Ministry of Defence

Cyber Resilience Strategy for Defence

Building a cyber resilient Defence

Contents

Contents 2
A Cyber Resilient Defence 3
Executive Summary 4
Strategy on a page 6
Strategic Context 7
01 The Imperative 8
02 Delivering Success 9
03 Strategic Priorities 11
04 Delivering the Vision 18
Appendix 1- Mapping the Strategies 21

A Cyber Resilient Defence

Laurence Lee, Second Permanent Under Secretary, Ministry of Defence

The risk of cyber-attack is amongst the highest that is managed by the Defence Board and it requires a collective response to address it. Becoming cyber resilient is the first challenging milestone. Remaining resilient will require constant appraisal of our adversaries and ourselves. We are not alone in developing and exploiting technologies and will need to work together across industry, Government, Allies and Partners to maximise our collective capabilities.

This MOD Strategy applies across Defence and outlines how we will successfully deliver the vision to:

Build a cyber resilient Defence

We must shape the secure Digital Backbone as the game-changing transformation that will reset cyber defence. We will build resilience into our critical capabilities and systems, and make new capabilities Secure by Design. Our relationship with industry will fundamentally shift to work ever closer in delivering wider defence and security. Our people will become increasingly cyber aware to become sensors of the abnormal and informed decision makers.

Building resilience into the delivery of our Defence Outcomes is a whole force challenge. A constant assessment of risk and continual assurance of our capabilities will inform our priorities and drive our focus to the right places. We will need to evolve our plans to counter, and rapidly recover from, an effective cyber-attack.

The focused pursuit of experimentation and innovation will underpin a ‘learn fast’ and ‘fail fast' approach which will allow Defence to securely adopt disruptive technologies that allow us to compete decisively with our adversaries.

I look forward to working with colleagues across Defence and Government, alongside those from science and technology, industry, academia, and with our partners and allies around the world, to deliver this ambitious and exciting agenda.

Our ambition to ‘*build a cyber resilient Defence’* is fundamental to delivering the singular secure, modern digital backbone for Defence. Our future success will be shaped by how we prepare ourselves to protect against, and respond to, our cyber adversaries. We must build our military capabilities with inherent resilience. This is the clear intent of our Cyber Resilience Strategy. It describes the journey we must all support to effect change across Defence. It is our people, our capabilities and our effectiveness as a military force that will benefit from Defence’s transformation to a cyber resilient organisation.

Charles Forte, MOD Chief Information Officer, Digital Functional Lead

Executive Summary

Context

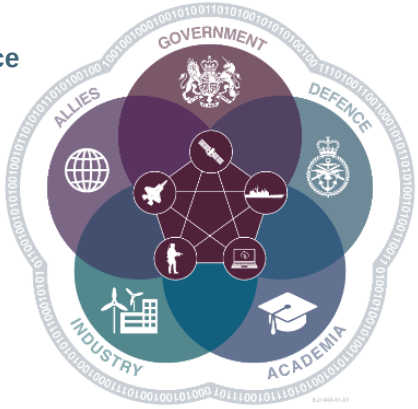
Defence's purpose is "to protect the people of the United Kingdom, prevent conflict, and be ready to fight our enemies. We are prepared for the present, fit for the future". Defence has a key role to play in underpinning the UK's legitimacy and authority as a cyber power by contributing to the National Cyber Strategy and Government Cyber Security Strategy.

In a world fundamentally shaped by technology, maintaining the Defence Purpose is dependent upon our resilience to cyber-attack. While Defence has made notable progress in recent years, there remains a significant gap between our cyber resilience today and where it needs to be. This gap is brought into sharp focus by the sheer volume of cyber-attacks that the Government sector experiences from a range of malicious threat actors.

The NCSC provides analysis[1] of cyber threats and global threat actors, like Russia and China, who continue to compete in cyberspace and develop capabilities and techniques that pose a serious risk to Defence in achieving its purpose.

Vision and Aim

This strategy's vision is therefore to **Build a Cyber Resilient Defence** to ensure that Defence can continue to deliver its purpose and support the national effort **strengthening the UK in the cyber domain and cement its authority as a democratic and responsible cyber power.**



To achieve its vision the strategy pursues a central aim - **for Defence's critical functions to be significantly hardened to cyber-attack by 2026, with all Defence organisations resilient to known vulnerabilities and attack methods no later than 2030.**

This is an ambitious but necessary aim. It will require the contributors from across Defence organisations and functions to proactively strive to deliver the Aim and the Strategic Priorities; they are the intended audience of this strategy.

The funding provided through the Integrated Review will deliver core capabilities, but it will not fund the totality of the demand necessary to achieve the aim. Defence organisations will need to collaborate with Defence Digital to define the resilience required to deliver the Defence Outcomes before reviewing the resource options and balancing the cyber risks posed by the adapting threats.

Delivering the aim will require immediate focus on delivering the basics of cyber resilience to implement the 'protect' element of the Integrated Operating Framework.[2] Achieving "an enduring foundation to both operate and warfight that is fundamental to deterrence and denial", will make Defence a significantly hardened target, protecting its data and operating without undue disruption. With foundational cyber resilience in place, Defence will be positioned to engage in increasingly sophisticated threats and continue to deliver the Defence purpose in a complex, dynamic and competitive world.

---

[1] NCSC Annual Review 2021- The Threat
[2] Integrated Operating Concept 2025

Strategic priorities

Defence's approach to achieving the aim is centred around seven strategic priorities each broken down into a series of outcomes. The outcomes are divided between those that will be led by Defence Digital and those that contributors from across the Defence organisations will need to proactively address.

Secure by Design: Our capabilities are inherently protected from the outset throughout their lifecycle, built to be resilient against cyber-attacks with pre-planned recovery measures in place.

Governance, Risk and Compliance: Our risk management approach provides good governance that drives change and achieves compliance.

Rapidly Detect and Respond: Our integrated cyber defences cover our critical functions providing the ability to detect and respond to cyber-attack.

People and Culture: The people in Defence are cyber aware, exhibiting the appropriate behaviours that form a positive culture and embeds cyber resilience across Defence's outputs.

Industry: Our relationship with industry is enhanced, allowing us to achieve improved supply chain security and resilience outcomes.

Secure Foundations: Our entire digital enterprise incorporates security controls, supported by people and processes, that make it resilient to cyber-attacks.

Experimentation, Research and Innovation: Our approach seizes upon experimentation, research and innovation opportunities to ensure we can stay ahead of the developing cyber threat.

"To deliver this strategic priority, Defence organisations must have:"

These call out boxes will highlight to organisations beyond Defence Digital what activity they need to prepare for.

Look out for these quick-info boxes throughout the strategy

I commend this strategy to everyone in Defence. A cyber resilient Defence is the foundation that enables us the freedom of action to achieve decision advantage and enables the successful delivery of the Defence Outcomes.

R Adm Nick Washer,
Director of Operations for Defence Digital in Strategic Command

Strategy on a page

DIAGNOSIS

Where Defence is today

FACTORS DRIVING THE NEED TO CHANGE:

- Developing Threats
- Evolving Environments
- Advancing Technology

The risk of cyber-attack is amongst the highest that is managed by the Defence Board and it requires a collective response to address it.

FACTORS THAT MUST BE OVERCOME:

- Misaligned Culture
- Endemic Obsolescence
- Inadequate Cyber Resilience

STRATEGIC PRIORITIES

Where Defence needs to be:

THE AIM: for Defence's critical functions to be significantly hardened to cyber-attack by 2026, with all Defence organisations resilient to known vulnerabilities and attack methods no later than 2030

Secure by Design	Governance, Risk and Compliance	Rapidly Detect and Respond	People and Culture	Industry	Secure Foundations	Experimentation, Research and Innovation
Our capabilities are inherently protected from the outset throughout their lifecycle, built to be resilient against cyber-attacks with pre-planned recovery measures in place.	Our risk management approach provides good governance that drives change and achieves compliance.	Our integrated cyber defences cover the entire digital environment to detect and respond to cyber-attack.	The people in Defence are cyber aware, exhibiting the appropriate behaviours that form a positive culture and embeds cyber resilience across Defence's outputs.	Our relationship with industry is enhanced, allowing us to achieve improved supply chain security and resilience outcomes	Our entire digital enterprise incorporates security controls, supported by people and processes, that make it resilient to cyber-attacks	Our approach seizes upon experimentation, research and innovation opportunities to ensure we can stay ahead of the developing cyber threat.

WAYS

How to achieve our strategic priorities

Based on the national effort led by Government, MOD will direct the activities across Defence to achieve the Vision

Adaptive in our approach

Adaptable to changing threats, risks and able to manipulate technology to our advantage, using agile processes to assure the Defence Outcomes.

Secure and resilient

Every part of the digital environment will be built to incorporate inherent protection from, and resilience against, cyber-attack, routinely updated to maintain cyber security, and designed to be interoperable with cyber defence capabilities through-life.

Whole Force Effort

Every person who interacts with the digital environment, regardless of the system they are using, is responsible for protecting Defence against its adversaries. Every person is part of our cyber defences and has a role in protecting against malicious activity.

Collaborative, integrated and cohesive

Defence must work ever closer with the National Cyber Security Centre, Government, Allies and Partners, and Industry to counter emerging cyber threats together as a National effort.

MEANS

Enablers and contributors to achieve Ways

Delivering the Vision requires the following *enablers*

- Construction of the secure Digital Backbone,
- Successful delivery of the Defensive Cyber Programmes,
- Equipment capability programmes focusing on cyber security from the outset to make Defence capabilities secure by design,
- Embedding modern security ways of working and constructively challenging security preconceptions,
- Shift towards a new security relationship with industry,
- Acceleration of agile commercial constructs for the procurement of cyber capabilities,
- Development and employment of the cyber workforce with suitable cyber skills within Defence,
- Establishment of cyber defence organisations within the organisations of the contributors to the strategy,
- Creation and testing of operational resilience plans by the contributors to the strategy,
- Development of clear and agreed accountabilities for all aspects of cyber resilience.

Delivering the Vision requires the following *contributors*

- Capability Sponsors, Senior Responsible Owners (SROs), Acquisition Organisations and Operating Authorities (OAs).
- Leaders of Functions and Defence organisations.
- CIOs and security specialists of Defence organisations.
- Operational Commanders
- Industry

Strategic Context

Defence needs to be a hard target in cyberspace, resilient to cyber threats, able to operate with freedom in all the operational domains and compete both below and above the threshold of conflict. Achieving this will enable us to exert influence and present credible deterrence, and support the UK's ambition of being a responsible cyber power.

The challenge is both individual to Defence and a collective whole force mission for industry, Government, and our Allies and Partners. Achieving the aim is crucial to enabling the Government's vision[3] to place the UK at the forefront of global action on a safe digital future across the 'future frontier' of cyberspace.

The Digital Strategy for Defence outlines the step-change in approach that is required for Defence to leverage our digital capabilities and our data as fundamental enablers to facilitate faster, better decisions and improved Defence outcomes. Defence's deepening dependency on digital, ICT and data is at the heart of transformation plans and future Defence operational capabilities. However, the dependency also carries risks for Defence, as it provides increased opportunities for our adversaries if we do not develop, at the same time, our digital security and operational resilience.

Over the last 5 years we have seen an exponential rise in the number of global cyber-attacks, crippling organisations and highlighting the need for good cyber hygiene and a firm appreciation of the cyber risk in context. For Defence, this means understanding the threat to Defence capabilities, functions and operational outcomes. It is critical to Defence's operational delivery that capabilities are Secure by Design throughout their lifecycle, or we risk fundamentally undermining the game changing opportunities that come with automation, artificial intelligence, autonomous vehicles, mixed reality, synthetic environments and, eventually, quantum computing.

To integrate the operational domains, as detailed in the Integrated Operating Concept[4], we must be persistently secure, defendable and operationally resilient in the right place at the right time.

Delivering the vision involves being ever more intelligence led about our adversaries, understanding the wider cyber threats to Defence Outcomes and adopting the mindset of our adversaries to counter them. Achieving our aim will allow Defence to continue engaging in the sub-threshold to effectively protect, engage and help constrain our adversaries who seek to exploit the Cyber and EM domain for their own ends.

This strategy details the necessary changes to embed cutting-edge defensive cyber capabilities and represents the ambitions of the Digital Strategy for Defence and the Defence Cyber Strategy. It focuses on the strategic priorities that will be directed and cohered by Defence Digital as the functional owner for digital across Defence. The outcomes will be delivered in collaboration with industry and academia, and in cooperation with Government, Allies, and Partners.

*"The Cyber and Electromagnetic **threat to Defence** and its outcomes as part of a multi-domain force is both **potent, live, ubiquitous and increasing**.*

Success in the land environment, as with all others, is critically mortgaged on the security and resilience of our use of Cyber and Electromagnetic ecosystem.

This freedom of action is far from assured; redoubling our awareness, our capability our processes and drills in cyber resilience is essential and increasingly so."

Maj Gen John Collyer, Director Information and Army Chief Information Officer

[3] Set out in Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy Integrated Review Announcement, dated March 2021

[4] Integrated Operating Concept 2025, (publishing.gov.uk)

01 The Imperative

Defence is in an era of systemic competition with those who seek to gain an advantage over us. This means Defence must adapt to maintain pace with digital change, rapidly adopt game-changing technologies and assure the secure delivery of the Defence Outcomes.

Factors driving the need to change:

Developing Threats. Cyber adversaries continue to proliferate. Tools and capabilities previously only available to high-end State actors are more openly available. Proxy actors offer malicious cyber effects 'as a service' to deliver disruptive attacks or espionage. State actors remain willing to engage in complex, malicious activity through cyberspace in the knowledge that attribution is challenging and will further broaden their techniques to incorporate automation of their techniques.

Evolving Environments. Defence is changing how it works in relation to digital technology, pushing out to the tactical edge with an increasing dependency on data that resides in industry. The digital threat surface is expanding and crosses traditional security environments increasing the demand for new solutions to secure our digital environment. The traditional methods of securing digital will not see us into the future.

Advancing Technology. Exponential advances in technology have made the world more interconnected than ever before, driving extraordinary opportunity, innovation and progress. The scale and pace of this change often exceeds the evolution of our doctrines, policies and organisations whilst unleashing unprecedented complexity, instability and risk.

Factors that must be overcome:

Misaligned Culture. From personal awareness and behaviours through to the frameworks guiding capability decisions, our people must be equipped to make wise choices and operate securely on the front line of the digital environment. All people in Defence have a role to play in delivering the vision. They must become, and remain, cyber aware and capable of making appropriate security decisions.

Endemic Obsolescence. Defence's existing digital environment has grown organically over many years, with ever perpetuating technology debt and security vulnerabilities. This has allowed obsolescence to endure and risks our ability to deliver Defence Outcomes. Defence organisations will need to will need to accelerate the elimination of obsolete technologies across the digital environment. Where obsolete technologies continue to remain in-service, they must be actively risk managed and funded.

Inadequate Cyber Resilience. There is an inextricable dependency between the delivery of the Defence Outcomes and the digital environment that underpins and enables activity. The dependency extends out to industrial digital eco-systems. The reliance on digital services carries a large risk, therefore the impact of losing these services must be clearly understood. This risk can be mitigated through resilience and recovery measures that appreciate and counter cyber threats.

"MOD has a key role to play in the UK being a responsible cyber power. This means it has never been more important to focus and reset defensive cyber.

This strategy is central to actively tackling threats to cyber security, securing the Digital Backbone, and underpinning Defence's ability to operate freely in cyberspace.

We all have a role to play to build a cyber resilient Defence."

Christine Maxwell

Director of Cyber Defence and Risk

02 Delivering Success

The Contributors

The MOD Chief Information Officer (CIO) is accountable to the 2nd Permanent Under Secretary of State and to the Commander UKStratCom as the functional leader for digital.

The Director of Cyber Defence and Risk (CyDR) is responsible to CIO for directing the effort to deliver the vision. The Cyber Resilience Strategy is the document that coheres the required outcomes which must be achieved across Head Office, Front Line Commands, the Top Level Budgets and all Enabling Organisations (hereafter referred to as "Defence organisations").[5] The Higher Level Budgets (HLB) are assumed to be a subset of the appropriate FLC or TLB. The individuals who perform the functions detailed below are the audience of this document.

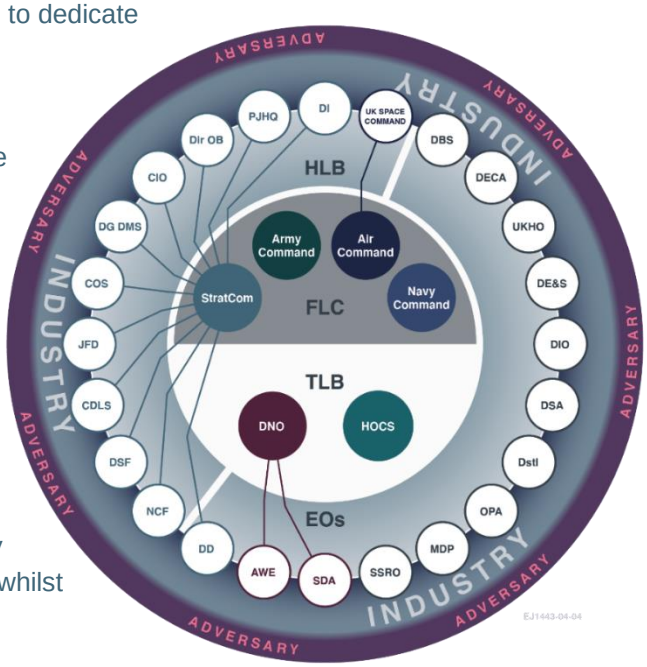
Capability Sponsors, Senior Responsible Owners (SROs), Acquisition Organisations and Operating Authorities (OAs). These contributors are responsible for developing, procuring, and operating Defence capabilities and the digital enterprise. They will need to fund the cyber resilience measures to make capabilities secure.

Leaders of Functions and Defence organisations. These contributors are responsible for delivering Defence Outcomes and will need to dedicate resources from their organisation to deliver resilience.

CIOs and security specialists of Defence organisations. These contributors are responsible for the security and resilience of their digital assets and will require specialists who can advise and guide capability decision makers and leaders of Defence organisations.

Operational Commanders. These contributors are responsible for the secure and resilient operation of digital assets worldwide and will need to invest intellectual effort in developing operational resilience that minimises the impact of cyber-attack.

Industry. These contributors will need to deliver capability that is Secure by Design and integrated with our defences whilst actively protecting our data throughout the supply chain.



This strategy will steer contributors by laying out the **digital environment** we seek to change and outlining the **guiding principles** to successfully deliver the vision. Supporting these contributors will be enthusiastic teams comprising industry, Government, Allies, Partners and academia. This joint effort will deliver the best for Defence; their understanding of the detail of this Strategy will be essential to enable them to contribute effectively.

[5] How Defence Works dated Dec 20.

The Digital Environment

Defence's **digital environment** has been divided into three high level areas:

Defence capabilities. All capabilities, platforms or otherwise, which incorporate digital assets organically. This typically includes the digital assets procured by DE&S and other acquisition organisations.

Digital enterprise. The digital assets, networks, applications and data which form the Digital Backbone upon which most Defence capabilities, functions and outputs depend. This typically includes traditional Information eco-systems purchased either by Defence Digital or directly by the FLC, TLBs and EOs.

The Whole Force. The people, including their digital identities, who operate the Defence capabilities or interact with the digital enterprise. This typically includes all Crown Servants, defence contractors, industry, and Government.

***Digital Assets*: A term that captures all digital devices in Defence be they Information Communication Systems, Operational Technologies, smart devices, Internet of Things devices, wearable technologies, Electro-magnetic devices, SCADA devices and any other devices that could be exploited by cyber-attack. Although not digital, analogue devices have been included in this definition for completeness as part of the human-made environment of cyberspace.**

The Guiding Principles

The delivery of the strategy will adopt the following guiding principles:

Adaptive in our approach. Adaptable to changing threats, risks and able to manipulate technology to our advantage, using agile processes to assure the Defence Outcomes.

Secure and resilient. Every part of the digital environment will be built to incorporate inherent protection from, and resilience against, cyber-attack, routinely updated to maintain cyber security, and designed to be interoperable with cyber defence capabilities through-life.

Whole Force Effort. Every person who interacts with the digital environment, regardless of the system they are using, is responsible for protecting Defence against its adversaries. Every person is part of our cyber defences and has a role in protecting against malicious activity.

Collaborative, integrated and cohesive. Defence must work ever closer with the National Cyber Security Centre, Government, Allies and Partners, and Industry to counter emerging cyber threats together as a National effort.

03 Strategic Priorities

Secure by Design

Our capabilities are inherently protected from the outset and throughout their lifecycle, built to be resilient against cyber-attacks with pre-planned recovery measures in place.

Instil Secure by Design as standard into the digital environment of Defence capabilities. We will:

1. Define and communicate the key principles of Secure by Design[6] based on international standards and NCSC guidance.
2. Update policy based on modernised, simpler cyber security standards.
3. Support programme teams to adopt new Secure by Design ways of working.
4. Refresh and modernise approach to accreditation.
5. Revise mechanisms for escalating non-compliance and subsequent risk management.

Counter threats to the digital environment. We will:

1. Identify and implement risk reduction measures that can be applied in the near term to enhance the cyber resilience for operations.
2. Reset the standards for digital business continuity (fight through) and disaster recovery (rebuild).
3. Participate in Government, Allied and Partners business continuity and disaster recovery exercises.

***Secure by Design*:** An approach that enables a culture of proactive risk management and appropriate security consideration throughout a capabilities' lifecycle by connecting cyber security principles, roles, processes, tools and techniques to achieve secure systems

"In a competitive world where the cyber threat and our reliance on digital technology is constantly increasing, it is imperative that cyber-security is a driving function in all that we do. Whether projecting power or keeping the homeland secure, we must preserve our freedom of action through proactive cyber defence and integrated 'Secure by Design' thinking."

Lt Gen Robert Magowan

Deputy Commander UK Strategic Command

To deliver this strategic priority, Defence organisations must have:

1. Ensured that new capabilities will adopt the Secure by Design policy and principles.
2. Resourced security skills into programme and project teams to properly identify security requirements.
3. Created mechanisms to support SROs and delivery teams to assess security risks clearly before considering options to trade out security.
4. Passively and actively exercised the business continuity and disaster recovery plans to demonstrate operational resilience.

[6] https://www.ncsc.gov.uk/collection/cyber-security-design-principles

Governance, Risk and Compliance

Our risk management approach provides good governance that drives change and achieves compliance.

Identify and visualise the risks posed to Defence Outcomes.
We will:

1. Continue to analyse the risks posed to Defence Outcomes considering developing cyber threats.
2. Define our critical systems and the levels of resilience each needs.
3. Engage with our critical suppliers to improve the supply chain security.

Implement governance mechanisms to deliver risk reduction across Defence. We will:

1. Provide new pan-Defence cyber security policy.
2. Continually evolve our risk response plans and use key risk indicators to measure progress across all Defence organisations.
3. Conduct compliance checks across Defence organisations and industry to identify and remediate shortcomings in cyber resilience.
4. Direct the coherent pan-Defence view of risk by supporting Defence organisations in their internal analysis.

Support National efforts to achieve the vision of the UK as a Cyber Power. We will:

1. Work ever closer with the National Cyber Security Centre (NCSC) and other Government Departments to accelerate advances in defensive security maturity
2. Adopt a default 'share' posture and actively collaborate with Government, Allies and Partners where policy permits.
3. Assess the cyber maturity of MOD as a department to demonstrate Defence's contribution to improving cyber resilience across Government.

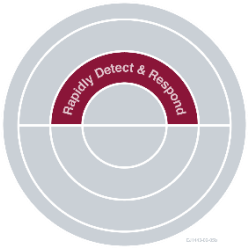
"One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks. Fix the basics, protect first what matters for your business and be ready to react properly to pertinent threats."

Stéphane Nappo, Global Head Information Security Société Générale International

To deliver this strategic priority, Defence organisations must have:

1. Defined their cyber risk governance arrangements and identified persons accountable for driving down cyber risk.
2. Understood their information assets, cyber risks and risk appetites to inform risk reduction planning.
3. Proactively engaged in the range of compliance assessments and evidenced progress in risk reduction.

Rapidly Detect and Respond



Our integrated cyber defences cover our critical functions providing the ability to detect and respond to cyber-attack.

Entrench strong detect and respond functions for all teams engaged in cyber defence. We will:

1. Produce situational awareness which informs the decision-making process.
2. Generate and implement use cases for detections, informed by threat user behaviour.
3. Aggressively implement higher quality detection methods.
4. Evolve our processes and authorities[7] for coordinated response to detections.
5. Assertively automate our processes to reduce the workload on the cyber defenders and increase the speed of response.
6. Continue to identify learnings from experience to implement positive change in detect and respond.

Equip our cyber defenders to outpace our adversaries. We will

1. Strengthen defensive cyber planning for our standing operations.
2. Provide the necessary detection and response tools to defend the digital environment.
3. Integrate resilience into the function of cyber defence.
4. Mature our federated cyber defence organisation to be adaptive.
5. Improve our integration with the National Cyber Force to develop our counter cyber operations as part of a more active defensive posture.

Instil a collaborative approach to cyber defence with Government, Allies and Partners. We will:

1. Further integrate and improve our operational effectiveness.
2. Participate in cyber exercises which test our collective cyber response.

"Too often organizations repeat the mistakes of the past and do not learn lessons from significant cyber incidents."

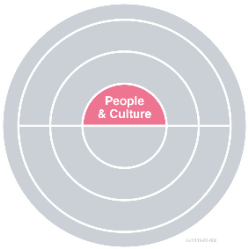
US Executive Order on improving the Nation's Cybersecurity

To deliver this strategic priority, Defence organisations must have:

1. Determined their requirement for organic cyber defence organisations that will operate as part of the federation.
2. Generated and resourced organisations to conduct cyber defence for their part of the digital environment.
3. Implemented detection capabilities across their part of the digital environment.
4. Adopted common cyber defence playbooks and regularly conduct exercises to test coordinated cyber incident response.
5. Routinely conduct post-incident analysis and take action to improve cyber resilience.

[7] There is a Chief of Defence Staff Directive that provides the authorities and actions for the coordination of Defensive Cyber Operations within Defence.

People and Culture



The people in Defence are cyber aware, exhibiting the appropriate behaviours that form a positive culture and embeds cyber resilience across Defence's outputs.

Enhance individual awareness of cyber threats and good digital security practises. We will:

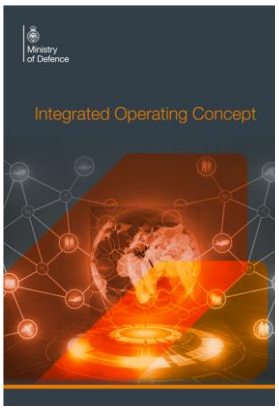
1. Ensure the mandatory training for the Whole Force incorporates up to date cyber security and resilience content.
2. Identify and counter the top bad behaviours, bespoke to specific missions where appropriate, through engaging and relevant discourse-shaping content.

Improve collective behaviours by making the right thing to do the easy thing to do. We will:

1. Impact culture progressively by identifying and countering the top risk behaviours.
2. Train and educate people how to act as part of our cyber resilience.
3. Adopt the available information management and data protection tools to help the Whole Force do the right thing naturally.
4. Integrate with 'good suggestion schemes' to own, prioritise and progress cyber resilience proposals.
5. Provide the appropriate training to enable collective cyber defence.

Nurture the cyber specialist cadres within Defence. We will:

1. Support the development of the cyber specialism within the wider security profession.
2. Maximise the use of unified career management for military cyber specialists.
3. Build advisory services that can support the contributors to this strategy.



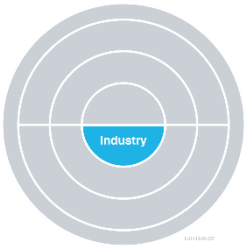
"Sub-threshold operations are continuously executed at reach by malign actors who seek to undermine our military readiness, our critical national infrastructure, our economy, our alliances and our way of life."

Integrated Operating Concept

To deliver this strategic priority, Defence organisations must have:

1. Developed the foundational cyber security skills across their workforce, whilst continuously enhancing and maintaining the proficiency of their cyber professionals.
2. Fostered a positive, whole force, culture which empowers its people to learn, question and challenge resulting in continuous improvements of cyber security practises and design.
3. Understood the cyber skills demand and populated their organisations with the appropriate expertise to deliver their Defence Outcomes.

Industry



Our relationship with industry is enhanced, allowing us to achieve improved supply chain security and resilience outcomes.

Reset the relationship with industry. We will:

1. Create security relationships that transcend contracts to build mutually supportive cyber resilience based on clear strategy and policy.
2. Use cyber security forums, in conjunction with NCSC, to set out the critical reliance Defence places on cyber security and to collaborate on solutions to supply chain security issues.
3. Improve visibility and understanding of suppliers of our critical capabilities.

Protect Defence data residing in Industry. We will:

1. Strengthen the protection of high value Defence information residing in industry and the supply chain by refreshing the Defence Cyber Protection Partnership process.
2. Implement solutions to allow controlled and auditable access to data held on Industry or Defence's networks.
3. Audit cyber resilience of our suppliers, using recognised international standards, and work together to implement required improvements.

Unite with industry to implement the Secure by Design principles and policies. We will:

1. Ensure industry generates future capabilities that are Secure by Design by using new contractual mechanisms developed collaboratively with our suppliers.
2. Collaborate with industry to improve the resilience of current capabilities by ensuring they are compliant with best practise and policy.

Strengthen cyber resilience in the supply chain. We will:

1. Recognise those suppliers who progressively improve their cyber resilience.
2. Conduct cyber security exercises, together and independently, to allow continuous improvement of our collective cyber resilience.

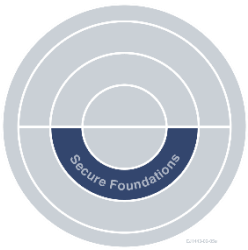
"DE&S places over 800 new contracts every year; each one representing a golden opportunity to embed stronger cyber discipline into Defence's relationship with industry."

Nigel Shaw, DE&S Chief Digital Information Officer

To deliver this strategic priority, Industry will need to:

1. Adopt an open mindset to resetting security relationship.
2. Actively support cyber resilience audits and drive forward remedial actions.
3. Improve the protection of Defence information and embrace the adoption of Secure by Design policy throughout the lifecycle of military capabilities.
4. Proactively develop Business Continuity and Disaster Recovery Plans, intentionally engage in creating exercising opportunities, and demonstrate operational resilience.

Secure Foundations



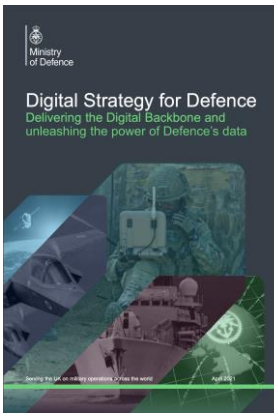
Our entire digital enterprise incorporates security controls, supported by people and processes, that make it resilient to cyber-attacks.

Build secure foundations into the Digital Backbone of Defence. We will:

1. Embed modern security controls and requirements into the digital backbone programmes that underpin the Digital Strategy for Defence.
2. Implement a zero-trust architecture that applies the appropriate security controls based on a data centric security model.
3. Transform the crypt-key capability to keep our secrets secret.
4. Deliver a modern, centralised identity and access management service to make sure the right individuals to access to the right resources at the right time, and for the right reasons.
5. Create a service catalogue of trusted security control solutions that must be adopted across Defence.
6. Trial and test new security solutions early to be on the front foot.

Extend cyber resilience foundations to the wider Digital Environment. We will:

1. Create and embed cyber common technology architectural patterns for wide adoption.
2. Drive robust information management and data protection solutions and ways of working.
3. Embrace opportunities to connect cyber resilience foundations with industry.



"Warfare will be enabled at every level by a digital backbone into which all sensors, effectors and deciders will be plugged."

Digital Strategy for Defence

To deliver this strategic priority, Defence organisations must have:

1. Adopted standard technologies and centrally implemented cyber resilience solutions as they are developed and launched.
2. Driven security improvement through obsolescence replacement and robust IT basics.

Experimentation, Research and Innovation

Our approach seizes upon experimentation, research and innovation opportunities to ensure we can stay ahead of the developing cyber threat.

Operationalise the approach to experimentation, research and innovation (ERI). We will:

1. Align to Defence ERI efforts, coherent with the MOD Science and Technology Strategy 2020 and the Digital Foundry.
2. Create an innovation model that allows Defence people to engage with the continuous improvement of our cyber resilience.
3. Work with the Digital Foundry to ensure all Defence contributors can maximise their data and be secure in the rapid development of applications.
4. Work with the Defence Science and Technology community to drive the development, analysis, and testing of concepts for future Defensive Cyber capabilities.
5. Engage with science, technology, research and innovation hubs across the UK to seize opportunity and integrate it into our cyber resilience efforts.
6. Relentlessly innovate to improve the capabilities of the Cyber Security Operations Capability that stretches across Defence.

Develop insights through learning. We will:

1. All cyber security and resilience activities will have a lessons learnt process embedded.
2. Analyse lessons to generate learning and insights for prioritisation and risk reduction action.

Scan the horizon of cyber defence technologies and research for utilisation in Defence. We will:

1. Commission research through industry and academia.
2. Review research from a range of sources, including academia, to maintain awareness of thinking in cyber security and resilience.
3. Track future cyber threats and technological mitigation opportunities.

"The National Cyber Strategy outlined how the UK would take the lead in the technologies vital to cyber power. This will be a national effort, built on world class Science and Technology (S&T) skills, alliances, industry and university partnerships, and one in which Defence has an important role."

Defence Cyber Strategy

To deliver this strategic priority, Defence organisations must have:

1. Engaged in Experimentation, Research and Innovation as part of whole force improvements to cyber resilience.
2. Implemented an approach to share insights and horizon scanning observations.

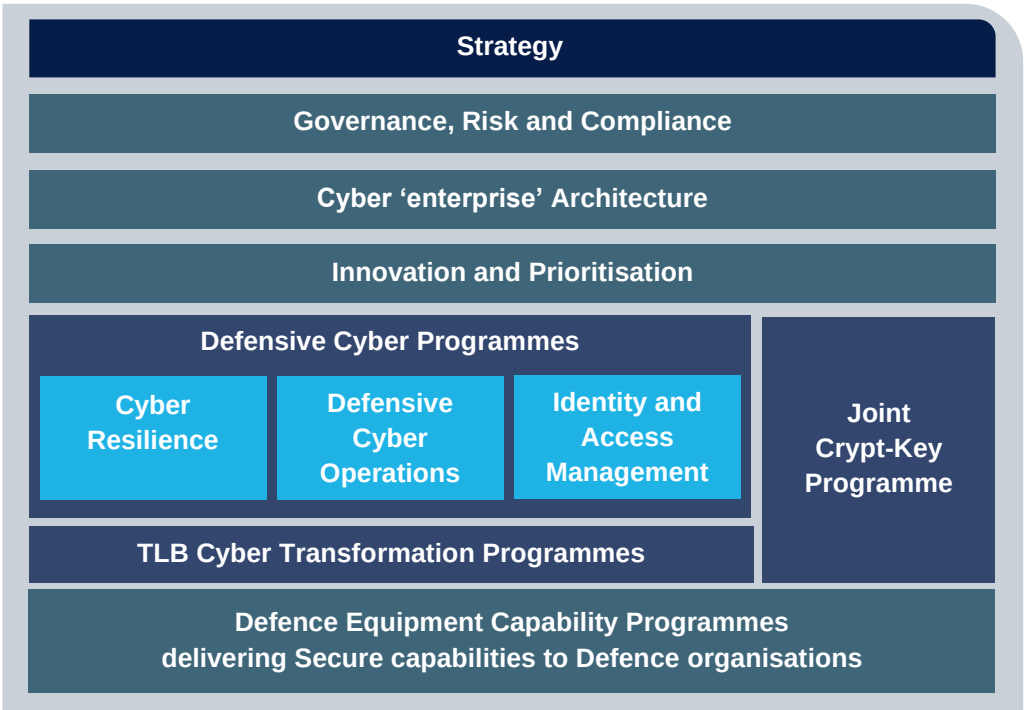
04 Delivering the Vision

Governance

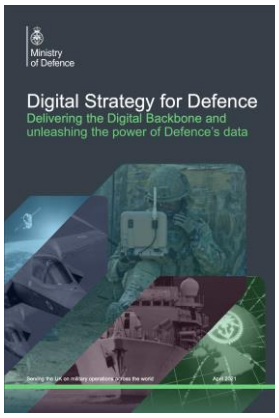
The coherence of all activity detailed in this Strategy will be managed through a defensive cyber governance structure that supports the overlapping efforts of the Security Function, Digital Transformation, and Domain Coherence.

Clear cyber security policy will guide the whole force effort to become secure and resilient. Architectures will be defined to inform the secure design of the Digital Environment and cyber security organisations equipped with technology to defend Defence from cyber-attack. An updated innovation engine will become the focal point for rapidly taking ideas through to impact. This will enable all Defence organisations to deliver their contribution to the vision. Prioritisation will continue to be risk-led and threat-informed to focus our investment onto the right areas.

Defensive Cyber Programmes[8] will be the delivery mechanism for centrally run and specialist cyber capabilities and these will complement existing cyber transformation programmes from across the Defence organisations. Cyber Defence and Risk will be the authority that guides the wider Defence equipment capability programmes as they implement the core cyber protections and oversee the delivery of Secure by Design capabilities to Defence organisations. In parallel, the Joint Crypt-Key programme will transform how crypt key solutions are delivered for high grade use.



The Integrated Review settlement has funded the Defensive Cyber Programmes. There remain some cost liabilities that will lie with the strategy contributors. These are costs relating to specific cyber protections and mitigations implemented by the Defence organisations. Defence capabilities have always had the requirement to fund



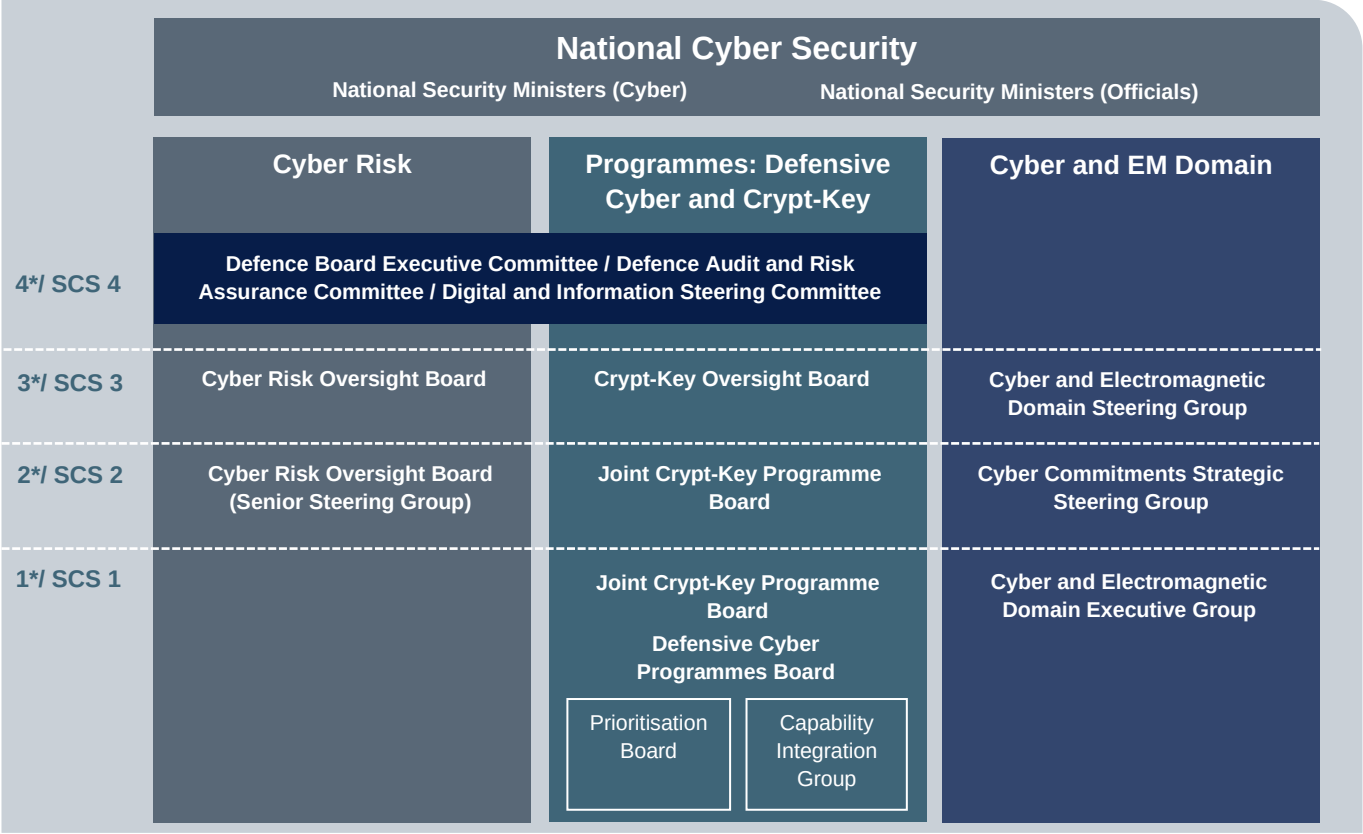
"In the future, technology will be the backbone of a truly integrated force – but today, a significant proportion of our technology systems are fragmented, fragile and obsolescent."

Digital Strategy for Defence

[8] Beyond the three key programmes there is also the Future DCO (FDCO) project that is currently managed by UK Strategic Command CapC4ISR, as the defensive cyber work strands of the Science and Technology programme that links into Dstl.

security although the new secure by design approach will change the profile of this and hopefully reduce cost overall.

The current governance structures that manage risk, programme delivery, and development of the cyber domain all feed into the National Security Ministers forums to demonstrate Defence is delivering towards National Cyber Strategy and Government Cyber Security Strategy outcomes.



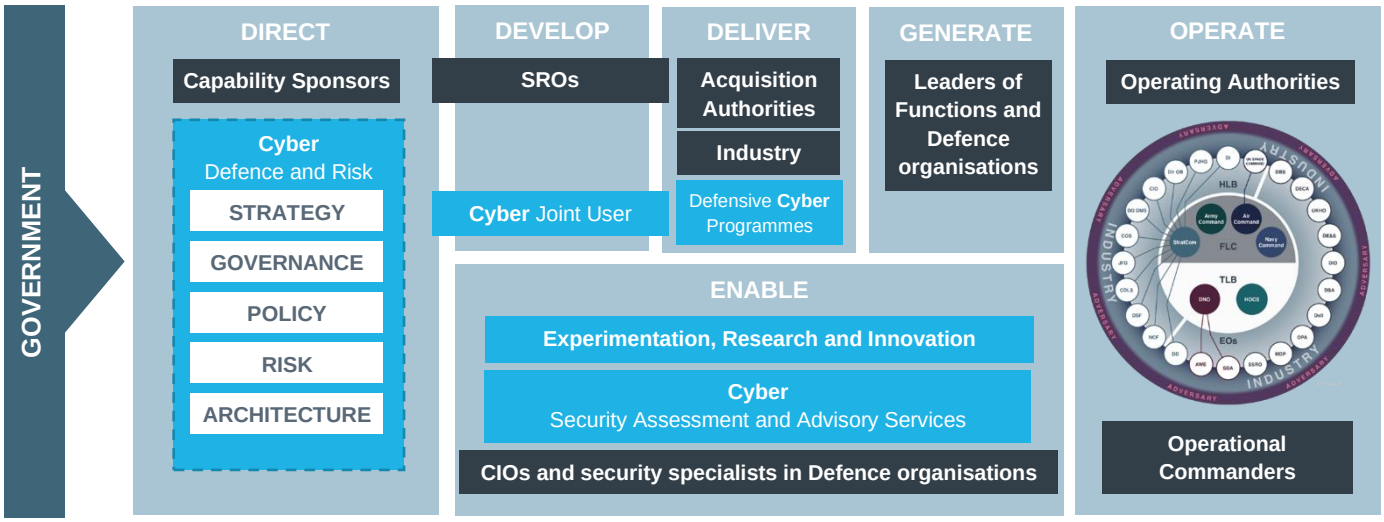
Key Enablers

Delivering the vision requires the following enablers:

- Construction of the secure Digital Backbone,
- Successful delivery of the Defensive Cyber Programmes,
- Equipment capability programmes focusing on cyber security from the outset to make Defence capabilities secure by design,
- Embedding modern security ways of working and constructively challenging security preconceptions,
- Shift towards a new security relationship with industry,
- Acceleration of agile commercial constructs for the procurement of cyber capabilities,
- Development and employment of the cyber workforce with suitable cyber skills within Defence,
- Establishment of cyber defence organisations within the organisations of the contributors to the strategy,
- Creation and testing of operational resilience plans by the contributors to the strategy,
- Development of clear and agreed accountabilities for all aspects of cyber resilience.

Operating Model

The high-level operating model, overlaid across the Defence Operating Model, is shown below with key cyber functions in blue and strategy contributors shown in dark grey.



Based on the National effort led by Government, Cyber Defence and Risk will direct the activities that must be completed to deliver the vision. It will be for the Capability Sponsors, SROs, and Operating Authorities to implement core cyber protections and oversee the delivery of Secure by Design capabilities that will be delivered by equipment capability programmes, industry and delivery teams. For the Defensive Cyber Programmes, the Defensive Cyber Joint User will perform this role.

The force generation of capabilities will continue to lie with Front Line Commands and wider Defence organisations who will then operate the capabilities and underpinning digital environment.

Enabling all of this activity to occur will be the CIOs and security specialists within the Defence organisations who may call upon the Cyber Advisory Services to provide specialist advice and guidance based on Security Assessments. The Experimentation, Research and Innovation effort will enable solutions to novel or emerging problems that must be overcome to become cyber resilient.

Operating models with greater detail and specific accountabilities will be delivered as required.

Appendix 1- Mapping the Strategies

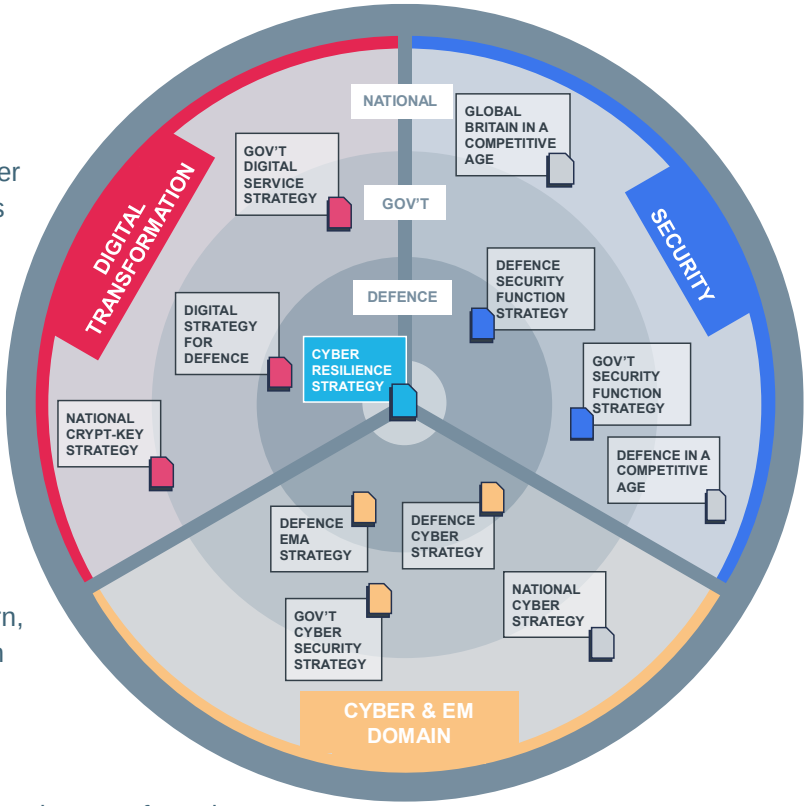
To achieve the vision, the Cyber Resilience Strategy will support three overlapping efforts:

Domain coherence

The projection of power through the Cyber and Electromagnetic Domain requires defensive cyber to work in combination with offensive cyber. This Strategy will support the Defence Cyber Strategy and align to the National Cyber Strategy and the Government Cyber Security Strategy. Over time, the various strategies across the Cyber and Electromagnetic Domain will mature and converge.

Security function

Cyber security is a sub-set of wider security. This strategy will support the delivery of the Defence Security Function Strategy which, in turn, contributes to the Government Security Function Strategy.



Digital function

A secure Digital Backbone is critical to maximising the use of our data. This Strategy will support the creation of the Digital Backbone by ensuring it is built upon a secure foundation. The strategies that sit within the Digital Strategy for Defence include the Data Strategy and the Digital Technology Strategy along with a grown number of strategies that focus on specific topics.

Within this wider context, this Strategy will define and cohere the initiatives necessary to deliver the vision. This document will be reviewed every 18 months to maintain coherence with National and Defence concepts, policy and wider strategies.