Contemporary Issues in Air & Space Power
Air and Space Power Centre

Sobb, T., & Turnbull, B. (2026). Prioritising Mission Survivability through Defensive Cyber Operations: A Unified Mission Assurance Approach. *Contemporary Issues in Air and Space Power*, *4*(1), BP55879751. https://doi.org/10.58930/BP55879751

Other Operating Domains (Maritime, Land, Cyber)

Prioritising Mission Survivability Through Defensive Cyber Operations: A Unified Mission Assurance Approach

Theresa Sobb[1,2], Benjamin Turnbull[1]

[1] University of New South Wales, [2] Australian Defence Force

Keywords: Cyber, Mission Assurance, Survivability

https://doi.org/10.58930/BP55879751

Vol. 4, Issue 1, 2026

Air missions are reliant on interconnected subsystems comprised of cyber, physical and human components. A breakdown in, or loss of, a component that delivers a mission essential service will have flow-on effects to operational lethality and survivability. In the cyber domain, taking a mission-centric approach to defending infrastructure instead of a traditional system-centric approach is called 'mission assurance'. Cyber operations for mission assurance purposes focus on protecting critical mission services instead of simply securing cyber infrastructure. This work offers a novel approach to mission assurance in the form of a Unified Mission Assurance (UMA) framework. This framework simplifies the mission assurance process into a four-phase operation that can be applied cyclically over enduring operations to ensure that systemic resilience is improved over time. The model is described in detail and then applied to an emergency response scenario use case. Future work is detailed and the impact that the UMA framework can provide to build systemic resilience against emergent phenomena is discussed.

1. Introduction

Cyber services underpin critical aspects across the modern battlefield, with their effects transcending into the air domain. Communications systems, navigation, command and control, and weapons systems all rely on cyber to deliver mission outcomes. Subsequently, a precision-targeted strike within the cyber domain can have devastating kinetic consequences, sending ripple effects across wider military campaigns. Cyber systems exist to meet an articulated service need within an organisation. Within a military context, that service need translates to capabilities that achieve missions, and so effective cyber assurance is a pathway to 'mission assurance'. This term was first defined by the United States (US) Air Force, as the 'process to protect … the continued function and resilience of capabilities and assets … critical to the execution of DoD mission-essential functions' (U.S. Air Force, 2019, p. 9). This approach brings a mindset shift away from system-centric forms of thinking where protection of cyber resources is seen as the main goal, into a mission-centric form of thinking where protection of cyber-infrastructure is seen as a means to an end to achieve ultimate mission success. In this mindset, operations with mission assurance are capable of mission success even in the presence of cyber-attacks, and do not simply aim to prevent them (Bigelow, 2017). This approach to cyber security is especially applicable in sectors that undergo enduring essential operations, such as military missions, financial sectors, government and national critical infrastructure.

Mission assurance is related to, but distinct from, the concept of cyber-worthiness. Cyber-worthiness, as used in Australian Defence, ensures a system, platform or network can continue operating effectively in a hostile, degraded or contested cyber space environment (Coyle, 2021). Whilst cyber-worthiness also incorporates complex systems, cyber and security, in practice it takes a more 'cybernetics' approach, of which cyber security is only one factor. Cyber-worthiness is achieved by using a Test and Evaluation (T&E) approach for a system's goals, identifying threats, vulnerabilities and associated risks, and implementing security controls for these (Boswell et al., 2021). These processes are analogous to other cyber security risk management frameworks, with an emphasis on system goals. However, criticisms of cyber-worthiness note that there are limitations in the processes, noting the need for ongoing adaptability in systems that are largely static in response to changing environments, and the tension between compliance and security (Shahzad et al., 2024).

Cyber-worthiness is distinct from mission assurance because it is based in purposeful engineering design and a focus on the delivery of cyber products to end users that meet their requirements. This is different to mission assurance, which takes a temporal, agile approach to defending cyber terrain in response to mission priorities. The two terms are not mutually exclusive. Instead, a system that is cyber-worthy – that is, able to maintain its cyber functions in its operating environment – is better positioned for the delivery of mission assurance. In simple terms, defending a system that was built poorly is significantly more difficult than defending one that is pre-fortified and fit-for-purpose. Cyber-worthiness ensures the design of secure, ready and compliant systems; whereas mission assurance is an applied approach to ensure the delivery of critical mission outcomes.

This paper presents a novel Unified Mission Assurance (UMA) framework that can cyclically be applied across mission sets to improve their resilience against threats. This is consistent both with advances in international cyber-resilience research and also with cyber-worthiness paradigms used in Australian Defence.

The remainder of this paper is structured as follows. Section two describes the background and identifies the research gap. Section three introduces and explains the UMA framework, including each of its phases. Section four provides an in-depth case study of the UMA, where it is applied to an emergency response scenario. Finally, section five discusses future work and provides conclusions.

2. Background

The US Air Force created the concept of Mission Assurance out of the requirement to maintain mission essential functions regardless of periods of potential degradation, attack or outage (U.S. Air Force, 2019). They define it as the 'process to protect … the continued function and resilience of capabilities and assets … critical to the execution of DoD mission essential functions' (U.S. Air Force, 2019, pp. 2, 9). Effective mission assurance through the cyber domain requires the ability to assess cyber security events and their corresponding impact within the mission environment (Rheaume, 2019). Core to mission assurance are the concepts that a portion of all systems are compromised in integrity, confidentiality or availability and that, despite this, mission needs are paramount. This necessitates responses in cyber defence processes to ensure that mission success and/or survivability are not compromised. Within NASA, mission assurance integrates with the domains of hardware quality, software quality, cyber security, reliability, safety and electronic parts (Brace, 2005; Wilf, 2023). In this way, mission assurance involves consideration of the wider ecosystem that justifies cyber security.

Methods for mission and asset dependency mapping is a significant research area within the literature for mission assurance, as it is used as a prerequisite to determine which cyber assets correlate to mission outcomes. Prioritisation of Mission Essential Functions (MEFs) and decomposing them into sub-functions that cyber capabilities support is one method through which this mapping can occur (Jabbour & Muccio, 2011). Dependency graphs or trees were used as the basis for some methods, whilst others explored the feasibility of ontological applications (Buchanan et al., 2012; Cam & Mouallem, 2013). There are several challenges to mission mapping ventures, including that the defence departments only own a fraction of information infrastructure on which national security missions depend, and bottom-up mission mapping misses critical infrastructure that is outside of defence control (Jabbour & Muccio, 2013).

Determining the risk and impact to mission is a core component of the mission assurance process and is a significant research area within the literature. In one study, mission assurance levels were determined using binary or multi-valued logic decision diagrams, with the security status of cyber assets determined via Petri net modelling (Cam & Mouallem, 2013). From these outputs, it described a risk management scheme to assist decision-makers with real-time mission assurance decisions (Cam & Mouallem, 2013). Another framework for mission risk management consists of a four-pronged breakdown of cost benefit analysis where the economic goals are to spend as little on mission assurance as possible, whilst minimising the cost of failure, increasing the cost to an adversary and lowering the adversary's return-on-investment (Jabbour & Muccio, 2013). Tools specifically made to meet defence force needs are also available, with the Cyber Evaluation and Management Toolkit offering a method for cyber security risk evaluations for complex cyber-physical systems (Fowler et al., 2024). Whilst these processes are useful for understanding risk thresholds within tolerance levels, they are primarily compliance-based and consider business impact instead of temporal mission impact.

Several frameworks are also introduced within the literature as methods to approach and apply mission assurance processes. Cyber-ARGUS is one such framework that contains a three-phase approach of mission design analysis, collection of mission and cyber data, and assessment of mission impact (Barreto & Costa, 2019). This approach incorporates an understanding of mission characteristics, vulnerability discovery and enemy behaviour modelling as part of its analysis in order to develop relevant assessments that calculate the combined effects produced by attacker and defender plans (Barreto & Costa, 2019). Alternatively, Jabbour and Muccio present a five stage mission assurance process that incorporates MEF prioritisation, mission mapping, vulnerability assessments, mitigation and red teaming (Jabbour & Muccio, 2011). This approach prioritises stopgap measures to assure systems in a contested cyber environment, where systems may already be compromised. A Cyber Preparedness framework is also offered in the literature as a way to characterise cyber threats, determine the level of preparedness needed to ensure mission success, set objectives and establish decision priorities (Bodeau et al., 2010).

Tactical applications for mission assurance are also discussed in the public domain literature, including methods for implementing mission assurance behaviours at the practitioner level. Proactive techniques such as network segmentation and moving target instrumentation, and reactive techniques including deception strategies, are methods that modify the attack surface and impose cost on the adversary (H. Goldman et al., 2011). Building resiliency through specified objectives is also examined, with different actions chosen to reflect temporal mission assurance priorities including protection, deterrence, detection, isolation, recovery and adaptation (H. G. Goldman, 2010). The nature of the objective most suitable to a system will be shaped by the system's environmental context, with factors such as mission criticality, time and threat influencing the appropriate outcome. For example, as protect scenarios improve the defence of systems and disincentivise malicious actors, they are resource intensive and are therefore most suitable to high-value systems that exist to complete a specific temporal mission. Command and control systems, census collection and electronic election voting platforms are

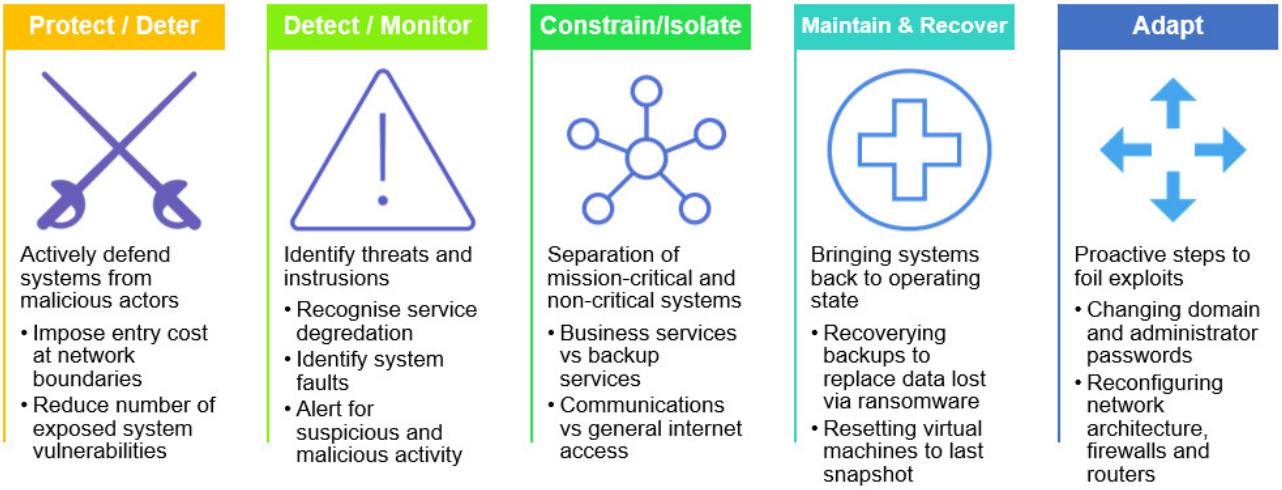

Figure 1. Applied examples of different objectives for resilient architecture. Adapted from H. G. Goldman (2010) .

all examples of systems that would be suited to a protection mission assurance objective. Conversely, a monitor approach consists of the deployment of sensors to collect information over long periods and is therefore more suited to systems requiring ongoing assurance. Examples of such systems include logistics platforms, air traffic control and business datacentres. Figure 1 demonstrates different applied methodology techniques for each objective.

Existing research relating to mission assurance broadly falls into the categories of defining and expanding the term, mission mapping methodologies, risk and mission impact assessments, frameworks and models, and tactical applications. Typically, this research base looks at the nature of mission assurance and applying it to specific operational scenarios. The current literature lacks a holistic approach to mission assurance that can be applied at an operational level, and implemented cyclically through agile development methods to improve resiliency steadily over time. Mission assurance needs to be integrated into existing project management and development paradigms at all stages of mission planning and operation. This is extremely important for critical enduring organisations, such as military forces and national critical infrastructure, where cyber threats may remain persistent and consistent. For the missions of such organisations to be assured, temporal tactical mission assurance is not enough, and there is a requirement for long-term shock absorption and resiliency.

3. Unified Mission Assurance

Organisations require the sustainment of operational capability and delivery of effects over extended periods, where environmental circumstances require agility and adaption. As cyber is a critical underpinning capability of mission effects, providing a methodology to sustain mission assurance efforts within this context is critical to operational needs. This paper presents a new framework for mission assurance that leverages developments from the literature and fills the need for a long-term cyclic option for mission sustainability in complex adaptive environments. Its strength comes from defining the parameters in which previous and future mission assurance research can be applied, whilst also addressing the critical research needed to offer mission assurance solutions that are both long term and adaptable. UMA is a whole-of-life continuous defence framework that can be applied across mission sets to increase their resiliency to cyber threats and enhance overall mission survivability. The framework is designed to be scalable; and can be applied to a single mission thread or a larger mission set. The UMA framework has been specifically developed for organisations that have critical business and mission outcomes that must be sustained over extended periods, where traditional short-term temporal mission assurance approaches are less appropriate. The UMA approach is therefore a novel model that can be used to enhance the defensive cyber posture of essential service organisations including defence forces, financial institutions and national critical infrastructure such as power grids and water. It takes a mission-first multi-domain approach to cyber defence that serves to adapt security measures as environments change in order to maximise mission assurance effects.

The UMA is a cyclic model with four key phases, as shown in Figure 2. Each phase has a specifically defined purpose, method and end-state that contributes to the mission assurance effects for that defined mission. The phases can be delineated based on whether they are administrative or cyber-based tasks, and whether they are conducted in a mission-ready posture or a post-mission posture, as illustrated in Table 1. As the model is cyclic, UMA is something that is a constant goal. Whilst individual temporal missions may change, the overall process to assure those missions strategically maintains the priority. It extends beyond tactical defensive actions during mission-execution periods and encompasses proactive protective activity across the entire mission lifecycle. Through UMA, cyber architecture is secured, mission services are protected, and therefore mission capabilities become more survivable due to the continuous cyclic nature of the model.

Figure 2. Unified Mission Assurance (UMA) framework.

The UMA framework differs from traditional cyber worthiness, mission assurance and vulnerability assessments. The variance in the nature of these methodologies is highlighted in **Table 2**, with the UMA framework notably being the most adaptable, mission-focussed framework that evaluates security outcomes over the whole system lifecycle.

The **Mission-centric Analysis** phase refers to the process of synthesising and overlaying mission, threat and infrastructure relevant information. The format of mission-centric analysis is heavily informed by previous mission assurance models such as cyber-ARGUS (Barreto & Costa, 2019). Mission-centric analysis also involves the active mapping of cyber infrastructure to mission essential functions, generating identifiable mission links that must be protected (Jabbour & Muccio, 2011). This is explained visually in Figure 3.

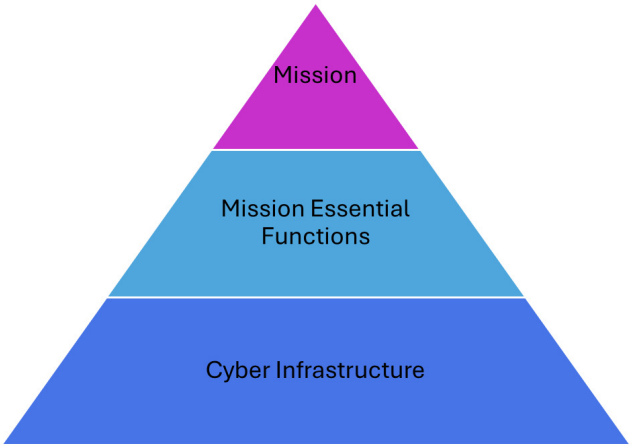

Figure 3. Visual representation of mission mapping hierarchy.

The **Applied Environments** phase refers to events in which mission assurance activities or actions are taken on a network. These may include, but are not limited to, real-world mission assurance tasks on operation, exercises, simulations, digital twins and other forms of testbed environments. In essence, these spaces allow for conditions through which mission assurance principles can be planned, tested and executed.

Table 1. Unified Mission Assurance phase delineators.

	Administrative Task	Cyber Task	Mission-Ready	Post-Mission
1. Mission-centric Analysis	X		X	
2. Applied Environments		X	X	
3. Employed Lessons	X			X
4. Resilient Infrastructure		X		X

Table 2. Framework comparison.

	Applicable across whole of system lifecycle	Unforeseen and multiple mission set adaptability	Focuses on mission over system compliance	Tests and evaluates security components
Unified Mission Assurance	X	X	X	X
Traditional Mission Assurance		X	X	X
Cyber Worthiness				X
Vulnerability Assessments				X

The **Employed Lessons** phase refers to the taking of lessons identified out of the Applied Environments phase, and inputting them into policy, business continuity planning, procedures and capability acquisition to increase resiliency for the future. This phase may include bureaucratic ventures or may initiate projects to address fundamental flaws identified throughout the mission assurance process.

The **Resilient Infrastructure** phase involves the implementation of actions and changes to the cyber system to increase its resiliency. This could involve actions designed to minimise the effects of disruptive adversary action or outages on the system affecting the overall mission, security uplifts based on vulnerability assessments, diverse network reconfigurations or the implementation of pre-emptive deception plans (H. Goldman et al., 2011).

4. Technical case study

In this section, the UMA approach will be applied to an Emergency Management Centre (EMC) scenario. This scenario was chosen because it is representative of a typical dual civilian or military service, with parallels to other use cases including logistics hubs, command and control centres, and airfield operations. Each phase of the UMA will be cycled through, illustrating the depth and scope of considerations required as part of the analysis process. As the UMA process is one of continuous improvement, this worked example will show the first iteration only.

4.1. Scenario background

An EMC requires 24-hour operations. EMCs are responsible for a variety of tasks including emergency call taking, emergency vehicle dispatch, emergency response management and emergency evacuation support. The service packages for the EMC are sourced from the National ITS Reference Architecture (Office of the Assistant Secretary for Research and Technology (OST-R), 2025).

In this scenario, this specific EMC has been identified as a critical service provider and requires cyber security support to ensure that its services remain online and available. Other critical service providers including the local hospital and Red Cross have experienced cyber-attacks over the last week, and authorities are concerned that the EMC may be a potential target.

It is important to note that approximately 30% of the employees work from home, relying on Remote Desktop Protocol (RDP) and Microsoft Teams to work.

The network architecture of the EMC consists of five subnets (**Appendix 1)**. The Servers subnet contains the domain controller, file server, mail server and web server. The Administration subnet is used by the EMC network administrators to manage the wider network, using RDP to manage hosts. The Call Centre subnet receives emergency calls. The Emergency Response subnet manages emergency events. Finally, the Management subnet contains the EMC's chain of command.

The typical workflow of an emergency starts with an emergency call coming into the Call Centre via VOIP over the internet. The Emergency Response group manages the event tickets within wider incidents and coordinates the dispatch and liaison with other external to EMC entities. These may include other emergency response services such as air-medical transport, the fire brigade, hospitals and police force. They are the central liaison between these services. The Management group monitors operations and closes incident tickets if required.

The file server contains the incident records for the EMC, both current and historic. They are kept in a Microsoft Access database. Entries are organised by date, incident call time and incident ID. The records include data from emergency services, call logs, recordings and images.

The webserver hosts updates on current emergency information that is pertinent to the public. This includes significant weather events, road warnings and national disaster information. It relies on external API feeds to third party government and commercial systems

4.2. Mission-centric analysis

Upon being given the task to provide mission assurance to the EMC, the first step as part of the UMA process is to conduct mission-centric analysis. In this step, task, threat, infrastructure and options will be analysed to develop a comprehensive plan for securing the network.

Task analysis. Within task analysis, an understanding of the expected outcomes and success factors is required within the context of the mission. The EMC is a critical service, providing a point of contact for people in dangerous situation and connecting them with emergency services.

The EMC's mission can be broken down into four mission essential functions:

- MEF 1. To receive emergency calls from the community
- MEF 2. To liaise with emergency services over the phone and internet
- MEF 3. To track and manage emergency incidents
- MEF 4. To provide emergency information to the community via the EMC website

The EMC's MEFs are time sensitive and crucial. Thus, maintaining each is critical to achieving overall mission success.

Threat analysis. The last six months has seen a general uptake in general botnet attacks against the internet-facing firewall of the EMC domain. There have been no reported incidents.

There have been previous financially motivated cyber-attacks on similar critical service providers including two local hospitals and the Red Cross. One of these attacks was attributed to the actor Exotic Lily, a ransomware group that uses software including Diavol and Conti (Taylor, 2022). APTs with the capability and intent to attack a critical public service such as the EMC include APT41 and the Lazarus Group (Htet & Rostovcev, 2019; 2025a).

Across these three APTs, a selection of tools, techniques and procedures (TTPs) are used to progress through the kill chain to achieve their actions-on-objectives. **Appendix 2** shows a selection of techniques that the actors use for different phases of their operations. The most common TTPs

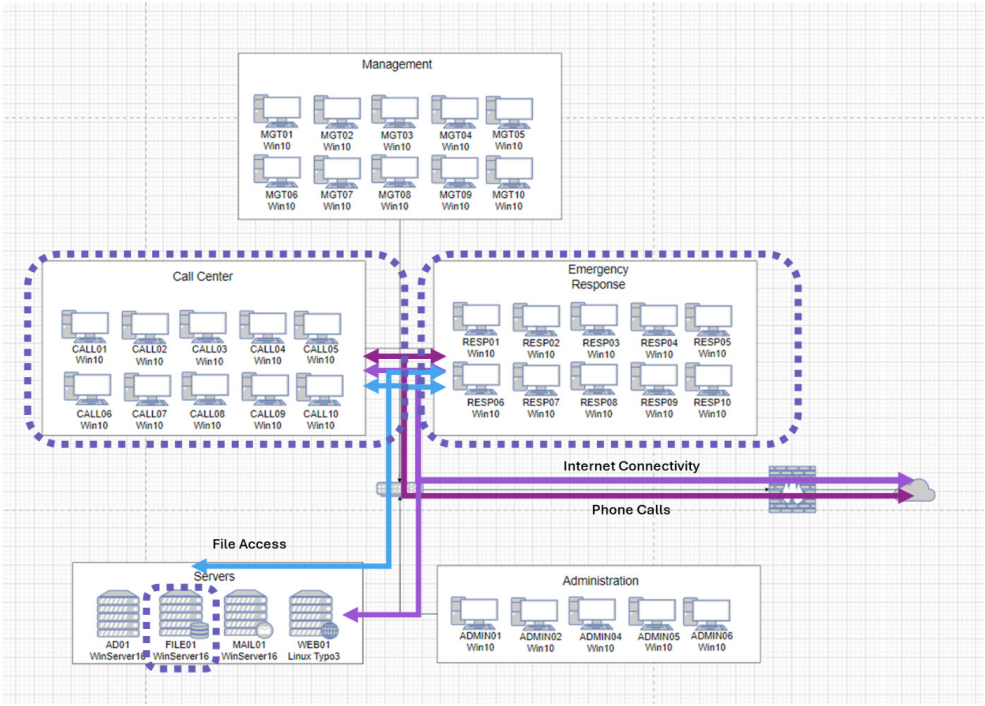

Figure 4. Emergency Management Centre critical mission infrastructure overlay.

to note as part of the threat analysis have been determined through a MITRE overlay of the three identified most likely threat actors. **Appendix 3** describes the most likely TTPs to be used by the identified threats by phase.

In the **infrastructure analysis** step, the cyber terrain of EMC is analysed to determine its defensive characteristics and capabilities. Firstly, the cyber-critical components within the network must be identified. These are the elements of the network that are essential to the maintenance of standard network service operations, agnostic of mission or task.

Appendix 4 shows the critical cyber overlay of the terrain. The domain controller hosts the active directory and the DNS for the domain and is therefore critical to enabling the management of the EMC network. This includes services such as user logins and computer management. The Administration subnet is critical cyber terrain because it is through this subnet that the network administrators can maintain, administer and control requisite network functions. The central router is critical terrain because it is the central point through which all traffic in the network must route. Finally, the firewall is cyber-critical terrain because it serves an essential cyber-security function of limiting external access to the domain.

Next, the mission essential functions (MEFs) are considered analysed and overlaid over the cyber terrain, to determine any mission-critical infrastructure. **Figure 4** shows the output of this analysis. Each MEF that was derived as part of the task analysis must now be applied to the infrastructure analysis (**Table 3**). By considering the cyber and mission-critical terrain, there is now a firm understanding of what portions of the EMC network infrastructure must be prioritised to maximise mission assurance outcomes.

Within the **option analysis**, a series of sequences are devised, tested and validated as potential courses of action to support the EMC's mission assurance outcomes whilst still maintaining the cyber priorities. Three options are developed that represent different approaches to achieving the mission assurance objectives of the EMC, as shown by **Figure 5**. They each achieve the same set of cyber priorities, such as having a map of network architecture up to network boundaries and having an up-to-date network architecture; however, they implement different sets of methodologies to meet these ends. When considering each option, it must be evaluated in terms of its suitability, feasibility and appropriateness to the current task and mission.

Option 1 is heavily focussed on improving the security standing of the network before transitioning to an active defence posture. It prioritises actions that gain the greatest visibility of the cyber terrain and in particular the current vulnerabilities that the network has. Follow-on actions focus on hardening the cyber terrain and reducing the potential attack surface that a potential threat has available to them. This style of approach has the benefit of hardening any potential vulnerabilities upfront but comes at the cost of potential downtimes and outages, and equipment is taken offline to enable reconfigurations and updates. This approach also provides the least current threat-visibility. It is highly system and engineering focussed, with limited actions implemented to monitor for and respond to potential malicious actors on the network. It is therefore more suited to missions that require a 'system-uplift' style approach, where the risk of an adversary infiltration is low.

Option 2 takes a more active defence approach that prioritises methodologies that have the least impact on EMC services. For threat visibility, it utilises passive and native methods of data collection that do not require the instal-

Table 3. Mission essential functions infrastructure analysis.

Mission Essential Function	Infrastructure Analysis
MEF 1. To receive emergency calls from the community	Call Centre hosts must be available and able to receive phone calls over VOIP
MEF 2. To liaise with emergency services over the phone and internet	Emergency Response hosts must be able to connect out of the EMC network to emergency services, via VOIP or the web
MEF 3. To track and manage emergency incidents	Both the Call Centre hosts and the Emergency Response hosts must be able to access the incident database hosted on the file server
MEF 4. To provide emergency information to the community via the EMC website	Hosts within the Call Centre and Emergency Response subnet should be able to access and edit files on the webserver, and external-to-EMC internet users should be able to view and access an up-to-date version of the EMC's website

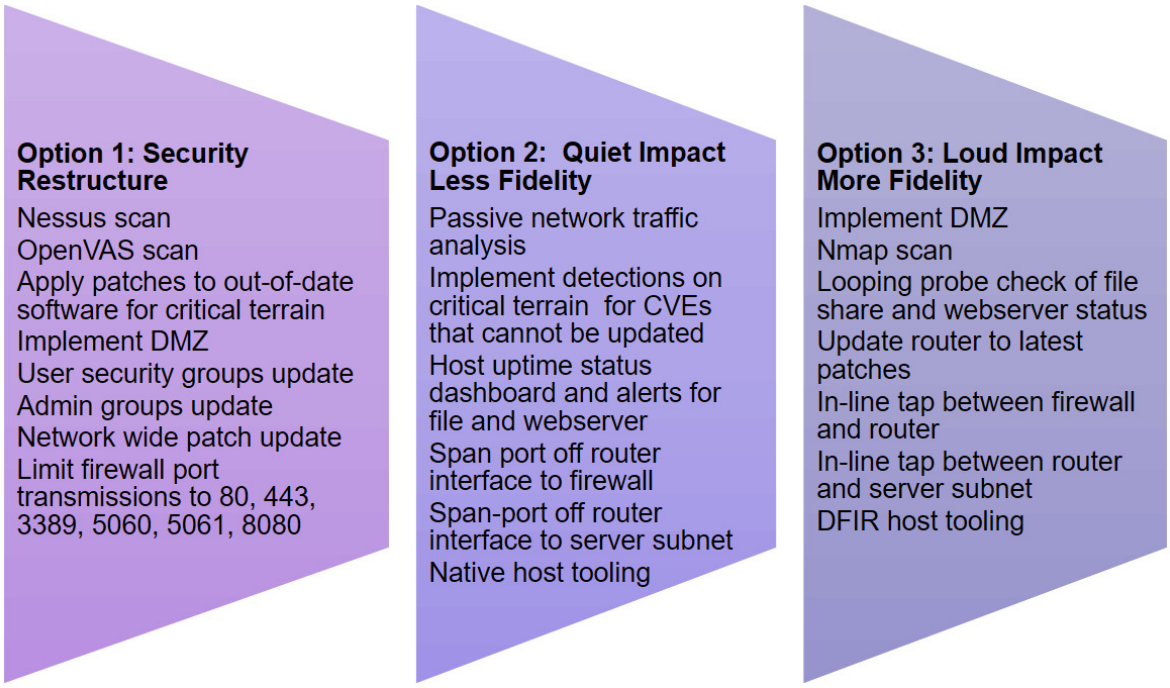

Figure 5. Options for EMC Mission Assurance Approach.

lation of additional tools to the EMC network, reducing the number of disruptions made to the EMC system. The approach still hardens vulnerabilities but prioritises those which pose the greatest mission risk rather than bulk updating all services and causing large downtimes. This is beneficial because it causes the least service disruption to the EMC but comes at the cost of compromising speed and fidelity in tooling for the cyber security team.

Finally, option 3 takes a more direct approach that prioritises active defence measures regardless of service impact. This includes installing software onto computers on the network and physical network taps to collect data. Activities to check and monitor the network are noisy, meaning that a potential threat actor would likely identify defensive actions occurring on the systems. There are clear benefits from a cyber security perspective in terms of freedom of tooling and visibility, but this comes at the cost of EMC service impacts through the installation and running of these additional tools.

Table 4 shows a summary of each option and the comparative factors for consideration. Considering that the team has been brought in specifically because of a concerned threat targeting the EMC, Option 1's *low* threat visibility makes it an unsuitable candidate for this assignment. Due to the criticality of the EMC's services, its MEFs impact to system is prioritised over other factors, disqualifying Option 3's *high* impact to system. Therefore Option 2 presents the best balance of methods to achieve mission assurance outcomes in the EMC environment given the priorities and constraints.

4.3. Applied environments

Temporal scenario. Execution of the EMC mission assurance plan occurs as part of the Applied Environments phase. The applied environment for this scenario is a real-world execution environment.

The phase begins with the configuration and implementation of host and network collection tooling, followed by

Table 4. Option analysis summary.

	Network Hardening	Threat Visibility	Noise Level	Impact to System
Option 1	High	Low	High	High
Option 2	Medium	Medium	Low	Medium
Option 3	Medium	High	High	High

their validation. The cyber team can then follow through with the methods described in the option developed as part of the mission-centric analysis.

In this hypothetical scenario, during the execution period, the cyber team is made aware that an unauthorised user is using John Dorian's administrator account. Based on initial triage, it is identified that that administrator account has logged into the domain controller (AD01), one of the cyber-critical hosts. A persistence sweep of the network identifies two outlier registry keys that do not conform with the rest of the domain's configuration (**Appendix 5**).

John Dorian's administrator account is logged in to the domain controller via remote desktop protocol from a suspicious IP address. That same suspicious IP address is also connected to a computer in the Call Centre, CALL06, and a computer in the Emergency Response subnet, RESP10. This second computer is the same host that has the outlier registry key.

Triage across these three hosts identifies process injection into the runtimebroker process on the domain controller, and the Microsoft Edge process on the other two hosts. This is enough data to transition the category of this incident from anomalous to malicious.

Framing mission risk in a mission assurance approach. In the current state, an actor has compromised three machines, including one that is critical to the EMC network functioning, and has active command and control from each of them. They also have at least one administrator password, and have employed mechanisms on each machine that will re-spawn their access if they are cleared from the network. The assessed risk to EMC operations is high.

Because this is a mission assurance task, maintaining the four EMC mission- essential functions is the priority. The current network adversary poses a direct threat to those mission essential functions, through their potential disruption, denial or further exploitation of the network. It is therefore a mission assurance imperative to stop the adversary's kill chain progressing.

Unfortunately, conducting a traditional incident response where the three infected hosts are taken offline for slow time forensics is not an option because this will also stop critical mission essential functions. This network does not have a back-up secondary domain controller, which is critical for the network to function, and the other two infected hosts are currently being used to manage real-time emergency incidents and cannot be taken offline.

Temporal scenario update. The system administrators update that the RYUK ransomware has been deployed on the Administration subnet, with all files being encrypted control being lost of each host (Haase, 2022). A quick-response survey of the rest of the network identifies that the domain controller has a mounted network share with the Administration subnet. A new share is seen opening between the same domain controller and the file server and main server. At the same time, the infected host in the Call Centre mounts a network share with five computers in the management subnet. **Appendix 6** shows a summary of the intrusion set.

Mission-prioritised eradication. The assurance of the delivery of the EMC's mission essential functions is the utmost priority of the cyber team. This intrusion set poses a direct threat to this mission, with a mission risk of extreme. The actor has demonstrated the capability to deploy ransomware and, by opening the shares to the file and web server, is demonstrating the intent to deploy it to these critical EMC services.

Stopping the ransomware deployment and then eradicating the threat actor is a priority over all other cyber security or forensics ventures. The first action of the cyber defence team is to stop the ransomware deployment on the servers, as this poses the largest risk to the EMC's mission essential functions by including the mission-critical file and web server. This is done by dropping the remote desktop session to the domain controller and stopping the injected threat on that computer. The second action would be to stop the Management subnet ransomware deployment, which occurs second because this subnet is not critical infrastructure. This is done by stopping the injected threat in Microsoft Edge on the infected Call Centre computer. Next, the priority is to remove any mechanisms enabling persistent access to the network and to stop all other forms of in-memory execution. This is to stop the adversary from re-spawning their tools once cleared from the network and removing any current footholds they have. This is completed by deleting the two registry keys identified in **Appendix 5**, and then stopping the process injection in Microsoft Edge on the compromised Emergency Response computer. After validating these initial steps, the network is monitored immediately for the malicious IP address to see if it is logged again within the EMC, which would indicate that a foothold was missed.

Post-eradication actions. This approach prioritises mission needs over security needs. Once the initial threat has passed and it is confirmed that the actor has been eradicated, then post-eradication security actions can be taken in the network. These include the resetting of compromised credentials, including John Dorian's administrator account, the administration of digital forensics to understand the nature of the historic compromise and to feed the intelligence cycle, and the resetting of the network back to its original configuration.

The forensic analysis of the EMC network paints a narrative of the entire intrusion set, from initial entry to actions on objectives. A summary of the forensic outcomes identified in this analysis is presented in **Appendix 7**.

Considering the most likely threat TTPs discussed in the Threat Analysis phase, several corresponded with actions conducted by the adversary on this operation. The overlap between behaviours observed in the scenario and those predicted in the threat analysis are detailed in **Appendix 8**.

From the indicators of compromise (IOCs) identified as part of the post-incident forensic analysis, it is identified that the TTPs aligned with those associated with the malicious cyber actor Wizard Spider (Haase, 2022; Millington & Gayda, 2025). Whilst this was not one of the threat actors specifically named in the threat analysis, Wizard Spider is closely linked to Exotic Lily, which was identified as a likely threat actor to the EMC (Taylor, 2022).

4.4. Employed lessons

Post-incident analysis and forensics, there are several lessons identified that can be taken and applied to EMC's governance, management and procedures.

Whilst working on the network, it was identified that there was no data backup policy pertaining to the file server, which contained information critical to current and historical emergency incidents. This posed risks to the network, as the potential corruption, exploitation or loss of service of the file server would leave the network with no alternative service solution. An administrative solution to this problem would be the implementation of a routine backup policy, enshrined within the system's designated operating procedures. This would assist in minimising the effects of future ransomware attacks (Thomas & Galligher, 2018).

Across the wider network, it was noted that the EMC system administrators did not have a broader recovery or contingency plan for incident response or for when infrastructure experienced outages. Such plans are critical for assigning responsibility, streamlining tasks and delegating authorities in crisis situations; without which the network is left at an increased risk of prolonged service disruption. It is recommended that the EMC system administrators establish both an incident response plan and disaster management procedures in order to enable business continuity planning between critical service interdependencies (Fisher et al., 2017). Such plans should include business risk management, security, technological and psychological considerations, and continuous improvement processes that harness learning and adaptation over time (Savolainen et al., 2024).

As revealed during the post-incident forensics, an Outlook scraper was successfully used to acquire the credentials for one of the EMC's users, Courtney Stones. This occurred because a password reset email had been sent to her that had stored her new password credentials in plain text. To administratively address this to reduce the risk of such an event happening again, password reset policies should be updated to ensure that password resets send each half of the new credential in a separate email to the member and their supervisor respectively. This reduces the risk of identifying both halves of the password together with a scraping tool.

Through the implementation of these administrative lessons into policy, governance and procedures, EMC will be able to mitigate the risks associated with an incident such as those experienced in this case. Importantly, paper-based implementations must be followed through with cognisant cultural acceptance and technique application for them to be truly onboarded successfully. This takes both organisational and individual accountability, active change management and dedication (Ramluckan et al., 2020; Watson et al., 2020) .

4.5. Resilient infrastructure

In this section, changes to the engineering baseline of the EMC network are discussed. Some of these relate specifically to stopping an actor like the one seen in the historical intrusion set from repeating their attack, whilst others are more general. These changes are designed specifically to protect critical services, assure mission essential functions, and build the network's overall resilience to attacks, outages and disruptions. **Appendix 9** summarises key infrastructural improvements to be made based on observations from the intrusion.

Through the implementation of these hardware and software recommendations, the Resilient Infrastructure phase is completed. This concludes the first cycle of the UMA framework. From here, cyber defenders are positioned for future iterations based on upcoming tasks or system needs. These may be in operationally live, exercise, simulated or test environments, depending on the mission context. Finalising this phase brings to conclusion the first cycle of the UMA process. From here, a new iteration can occur, that can encompass and adapt to new and changing needs in the system, mission and threat environment.

5. Building mission resilience

Critical mission services, whether in a military or industrial context, must be able to deliver outcomes throughout turbulent and adverse conditions. It is the resilience of these systems that informs their parent mission's ultimate survivability. In this section, critical elements enabling resilience will be discussed in the context of the UMA framework to inform mission assurance applications.

Adaptability enables change in response to new environments and situations. It is essential for resilience because a system that cannot adapt to new stimuli becomes vulnerable and not fit-for-purpose. The UMA approach is designed to be adaptable through its iterative cyclic design. Each cycle allows for temporal changes, such as new environmental data, mission updates and architecture modifications, to be encompassed within the upcoming loop. This continuous cycle forces cyber security updates to be made, regardless of how much the environment has changed, leading to greater continuous improvement outcomes overall. From a resilience perspective, the benefits are two-fold. First, legacy systems that have been in a state of inertia are

forced into resilience-improving cycles. And second, agile systems or missions with changing variables and environments can be suitably accommodated for at each variation.

Scalability enables the effective absorption of increased demand or expansion of work without the compromise of performance. In rapidly changing environments, services must be able to shift in scale to meet demands. The UMA is built with this in mind. It is not bound to a particular scope, be that the boundary of a computer system or a particular mission-set. It is scalable, able to be applied across the tactical, operational and strategic levels of organisations. This enhances its adaptability, so that it can be implemented in sectors where it is most needed regardless of scale of mission set or cyber infrastructure. Through this scalability, a wider range of systems can be encompassed by UMA, making it a resilience enhancing asset for organisations.

Sustainability refers to the ability to maintain a service over an extended period. It is a key feeding factor to resilience, as systems, services or missions that cannot be sustained or are stretched 'too-thin' become weaker and are less able to react to and absorb turbulent events. UMA builds sustainability by directly bolstering both the procedural and technical cyber defensive measures of a system. A system that is better secured, tested and robust will be more able to sustain services when under attack than one that is not. Human, physical and cyber domain factors all contribute to building sustainable systems that feed mission essential services. This sustainability feeds resilience against outages, attacks and emergent events.

Survivability is directly related to resilience. If resilience is the ability to absorb and 'bounce back' from adversity, then survivability is the ability to continue to exist, function and deliver outcomes regardless of damage received. UMA is designed explicitly to ensure that cyber systems are better equipped to assure the success of missions. This cannot happen if the cyber infrastructure or services are not survivable. Each stage of the UMA framework takes a different action towards the improvement of system survivability. Together, the entire UMA cycle advances system survivability, which in turn strengthens service resilience, and conclusively assures the ultimate mission.

6. Lessons for the Australian Defence Force

There is some existing ADF literature regarding the application and development of cyber warfare capabilities that can inform how approaches such as UMA can best align with ADF objectives and requirements. These documents assist in illustrating the problem space in which solutions like UMA may be applied.

First and foremost, the cyber must be recognised and applied as capabilities that integrate and extend across the other physical domains of space, air, maritime and land. The ADF's Capstone doctrine, Australian Military Power, supports this idea (Australian Defence Force, 2024). What this effectively means is that the ADF recognises the independence of cyber as its own domain, whilst simultaneously accepting its embedding and influence across the physical domains. Acknowledging the nature of this causal relationship is the first step in taking proactive cyber action that assures military action across all domains, that is, mission assurance.

In 2024, the 2024 National Defence Strategy was released as a guide for the delivery and transformation of the Australian Defence Force (ADF) into an integrated, focused force (Australian Government, 2024). The document specifically highlights that cyber's capability priority for the force is to 'strengthen situational awareness, the ability to project force and decision advantage' (Australian Government, 2024, p. 38). Doctrinally, it is established that the cyber domain itself is integrated across and through the other warfighting domains, making it a key enabler (Australian Defence Force, 2024, pp. 33–34).

Applying the UMA framework, especially due to its cyclic and phased nature, gives the opportunity to encompass the range of cyberspace mission sets across the system lifecycle. It enables the achievement of both building inherent resilience and denying adversary temporal advantage within a single procedure that can be applied at scale across the organisation. UMA's cyclic model allows for continuous and adaptive learning, collaboration and objective optimisation across all mission stakeholders; breaking it free of the temporal limitations of traditional defensive mission assurance and the other siloed cyberspace mission sets.

Finally, the impacts of applying UMA in the context of the Defence Cyber Security Strategy is considered (Department of Defence, 2022). This document was released before the NDS but still contains much of the principles and direction that guide cyber security activities in the military domain to this day. The five principles that guide the Strategic Vision of the strategy are mission-focussed, threat-centric, contemporary, best-practice and strong partnerships. Whilst the UMA framework is a new model to Defence, it fulfils each of these principles, strengthening cyber outcomes. The UMA framework is inherently *mission-focussed*, with mission assurance being at the core of the model's design. This innately links in with *threat-centric*, with temporal proactive threat analysis applied to mission scenarios that give operators the most up-to-date intelligence. UMA is not only *contemporary* in terms of its newness as a model, but also is inherently designed to integrate new, cutting edge and evolutionary technologies into each revolution of its life cycle, making it system agile. UMA also aligns with existing *best-practice* models, with the seamless integration of governance, standards and cyclic assessments of systems to continuously evaluate and uphold existing and future requirements. Finally, the nature of UMA encourages *strong partnerships* through the integration of different cyber subject matter experts towards a common mission-oriented goal. Cyber warfare operators have the opportunity to engage with specialists from the cyber engineering trade, in addition to linking with industry partners. This collaborative approach not only strengthens these individual relationships but has a positive emergent effect on the mission assurance culture as a whole.

Ultimately, these strategic level documents excel at providing principle-based guidance to the explanation and application of capabilities within the cyber domain; under which the UMA framework clearly aligns. They do not how-

ever tangibly and explicitly direct the ways and means to which these cyber outcomes can be achieved, and that is where options such as UMA stand out. UMA is an additional tool in the cyber toolset, adding and expanding beyond existing methodologies such as traditional vulnerability assessments, incident response, hunt and mission assurance. Its benefit is that it is built to be adaptable and encompass any of these tasks within its assurance cycle if required, making it less prescriptive and more descriptive in nature. Whilst it may not suit all mission sets, the UMA model provides a new mission-holistic approach to cyber defence that excels beyond the limitations of existing models and directly aligns with prevailing ADF strategic requirements.

7. Future work and conclusions

Mission systems, national critical infrastructure and essential services have interdependent reliance on cyber systems. To enhance technological innovation and achieve technological advantage for air superiority, Air Force must have mission assurance through the cyber domain. In extended operational circumstances, this mission assurance approach must be scalable, sustainable and adaptable in order to ensure mission survivability in contested environments.

Traditional cyber security approaches prioritise system security, whilst mission assurance approaches instead prioritise the delivery of essential mission services to the parent organisation. Historical research within the mission assurance space has been relatively limited to methodologies to conduct tactical mission assurance and assess organisational risk through this lens. These perspectives are temporal in nature, bounded by mission sets, space and time.

This paper extends and enriches this body of knowledge by presenting a UMA framework, which provides a holistic long-term approach to applying mission assurance principles to systems beyond discrete mission sets. The UMA is designed to be implemented cyclically with adaptive learning attitudes, to enable continual mission assurance over time that prioritises system resilience to emergent phenomena. This makes it well suited for environments where critical operations must be assured continuously, including military forces, financial services, power infrastructure, healthcare and emergency services. The framework builds mission resilience as a fundamental output, which is supported by its adaptability and scalability, and its contributions to sustainability and survivability.

Opportunities for future work within the scope of UMA include building out a comprehensive second-level architecture for each phase of the framework, as this is currently descriptive and not prescriptive. The development of such an architecture would provide more fidelity for mission assurance assessments and would build upon methods previously developed and described in the literature. This would improve the model's reliability across different user implementations based off skill and prerequisite knowledge, building model robustness and fitness for purpose.

Ultimately, the UMA framework offers a novel approach to applying long term mission assurance effects to critical service sectors in order to develop systemic resilience and adaptability over time. It equips defensive cyber teams with a structure through which they can understand the mission priorities they are trying to protect, translate those into cyber protection priorities, apply their defensive actions, and implement change at the policy and cyber infrastructure level. By completing iterations of the UMA cycle over time, service-critical organisations can have increased trust in the robustness and resiliency of their essential services against emergent phenomena, such as outages and cyber-attacks.

From an Air Force perspective, the UMA framework poses an opportunity to scope assurance in the cyber domain beyond tactical tasks, into strategic long-term assurance that is resilient to the turbulence of contested environments. Whilst consistent with Australian cyber-worthiness paradigms, it is also consistent with the broader international processes and provides a more expansive option for mission-focussed cyber operations. It offers an approach to defensive cyber activities that is compatible with commander's intent and delivers effects that prioritise the survivability of air missions above system security. In this way, applying UMA through the cyber domain directly contributes to the strengthening of air power.

Submitted: September 18, 2025 AEST. Accepted: December 05, 2025 AEST. Published: April 15, 2026 AEST.

References

Australian Defence Force. (2024). *ADF-C-0 Australian Military Power Edition 2*. Department of Defence. https://acmc.gov.au/sites/default/files/2024-10/ADF-C-0%20Australian%20Military%20Power-compressed.pdf

Australian Government. (2024). *2024 National Defence Strategy*. Department of Defence. https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program

Barreto, A. B., & Costa, P. C. G. (2019). Cyber-ARGUS – A mission assurance framework. *Journal of Network and Computer Applications*, *133*, 86–108. https://doi.org/10.1016/j.jnca.2019.02.001

Bigelow, B. (2017). *Mission Assurance: Shifting the Focus of Cyber Defence* [Paper presentation]. 2017 9th International Conference on Cyber Conflict (CyCon). https://ccdcoe.org/uploads/2018/10/Art-03-Mission-Assurance-Shifting-the-Focus-of-Cyber-Defence.pdf

Bodeau, D., Graubart, R. D., & Fabius-Greene, J. (2010). *Improving Cyber Security and Mission Assurance Via Cyber Preparedness (Cyber Prep) Levels* [Paper presentation]. 2010 IEEE Second International Conference on Social Computing. https://www.mitre.org/sites/default/files/pdf/09_4656.pdf

Boswell, L., Mooney-Collett, C., & Keane, J. (2021). *Cyber test and evaluation in a maritime context*. Sea Power Centre Australia. https://seapower.navy.gov.au/analysis/cyber-test-and-evaluation-maritime-context

Brace, R. P. (2005). *Mission assurance at the Jet Propulsion Laboratory* [Paper presentation]. Northrop Grumman Mission Assurance Summit. https://ntrs.nasa.gov/citations/20060044292

Buchanan, L., Larkin, M., & D'Amico, A. (2012). *Mission Assurance Proof-of-Concept: Mapping Dependencies among Cyber Assets, Missions, and Users* [Paper presentation]. 2012 IEEE Conference on Technologies for Homeland Security. https://ieeexplore.ieee.org/document/6459865

Cam, H., & Mouallem, P. (2013). Mission assurance policy and risk management in cybersecurity. *Environment Systems and Decisions*, *33*(4), 500–507. https://doi.org/10.1007/s10669-013-9468-z

Coyle, S. (2021). *Australia's Defence and National Security: How Defence is Enhancing Australia's Cyber Resilience*. The Cove. https://cove.army.gov.au/article/australias-defence-and-national-security-how-defence-enhancing-australias-cyber-resilience

Department of Defence. (2022). *Defence Cyber Security Strategy*. Australian Government. https://www.defence.gov.au/about/strategic-planning/defence-cyber-security-strategy

Fisher, R., Norman, M., & Klett, M. (2017). Enhancing infrastructure resilience through business continuity planning. *Journal of Business Continuity & Emergency Planning*, *11*(2), 163–173. https://doi.org/10.69554/XKKQ9269

Fowler, S., Joiner, K., & Ma, S. (2024). Cyber Evaluation and Management Toolkit (CEMT): Face Validity of Model-Based Cybersecurity Decision Making. *Systems*, *12*(7), 238. https://doi.org/10.3390/systems12070238

Goldman, H. G. (2010). *Building Secure, Resilient Architectures for Cyber Mission Assurance*. The MITRE Corporation. https://www.mitre.org/sites/default/files/pdf/10_3301.pdf

Goldman, H., McQuaid, R., & Picciotto, J. (2011). *Cyber resilience for mission assurance* [Paper presentation]. 2011 IEEE International Conference on Technologies for Homeland Security, HST. https://ieeexplore.ieee.org/document/6107877

Haase, M. E. (2022). *Adversary Emulation Library: Wizard Spider*. https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/wizard_spider

Htet, K. P., & Rostovcev, N. (2019). *APT41*. MITRE ATT&CK. https://attack.mitre.org/groups/G0096/

Jabbour, K., & Muccio, S. (2011). The Science of Mission Assurance. *Journal of Strategic Security*, *4*(2), 61–74. https://doi.org/10.5038/1944-0472.4.2.4

Jabbour, K., & Muccio, S. (2013). On Mission Assurance. In P. A. Yannakogeorgos & A. B. Lowther (Eds.), *Conflict and Cooperation in Cyberspace: The Challenge to National Security* (pp. 107–160). Routledge.

Millington, E., & Gayda, O. (2025). *Wizard Spider*. MITRE ATT&CK. https://attack.mitre.org/groups/G0102/

Office of the Assistant Secretary for Research and Technology (OST-R). (2025). *Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)*. https://www.arc-it.net/

Ramluckan, T., van Niekerk, B., & Martins, I. (2020). *A Change Management Perspective to Implementing a Cyber Security Culture* [Paper presentation]. 19th European Conference on Cyber Warfare and Security. https://www.proceedings.com/55393.html

Rheaume, F. (2019). *Risk-based cyber mission assurance model, process and metrics* [Paper presentation]. 24th International Command and Control Research Symposium (ICCRTS) Conference. https://easychair.org/publications/preprint/vx5BN/open

Savolainen, T., McCarthy, N., Neville, K., & Ruoslahti, H. (2024). *Business Continuity Management of Critical Infrastructures from the Cybersecurity Perspective* [Paper presentation]. 2024 IEEE Global Engineering Education Conference (EDUCON). https://ieeexplore.ieee.org/document/10578811

Shahzad, S., Joiner, K., Qiao, L., Deane, F., & Plested, J. (2024). Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers. *Systems*, *12*(10), 434. https://doi.org/10.3390/systems12100434

Taylor, P. (2022). *EXOTIC LILY*. MITRE ATT&CK. https://attack.mitre.org/groups/G1011/

Thomas, J., & Galligher, G. C. (2018). Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. *Computer and Information Science*, *11*(1), 14–25. https://doi.org/10.5539/cis.v11n1p14

U.S. Air Force. (2019). *Operations Mission Assurance (Air Force Policy Directive 10-24)*. Department of the Air Force. https://static.e-publishing.af.mil/production/1/af_a3/publication/afpd10-24/afpd10-24.pdf

Watson, H., Moju-Igbene, E., Kumari, A., & Das, S. (2020). *"We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together* [Paper presentation]. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3313831.3376605

Wilf, J. (2023). *Cybersecurity as Part of Mission Assurance* [Paper presentation]. International Conference on Human-Computer Interaction.

Supplementary Materials

Prioritising Mission Survivability through Defensive Cyber Operations: A Unified Mission Assurance Approach

Download: https://ciasp.scholasticahq.com/article/158427-prioritising-mission-survivability-through-defensive-cyber-operations-a-unified-mission-assurance-approach/attachment/333155.docx