regulations is increasing steadily. It is most important that the Department is seen to be answering all these requests, swiftly and accurately. The priority challenge for Information Rights is to maintain or improve standards, through good guidance and training, while dealing with the resource challenges and organisational reforms of transforming Defence.

Decision-making, our Information Rights obligations, and public and parliamentary accountability rely upon the quality of this data and information. By ensuring its quality our decision-making will be better informed and our trust in the information underpinning those decisions improved.

Data needs to be available to all personnel and systems with a requirement to use it, from authorities who understand what it should contain and how it should be used. Production of consistent and coherent information requires standardised data supported by clear definitions.

Data should have clear ownership, documented responsibilities, and be maintained and updated to keep its timeliness. This will allow data to be authoritative and make it easier to use with confidence.

In line with Government policy, **Defence has**, and continues to appoint Information Asset Owners (IAOs), to take responsibility for the information within their areas of responsibility. **The CIO is** contributing by establishing and maintaining simple and easily accessed information policy, that enables decision makers to achieve Defence goals and supports effective scrutiny of information related investment.

Assisting Counter IED Operations

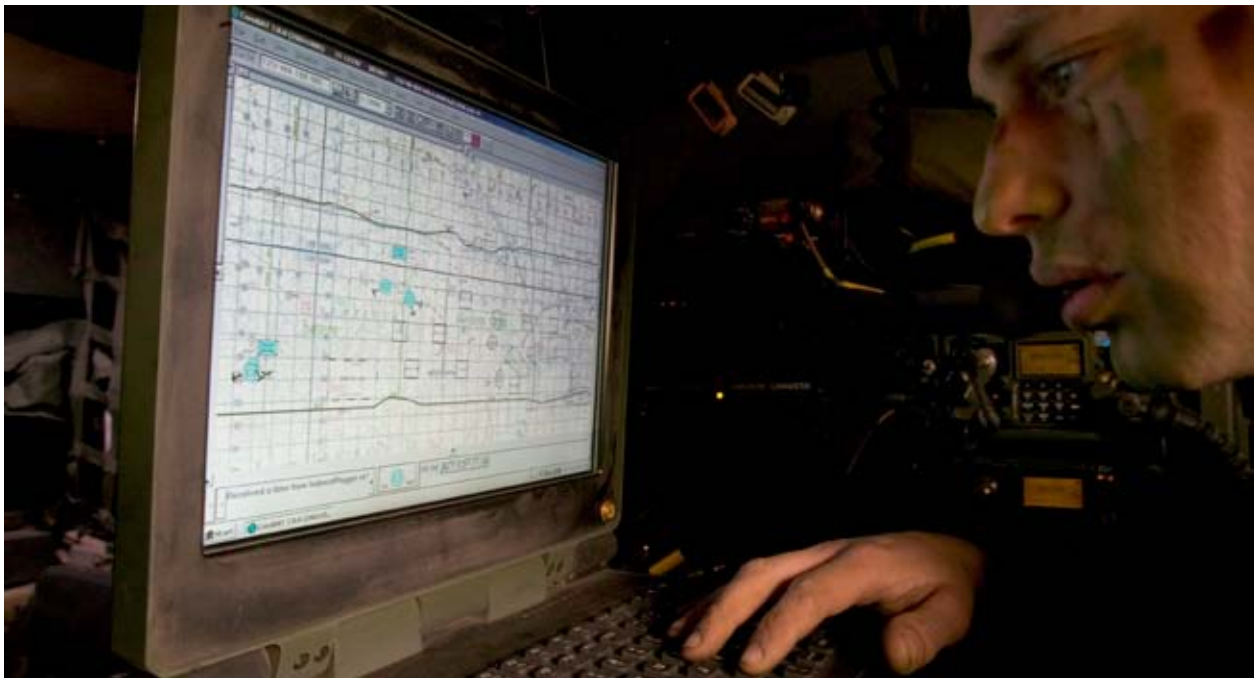
By adopting a common C-IED vocabulary, the MOD and US DOD have enabled improved analysis of IED components, which can in turn assist in the disruption of insurgent networks and bomb making facilities.

Under CIO leadership **TLBs and Process Owners will** use Communities of Interest (COIs) to agree standards, and create authoritative sources of quality data. **POs will** identify and empower data owners who will work with COIs to make authoritative data available to Defence. This will provide users with the opportunity to use authoritative data from known sources that is trustworthy and of a suitable quality for their needs. COIs will provide advice to organisations in need of authoritative data and share best practice to enable these organisations to understand how the data can be used to support their objectives.

Spatial Data Infrastructure

A consistent and coherent approach to handling the geographic aspect of data is essential for the efficient management, sharing and exploitation of such information. MOD has adopted a universal framework - the MOD Spatial Data Infrastructure - to coordinate policy, acquisition and information programmes, and ensure that spatial data is produced, managed and exploited effectively and efficiently.

In addition, the need to improve Defence's Records Management regime is well recognised. There have been several well publicised examples of where records management in MOD has been inadequate, resulting in financial cost and reputational damage to the Department. This has culminated in the announcement of a Records Management Improvement Programme, directed by Min (AF) and **led by CIO. Defence will** improve the management of key departmental records, in particular operational records, and those of strategic decision-making, with progress assessed by means of a records management maturity model. Action on communications, training and leadership, corporately and within TLBs, to take forward cultural change so that strategic risk is reduced, is also required.



Information Skills and Behaviours

Defence personnel need to be equipped with appropriate information skills and behaviours to deliver Defence outputs effectively.

Every person working in Defence generates and uses information, in one form or another, in their day-to-day activities. Information is as critical to the storeman who provides equipment to the frontline as it is to the commander or senior manager who makes key decisions on operations or in support areas. The strategic intent is that all Defence personnel use and exploit information proficiently and we seek to excel in areas which will have the greatest impact on the delivery of Defence outputs.

Improving our skills and behaviours is vital if Defence is to develop its desired information culture, a culture where we acknowledge the value of information and recognise that it is key to better-informed decision-making. We must develop this culture if we are to remain effective. This is not simple. As the Defence workforce reduces in size there is a significant challenge to maintaining the right skills, knowledge, IM organisations and tools. In addition there is a risk that corporate and organisational knowledge could be lost as organisations merge and seek to reduce in size. Maintaining a trained IM organisation provides essential mitigation to offset this risk.

Introducing Information Skills to new recruits to the Royal Navy

The e-learning package 'Information Matters', that forms an integral part of the Defence IM Passport product set, has been recognised by TLBs as an exemplar product that fully meets their requirements for foundation level IM up-skilling. Navy Command has decided that by the end of 2011 all officers will be required to undertake the Defence IM Passport as part of their basic training; this will ensure that the next generation of leaders are better prepared for the information challenges their roles will face.

This cultural change in IM behaviours is critical to Defence meeting its compliance obligations (such as the Data Protection Act (DPA), the Public Records Act (PRA), and Freedom of Information (FOI)). Cultural change is also required to meet the Defence aspiration of working better with allies, industry and OGDs. The Government's Civil Service Learning Programme will be a major influence on training offered on core IT applications; in addition the programme has already identified the Defence IM Passport as a package that could be adapted and applied pan Government.

CIO intends to continue engagement with the defence and security related departments to share our approach to improving skills and behaviours (including the training packages CIO has developed). This will promote more common and integrated ways of working across Government, resulting in economies of scale and therefore greater efficiency.

CIO will continue developing information professional training, including the validation of current courses and development of future requirements, where possible, with defence and security related departments.

CIO will provide consistent direction on information skills by introducing an Information Skills Compendium. The Compendium will provide the

essential on-line guidance and training pathways required by individuals wishing to develop and enhance their information skills. The Compendium will benefit those working in specific information roles and those seeking to enhance their core skills for wider development. The Compendium will include access to:

- The Defence Information Skills Framework and the related key information functional roles and competences;
- Information policies applicable to each role;
- The information related training available for each role.

CIO will (together with TLBs, Trading Funds and Agencies) agree the definition of "excelling in IM" for Defence, and target the areas that must strive to excel in IM. This will be benefits-led, based on information capabilities available and the experience from the IM "Beacons of Excellence" which have already been established across Defence and Government.

Operational Information Training

The introduction of IM foundation skills to those deploying on operations remains a key priority for CIO. We are working with both the Collective Training Group and The Defence College of Communications and Information to inculcate IM skills throughout mission specific training for deploying formations, tying together the behaviours required to the applications used in theatre. The most recent deploying brigade has benefited significantly from this approach and CIO will seek to ensure that this will become the standard way of deploying formation HQs.

CIO will carry out the role of Information Skills Champion for Defence, working coherently with wider Government initiatives.

Defence will, through the Head of Profession for IT (HOP IT), assess Defence priorities and the priorities of the Cabinet Office Government IT Profession Board to inform the continued development of the IT Workforce Plan. HOP IT will also reflect the priorities of other Heads of Discipline (including Information Assurance and Enterprise Architecture) leading to better alignment of military and civilian staff development.

The **Head of Profession for Knowledge and Information Management (HOP KIM) will** represent Defence at the Government Knowledge Council, and align interests to the Government KIM Profession. **HOP KIM will** lead on developing the KIM function in Defence, in collaboration with Heads of related disciplines. The introduction of updated information functional competences will assist with future workforce planning and guidance on professional development for staff.

CIO must scope the requirement for cyber skills, training and education at the generic and specialist level and scan the horizon looking at the impact of change on the generic information skill set required across Defence. The **Head of Profession for Cyber Skills (HOP Cyber Skills)** will take forward the cyber skills agenda for Defence.

Defence plans to embed the foundation skills laid down in the Defence IM Passport to achieve the IM maturity targets agreed with TLBs.

CIO will introduce an effective and timely induction process and CIO master classes for CIOs; this is a priority for the future if leadership is to start at Board level.

CIO will seek to provide more basic awareness training in the Defence IM Passport. This could include the incorporation of related information training such as; Protecting Information Level 1 and Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) / cyber foundational level training.

HOPs will, in consultation with CIO, undertake workforce planning for information professionals. In conjunction with TLBs, this will assess the skill sets and numbers of information professionals required for the future and, where possible, provide career mapping opportunities.

Information Architecture

We require a coherent federated Defence Information Architecture to support departmental decision makers by providing a clear, common articulation of information needs and processes.

We must become more efficient as well as more effective in our use of information; efficient in the use of ICT to exploit information and effective in understanding the information that we have and how it is being used across Defence. Today that understanding is fragmented.

In order to gain greater understanding a structured approach is required to both describe what we have today in information terms and where we wish to be in the future. To get this clarity **Defence will** use an Enterprise Architecture (EA) approach, a structured methodology built around the Ministry of Defence Architecture Framework (MODAF) and the Systems of Systems Approach (SOSA). This method will be used to capture and analyse information describing the current information environment and the future 'to be' state to help process owners and the acquisition community to produce effective and efficient information solutions; the Defence Information Architecture.

CIO will lead on the development and maintenance of the enablers required for the successful implementation of this architectural approach across Defence:

- Information Reference Architecture;
- EA policy;
- EA framework;
- EA skills;
- Governance;
- Federation.

Business Process Owner, Top Level Budgets, Trading Funds and Agencies will use the approach to capture and refine their information needs and flows against the CIO Information Reference Architecture. By ensuring a common approach, re-use patterns and common information services can be identified across Defence to help the Network Authorities develop an information Services Oriented Architecture.

Casualty Tracking

The effectiveness of casualty tracking was highlighted by adverse press coverage. To analyse the problem an architecture was used to understand the information flows both theoretical and in real life. Analysing these in a consistent manner allowed business planners to judge the risks in the areas of integration/interoperability or lines of development and make better decisions.

The successful implementation of the Defence Information Architecture is dependent on the availability of skilled information architects. **MOD needs** to grow its in-house pool of skilled architects to reduce the dependency on external support. The challenge is to develop architects that understand the business area they are working in, and who can apply their architecting skills. To support the growth of in-house skills, **CIO provides** a Head of EA Discipline to fit under the Information Skills Champion. **CIO will** lead on the development of best practice, including a methodology for producing the Defence Information Architecture, and describe the approach in a language that is understood by all, using plain English.

The Defence Information Architecture will provide:

- A top-level view of Defence which will be used to federate lower-level information architectures. This will allow for the identification of information flows between Process Owners;
- A reference architecture against which individual Process Owner architectures can be developed. By providing a common baseline it should be possible to identify where the same information service or ICT service can be re-used in different parts of Defence;
- A methodology against which to develop the architectures; this is in order to provide consistency of views;
- A means of describing new information needs, and references against which they can be judged.

The Defence Information Architecture can then be utilised to provide:

- The Network authorities with a common set of ICT services against which to develop a SOSA;
- Process Owners with a set of standardised information processes that can be re-used to support their core business;
- A reference guide against which procurement authorities judge the merit and fit of information projects.

Defence Information Services

Access to and management of cross-Defence information will be enabled via a portfolio of information services that serve individuals and organisations within Defence and externally.

The portfolio of services offered will change over the lifetime of this Strategy in response to the evolving information landscape and the opportunities that new technologies and innovation offer. **CIO will** continue to set policy in relation to these services. **Provision of some of these services is planned to be through the Defence Business Services Organisation (DBSO)**.

Existing legislative and cross-Government requirements retain their relevance for the foreseeable future, including the FOI regime, the DPA and our obligations in terms of record keeping. Newer drivers that will influence these services include the Government's transparency agenda, the Departmental Records Management Improvement Programme, the cross-Government digital agenda, and the reduction in the 30 year Rule for transferring records to The National Archives.

Defence Intranet

Contributing to the "Transforming Defence" agenda, the Defence Intranet has become the key communications channel with prominent access to information via the home page. The new Defence Intranet on DII F will exploit enhanced functionality to ensure messages regarding Transforming Defence are cascaded across Defence.

Core information services that are available to Defence and its external partners include:

- Web and Library Services. The Defence internet site provides a unified, coherent and consistent corporate website for Defence. Stakeholders can access authoritative information and connect with the right content, channels and services. It also enables them to engage openly with the Department. The Defence Intranet provides staff access to critical corporate and local tools, communications, information and applications. In the future these services must comply with the Cabinet Office-led programme of web rationalisation and support the Government's transparency objectives, where appropriate migrating MOD material to an expanded www.direct.gov.uk and making best use of appropriate shared services. **Defence will** develop a new, more modern and user-friendly Defence Intranet with improved functionality, including an enhanced electronic library. These electronic information services are complemented by other library services provided by Information Centres.
- Historical Analysis. Historical analysis supports policy and operational decision making, providing a stronger evidential base, enhancing the quality of decisions and ensuring that past lessons are considered. Maintenance of operational record keeping systems provides a body of information on which historical analysis can be undertaken and that is used to defend legal action taken against

the Department. It is also an effective and efficient way to identify and secure a vital record set that will be required for permanent preservation.

- Records Archiving and Review Services. Storing information safely and making it available to meet internal and external requirements ensures that the Department can keep and find information that it needs to re-use in the future and ensures that it complies with its statutory and legal requirements. We must meet the Department's Public Record Act responsibilities to review and transfer records to The National Archives, including preparing for the reduction in the 30 Year Rule in 2013. **CIO, with D IS and D ISS, will** develop an electronic archiving capability in Defence. **CIO shall** also position the Defence's paper archiving contract as the lead sector supply vehicle for the whole of central Government.
- Controlled Values Repository (CVR). The CVR makes authoritative data visible and available to Defence via a web-based service **provided by the DBSO**. It provides the Defence community with a portal to store and access authoritative sources of reference information. It improves information coherence, and thus interoperability, with future systems being built to recognised information exchange standards, to which legacy systems can also be mapped.

These information services contribute to the Defence Information Vision by reaching out to a wide audience within and outside MOD while also contributing to MOD's effective delivery of outputs by providing quality information. The services seek to improve Defence's ability to explain its actions and decisions in public, Parliament and the courts, which brings reputational, operational and financial benefits. The services serve to reduce costs through being able to defend better the Department against claims and legal cases improving efficiency through re-use of information. Better compliance with information legislation will also be achieved and keys national records preserved for future use by the public and historians.

Innovation

Innovation is required to enable the Department to exploit the opportunities offered by leading edge technologies and new WOWs.

Current and planned investment in information systems will deliver significant improvements, but there is scope to deliver far more through innovative use of information and new WOWs. Although pockets of innovation are delivering within Defence, we need to join these up and exploit other opportunities across Government, industry and our allies. In doing so, our staff will be more effective and efficient both on operations and in support areas.

Innovation will also help the Department optimise its investment in supporting ICT, by understanding how it can be exploited and where investment can deliver the greatest benefit by enabling new WOWs. It supports collaboration by identifying new ways to share and exploit information across Defence. Being Innovative will also allow Defence to lead in the cross-Government development and adoption of new uses of data and information.

Video Conferencing

Room based video conferencing facilities are now available in MOD, and DII will shortly be introducing desktop conferencing services. However use of video conferencing is currently patchy; further uptake will deliver savings in travel and subsistence, contribute to MOD sustainability targets and allow our people to collaborate and share knowledge more effectively. Through the innovation strand CIO is capturing the customer requirement to shape the delivery of video conferencing services and encouraging the user community to adopt these new ways of working.

To identify and benefit from innovation opportunities, **Defence needs** to:

- Capture external best practice. **CIO is** scanning the external environment to identify best practice and emerging trends to determine their potential application in Defence. Best practice will be sought from OGDs, industry and allies and other subject matter experts.
- Use research. **CIO is** identifying and capturing related research outputs from across Defence and other external bodies. Where appropriate, **CIO will** influence existing MOD research programmes or sponsor specific research to address particular innovation challenges. This activity will also help deliver coherence across the Department, and with OGDs, industry and allies.
- Identify existing shortfalls. **CIO will** work with Process Owners and CIOs to identify shortfalls in existing IM and IX practices and facilitate the development of innovative solutions.
- Identify latent IS capabilities. **CIO is** working with Defence ICT suppliers to identify latent and underused capabilities in our existing and future planned Information Systems which can provide information innovation opportunities.

To implement innovative ideas **Defence will**:

- Collaborate. **CIO is** developing a framework of innovation themes to guide the overall "direction of travel" within each area and help drive a coherent approach.
- Establish and refine policy, skills and standards. **CIO will** ensure that policy, skills and other supporting standards reflect and encourage the agreed direction of travel.
- Identify and implement short term wins. **CIO is** encouraging and supporting the implementation of short term innovation projects to deliver immediate benefit and ensure they are consistent with the long term direction. CIO will also sponsor concept demonstrators and pilots to raise awareness of the "art of the possible".
- Longer term development. **CIO will** plot the longer term development of innovation across Defence, influencing where required the future procurement of supporting ICT capability.

Workflow

DII is providing a workflow application. Workflow has considerable potential to deliver benefits through automating business and operational processes, ensuring consistent execution of those processes, enabling good information management, and providing effective management information. Workflow has been available on legacy systems for sometime but has achieved only limited uptake. Those areas that have used workflow have achieved significant benefits. The aim of the innovation strand of work in this area is to work with ATLAS as deliverers of the workflow capability to reduce the cost and time to implement solutions, and to identify exploitation opportunities and encourage uptake by the relevant process owner or TLBs.

To become more innovative **Defence must**:

- Develop innovation approaches and skills. There are specific innovations methodologies and supporting tools that can help teams find and deploy innovative solutions. The use of such methodologies, supporting tools and the requisite skills will be identified and where necessary further developed to encourage innovation within Defence.
- Embed innovation. **CIO is** working with the Through Life Capability Management team to clarify the key role of the Information Defence Line of Development (DLOD) to identify and embed innovation at all stages of a project lifecycle. This includes identifying skills required by staff fulfilling an Information DLOD role and looking to remove barriers to innovation. Working with sponsors, the Information DLOD will need to advise on how to facilitate and incentivise innovation by suppliers.
- Develop culture. As part of its commitment to developing skills requirements and sponsoring IM training, **CIO will** look to help change cultural attitudes. This includes encouraging innovative thinking and being prepared to challenge conventions. Innovative thinking is to be encouraged, valued and rewarded. Also, decision makers should be encouraged to balance the risks and benefits of innovative approaches rather than sticking to proven solutions.
- Share information. **CIO will** encourage communities of interest to be stood up and to exploit the new collaborative services being deployed across DII to share IM/IX best practice and innovations across the Department.

Way Forward

We live in a changing world and it is vital that we grasp opportunities as they arise and exploit information effectively. The continuing improvements in ICT are enabling rapid and widespread flow of information, which presents Defence with both challenges and opportunities. Current operations are no longer characterised by land, sea or air, instead they are a single battlespace, including cyberspace, in which our forces are increasingly dependent on information derived from a new generation of intelligence, surveillance and support systems. So that we continue to succeed we must become more agile and effective in how we manage and exploit information. This in turn will enable Defence to fulfil its standing commitments and to meet future challenges within its budgetary constraints.

This Strategy is intended to direct how we will improve our use of information across Defence by breaking down what needs to be done into seven Information Themes. Key high level activities are indentified within each theme; the details of each are contained within the SIP. **The MODIS EG will** provided oversight of progress of these activities and where necessary, will refocus priorities to ensure we remain on track to deliver the Defence Information Vision. However, to achieve the desired benefits **everyone involved in Defence from TLBs, Process Owners, industry, allies and OGDs, must recognise** their individual responsibilities and contribute to the achievement of the Vision. If you are unsure about your responsibilities seek help from your embedded IM professionals within your respective teams.

Published by the Ministry of Defence UK
This document is also available at www.mod.uk