Whitehall Report 4-22

A UK Joint Methodology for Assuring Theatre Access

Jack Watling, Justin Bronk and Sidharth Kaushal

RUSI
Royal United Services Institute
for Defence and Security Studies

A UK Joint Methodology for Assuring Theatre Access

Jack Watling, Justin Bronk and Sidharth Kaushal

RUSI Whitehall Report, May 2022

Royal United Services Institute
for Defence and Security Studies

191 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 191 years.

Published in 2022 by the Royal United Services Institute for Defence and Security Studies.

RUSI Whitehall Report, May 2022. ISSN 1750-9432.

Cover image: Courtesy of Vitaly V Kuzmin/Wikimedia Commons

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Executive Summary

THE BRITISH MILITARY is expeditionary and seeks to confront adversaries abroad before they pose a threat at home. Theatre entry is therefore a precondition for the utility of the British military. Adversaries are fielding increasingly capable and integrated anti-air and anti-ship complexes that threaten the viability of theatre entry. These complexes differ from older systems in their level of integration, redundancy and consequent resilience. To assure the future relevance of the UK's military instrument, it is necessary to have a methodology for breaking through these systems.

The number of components within these complexes makes the destruction of the system too resource intensive to be a viable strategy. Nor – given the levels of integration – will the destruction of a small number of key nodes bring about the system's collapse. For this reason, US concepts for degrading anti-access/area-denial (A2/AD) architectures provide a poor guide for the UK as they assume a level of resource that is beyond the UK's capacity. The problem is larger than any single service and must be tackled by the Joint Force.

For the UK, the objective of the theatre access phase in operations should not be a system's destruction, but rather changing the behaviour of the system so that it is unable to deny access to the environment. Integrated systems may be understood to function in three behavioural states:

- The **optimal** operational state in which the system can coordinate the most appropriate response to a given threat.
- The **stressed** operational state in which the system is forced to engage in sub-optimal responses to threats but remains mutually supporting.
- The **degraded** operational state in which the system functions as isolated components and executes sub-optimal responses to threats.

Degrading the system requires that joint activity adhere to three principles:

- Effects should be applied **simultaneously** so that the defenders are constantly trying to resolve conflicting imperatives in how they respond.
- The threats to the system must be **persistent** to prevent the operators recovering and managing a graceful degradation of system functionality.
- The **tempo** of operations must **increase** to exploit the greater permissiveness of the operational environment as the system degrades.

To apply effects against the system to degrade its behaviour it is necessary for the available components of the Joint Force to offer the Theatre Entry Commander a range of options they can execute against the system. These offers can then be synchronised and deconflicted by the

command in accordance with the principles. The key effects should aim to affect four target sets (Table 1).

Table 1: Effects and Target Sets

Deny, Disrupt or Corrupt *Information Inputs*	**Induce *Personnel* to Experience**	**Deny, Degrade or Corrupt the *Network***	**Deny or Disrupt Access to *Supplies* of**
Early Warning	Fear	Links	Munitions
Identify Friend or Foe	Loneliness	Capacity	Fuel
Fire Control	Stress	Redundancy	Power
Target Acquisition	Fatigue	Permissions	Food and Water
Blue Force Tracking	Uncertainty	Assurance	Spare Parts

Source: Author generated.

The Theatre Entry Commander must also track the patterns that comprise the key indicators of system behaviour to assess campaign progress and inform risk management as the force escalates activity against the system.

To be able to apply these effects, it is essential that the force is prepared as regards its equipment, training and understanding of how its own capabilities interact with the threat systems. Assurance of theatre entry therefore requires preparation before the outbreak of conflict. In order to coordinate preparatory activity the UK should appoint a Senior Responsible Officer empowered with access to understand what activities are being undertaken to prepare for theatre entry operations and to resource and approve preparatory activities. The primary lines of effort in competition must be to **understand** the threat systems, to **collaborate** to shape favourable conditions in theatre, and to **constrain** the proliferation of A2/AD complexes.

In competition, understanding can be developed through the pursuit of:

- Covert collection on threat systems.
- Overt collection on threat systems
- Stimulation of threat systems.
- Procurement of threat systems for analysis.
- Seizure and recovery of threat systems for analysis.

In order to gain opportunities to target threat systems in competition and to expand the threat surface against them in conflict it is necessary to collaborate with partners. Collaboration should be aimed at:

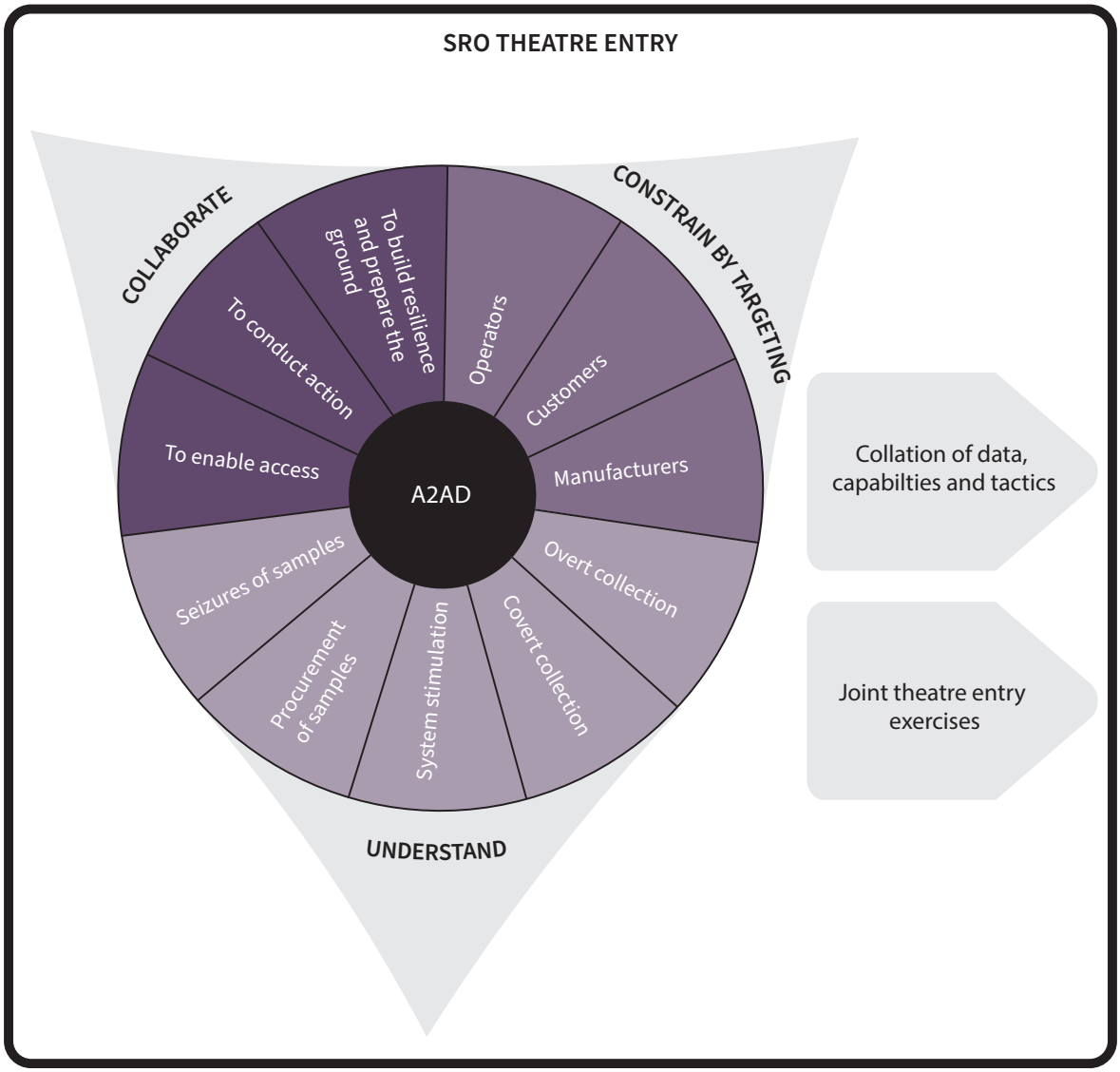
- **Developing access** to systems, either for collection in competition or disruption in conflict.
- **Conducting action** to seize systems in competition or destroy them in conflict.
- **Building resilience and preparing the ground** by training partners on how to identify and sabotage threat systems when they enter theatre.

Finally, the force should work to limit where systems are deployed and constrain their proliferation by targeting:

- **Operators**, through the threat of collection or seizure to limit where they are prepared to deploy systems.
- **Manufacturers**, by encouraging the defection of their personnel and imposing costs on association with companies to slow the development of new threat systems, while targeting the supply chains for critical system components.
- **Customers**, by imposing opportunity costs on procuring threat systems unless they collaborate, offering and facilitating alternative defences, and disrupting supply.

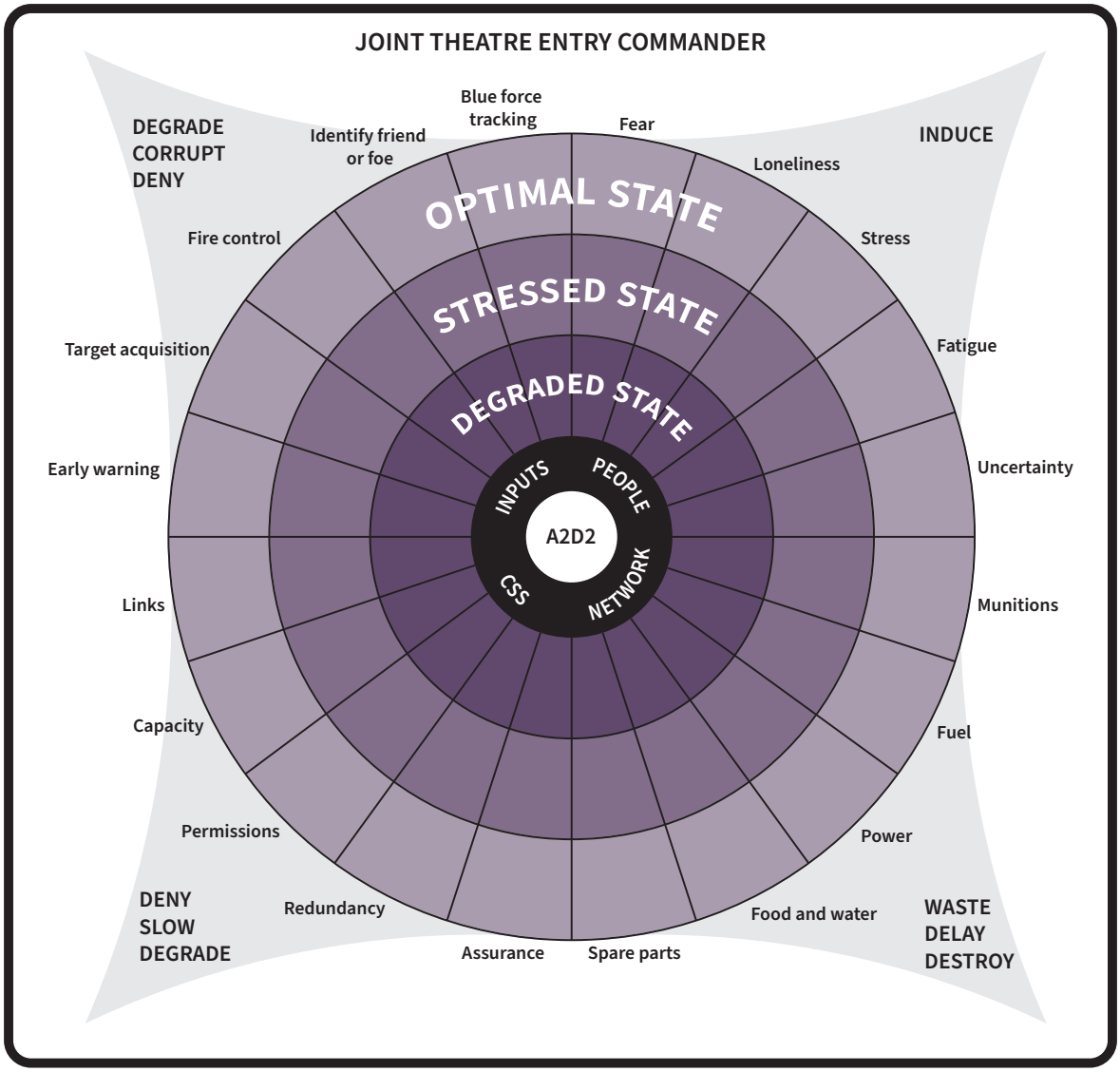
For preparatory work in competition to feed into options across the Joint Force in conflict it is essential that there is a repository of information developed about the threat systems, how they are fought, and the capabilities developed for disrupting them. This repository will necessarily be sensitive but access to it should be made available to those planning theatre entry operations in a format that is comprehensible to operators.

Figure 1: Targeting A2/AD Architectures in Competition



Source: Author generated

Figure 2: Targeting A2/AD Architectures in Conflict



Source: Author generated

Introduction

THE UK'S SECURITY has, for centuries, been premised on the ability to work with allies to constrain its adversaries in their spheres of influence, thereby limiting the impact of war on the trade and prosperity of the home islands.[1] Fundamental to offering allies support, and challenging adversaries at reach, is the ability to undertake expeditionary operations. British forces have persistently been tasked with pushing into contested waters, penetrating hostile skies, and ultimately projecting land forces onto enemy territory. The Integrated Review of Security, Defence, Development and Foreign Policy, setting out the government's vision for its future engagement with the world over the next two decades, reaffirms this approach.[2]

While the UK's aspiration has remained consistent, the viability of conducting expeditionary operations has been increasingly challenged by proliferating air, missile and coastal defence architectures that slow, challenge and potentially deny theatre access. Coastal defence batteries and air defence networks have been a planning concern for navies and air forces in any peer conflict for several decades. However, today these systems can be found in the arsenals of comparatively weaker states such as Algeria,[3] or even in the hands of non-state actors, including the Houthis and Hizbullah.[4] As a result, the capacity to project force anywhere is increasingly dependent on having a means of defeating these systems. The Russian invasion of Ukraine has demonstrated the highly constraining impact on air operations which even relatively poorly integrated air-defence networks can have.[5] In a conflict with a peer competitor such as Russia, being able to counter these systems quickly may determine defeat or victory since much of NATO's firepower is delivered by air. The denial of freedom of action in the airspace above an area of operations thus risks NATO ground forces being outgunned and overrun.

The countering of anti-ship cruise missiles (ASCMs) has been a major concern for navies ever since Egyptian forces sunk the INS *Eilat* with Styx ASCMs in 1967.[6] The threat posed by Argentine Exocet missiles during the Falklands War, for example, was a primary planning constraint on

1. Andrew Lambert, *Seapower States: Maritime Culture, Continental Empires and the Conflict that Made the Modern World* (New Haven, CT: Yale University Press, 2018), Chapter 6.
2. HM Government, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, CP 403 (London: The Stationery Office, March 2021).
3. Sidharth Kaushal, Archer Macy and Alexandra Stickings, 'The Future of NATO Air and Missile Defence', *RUSI Occasional Papers* (July 2021), p. 18.
4. Kaushal, Macy and Stickings, 'The Future of NATO Air and Missile Defence'.
5. Justin Bronk, 'Getting Serious About SEAD: European Air Force Must Learn from the Failure of the Russian Air Force over Ukraine', *RUSI Defence Systems*, 6 April 2022.
6. Toshi Yoshihara and James R Holmes, *Red Star Over the Pacific: China's Rise and the Challenge to U.S. Strategy* (Annapolis, MD: Naval Institute Press, 2018), p. 209.

Royal Navy operations throughout Operation *Corporate* in 1982.[7] The sinking of the Russian Black Sea Fleet flagship *Moskva* in April 2022 by Ukrainian anti-ship missiles provides a striking contemporary reminder of the continued importance of suppressing these systems to enable contested theatre access. Similarly, the arrival of SA-2 surface-to-air missile systems (SAMs) in Vietnam forced the US Air Force, Marine Corps and Navy to rapidly develop suppression or destruction of enemy air defences (SEAD/DEAD) tactics and capabilities.[8] The level of threat posed by increasingly capable and varied SAM systems meant that SEAD/DEAD rapidly became a key mission set for Western air forces, and one which drove major capability development from acquisitions to training and ultimately a new doctrinal approach to airpower campaigns.[9] Since the end of the Cold War, however, the growing range of threat systems, combined with the increased seeker performance of missiles and the interconnected networks that support these strike complexes, has fundamentally changed the way in which militaries must respond to these challenges. If historically ASCMs were the concern of navies, and SAMs the concern of air forces, then for medium powers today these systems pose a level of threat that is beyond a single service's capacity to counter and constitute a hurdle to the joint force's ability to operate. In response, a joint methodology nested within an integrated approach is needed.

Under the Levene reforms of the Ministry of Defence, capability development was devolved to the frontline commands.[10] The idea was that the navy was best placed to determine the requirement for its ships, the army for its tanks, artillery pieces and other equipment, and the air force its aircraft. The result has been that while operations have become increasingly joint, acquisitions and the development of fighting concepts has become increasingly siloed. Therefore, while there is an appreciation across UK defence of the threat posed by ASCMs and integrated air defences, the responses to these threats has been a rush among the services to 'own' the problem.[11] This threatens to be profoundly unhelpful, since no service is optimised for countering a concurrent and connected set of challenges that have been designed by adversaries with the specific purpose of imposing asymmetric costs on single domain capabilities. It is therefore necessary to see the degradation of these systems as a joint task.

The purpose of this report is to outline a joint methodology for the targeting of what has collectively been termed anti-access/area-denial (A2/AD) systems comprising ASCMs and integrated air defence systems (IADS).[12] The ability to counter these systems has become a basic requirement for expeditionary operations and therefore a fundamental hurdle for the

7. Yoshihara and Holmes, *Red Star Over the Pacific*.
8. John C Pratt, 'Project CHECO Southeast Asia Report: Air Tactics Against NVN Air/Ground Defenses, December 1966–November 1969', Pacific Air Forces, 30 August 1969, p. 50.
9. James R Brungess, 'Setting the Context: Suppression of Enemy Air Defences and Joint War Fighting in an Uncertain World', Air University Press, 1994, pp. 1–47.
10. Trevor Taylor and Andrew Curtis, 'Management of Defence After the Levene Reforms: What Comes Next?', *RUSI Occasional Papers* (September 2020).
11. Multiple author interviews and discussions with British Army, Royal Navy and Royal Air Force officers from operational and strategic planning branches, March 2021–February 2022.
12. For an early definition of the term, see Andrew F Krepinevich, Barry Watts and Robert Work, 'Meeting the Anti-Access and Area Denial Challenge', Center for Strategic and Budgetary Assessments (CSBA), 2003.

relevance of UK defence capabilities in most operational theatres. It is relevant not only to peer-level conflict, but also increasingly to executing the UK's basic obligations to protect its citizens or conduct humanitarian operations. A contested Non-Combatant Evacuation Operation in Lebanon – far from a remote possibility – for example, would see UK forces operate under threat of Bastion-P coastal defence cruise missiles (CDCMs), and potentially Syrian and Russian long-range air defences.[13] Similarly a humanitarian deployment to secure an oil spill from the FSO *Safer* off Yemen would place British forces in range of C-803 CDCM batteries operated by the Houthis.[14] In other words, counter A2/AD capabilities are not optional if the UK wishes to retain any pretence of sovereign power projection and deterrence capability.

Many of the terms used in this report require explanation, as do the boundaries of the problem set being analysed. First, it must be recognised that 'A2/AD' is not a doctrine or tactic of the Russian or Chinese military. Nevertheless, as a shorthand to encompass ASCMs and IADS, this term does encapsulate the challenge posed to British concepts of operation and is therefore used in this report. In terms of the focus on these two systems, it must be noted that in the Russian case CDCMs are but the innermost ring of their naval defensive architecture.[15] For China and Russia, meanwhile, their IADS are also bolstered by long-range precision strike capabilities that would hold the air bases of adversaries under threat.[16] China, in particular, places a considerable emphasis on the combined employment of long-range precision strike, anti-air and anti-ship missiles, with common missiles fired from land, air and sea assets in what it terms 'joint firepower campaigns'.[17] Nevertheless, from the point of view of British operations, the outer layers of Russian naval defences – from submarines to fixed-wing anti-ship capabilities – pose distinct operational challenges demanding their own tactical response. Similarly, land precision strike poses a challenge in terms of how land forces' logistics are organised and protected, and how air forces disperse their operations. For this reason, the US Army groups anti-ship missiles, IADS and land precision strike under the rubric of 'layered standoff'.[18] However, this report contends that the latter represents a very different targeting challenge. Land attack capabilities often do not rely on sophisticated kill-chains, given that their targets are static

13. Missile Defence Advocacy Alliance (MDAA), 'Hezbollah', <https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/non-state-actors/hezbollah/>, accessed 1 March 2022.
14. Sam LaGrone, 'USS Mason Fired 3 Missiles to Defend from Yemen Cruise Missiles Attack', *USNI News*, 11 October 2016, <https://news.usni.org/2016/10/11/uss-mason-fired-3-missiles-to-defend-from-yemen-cruise-missiles-attack>, accessed 1 March 2022.
15. Michael Kofman, 'Remarks at RUSI Sea Power Digital Conference: Session 1: Transforming Maritime Forces for an Age of Persistent Competition', 29 April 2021, 02:30–15:00, <https://www.youtube.com/watch?v=AfWS8hPdodc>, accessed 1 March 2022.
16. Thomas Shugart, 'First Strike: China's Missile Threat to U.S. Bases in Asia', Center for a New American Security, 28 June 2017.
17. Xiao Tianliang et al., *The Science of Military Strategy* (Beijing: PLA National Defence University Press, 2017).
18. Scott King and Dennis B Boykin IV, 'Distinctly Different Doctrine: Why Multidomain Operations Isn't Airland Battle 2.0', Association of the United States Army, 20 February 2019, <https://www.ausa.org/articles/distinctly-different-doctrine-why-multi-domain-operations-isn%E2%80%99t-airland-battle-20> accessed 1 March 2022.

rather than dynamic. Targets such as airbases, ports and logistical and transportation nodes can be attacked without access to real-time information from networks of radar and satellites, as is the case for both IADS and sea-denial systems. Precision strike against ground assets thus represents a complementary and self-contained system which supports the A2/AD threat. With modern Russian air-defence systems able to engage maritime targets, and the longer-range radar supporting Russian and Chinese anti-ship and anti-air missiles being the same, these capabilities are increasingly integrated into combined networks that consequently represent a common target set for the attacker. It is this problem set that this report attempts to address.

It may be asked why a UK joint methodology is necessary when the US Air Force has a long history of developing detailed doctrine for the conduct of SEAD/DEAD and the US Army's Multi-Domain Operations (MDO), which has grown into Joint All-Domain Operations, already proposes a joint approach to penetrating 'layered stand-off'.[19] In a NATO Article 5 scenario it is likely that the UK will be operating under US command and therefore pursuing an American campaign plan. Interoperability with the US and understanding of its doctrine is therefore important. However, because theatre access is now critical to most military operations, the UK needs sovereign options against this threat. US doctrine assumes a level of material superiority and mass that the UK, even operating alongside European allies, cannot replicate. Key tenets of this doctrine are unsuitable for UK needs. MDO, meanwhile, lacks granularity and aims at the complete destruction of the enemy standoff system, which is in the first instance attrition based, but more importantly inefficient and unrealistic for the UK as an objective end state. For this reason, the wholesale adoption of US approaches does not meet the UK's needs, and there is a need for a UK methodology to enable theatre entry.

The evidence for this report was gathered from a range of sources. The authors conducted a survey of literature on A2/AD architectures published in a range of countries that employ the systems, most notably Russia, China and Iran. The authors also considered the evolution of adversary doctrine and compared it with the historical record as to how these systems have been employed in combat. To understand the trajectory in the employment of these systems the authors interviewed officers from NATO and non-NATO countries who operate air defences, including those who were trained or involved in the development of Russian systems. It was also necessary to interview officers from all domains who were working on the concepts for how to defeat layered defences. These interviews were conducted between September 2021 and April 2022. For some of the systems under examination it was possible to access system components, and in some cases to turn these systems on to test the effectiveness of their sensors, the crew workload, levels of situational awareness and persistence. The authors also joined military exercises in which air defences attempted to acquire and simulate the engagement of targets, observing the processes, procedures, pressures and pattern of performance of the crews. Finally, the authors flew in helicopters from several NATO countries, UK air mobility platforms and fast air, and spent time aboard Royal Navy ships to better understand the processes involved in employing the systems required to degrade the target systems.

19. King and Boykin IV, 'Distinctly Different Doctrine'.

In seeking to develop a methodology for the joint targeting of A2/AD architectures, this report is divided into four chapters. The first seeks to outline how A2/AD architectures are structured to explain the design and consequent trade-offs and dependencies in the systems which a theatre entry force must target. This chapter largely uses Russian systems as the baseline for the architecture. This is first for the sake of consistency, second because they have proliferated more widely than Chinese systems, and third because there is a more even distribution of information available on Russian systems and their practical employment, whereas for many Chinese systems it is not always clear how their concepts will translate into operational practice. The chapters generally refer to NATO designations for Russian systems because while these signifiers (SA-15, SA-17, SA-21, SA-22, SA-23, etc.) do not offer a high level of granular detail, using Russian signifiers can reduce clarity because the Russian armed forces often deploy multiple generations of each system simultaneously in their formations. Where specific Russian types within these NATO designations pose challenges, the report uses the Russian designations. Short summary descriptions of these systems are included in the annex for readers not familiar with their characteristics.

The second chapter sets out the targeting methodology developed by the authors. It begins by setting out the results being sought – defining success in terms of shaping system behaviour rather than system destruction – and from there sets out key principles for orchestrating joint effects. The chapter then breaks down targets by type, based on the threats to the system that can be exploited to create stresses which will degrade its operational effectiveness.

The third considers the continuous activities and opportunities in competition that must be undertaken to limit and understand the threat systems that enable the types of targeting activity outlined in the targeting methodology contained in chapter two.

The fourth chapter seeks to outline the decision points that commanders will face in terms of how they move through the targeting phases identified in the methodology. It considers the challenges of battle damage assessment, and how a force can determine whether it has had its intended effects, thus allowing an expanded scope of operations into a contested environment.

I. Mapping the Threat and its Dependencies

A2/AD ARCHITECTURES HAVE been developed and deployed in multiple forms around the world by states concerned about the potential threat posed by military forces to their sovereignty or freedom of action. Policy discussions on A2/AD tend to focus on the missiles which make up the kinetic effectors within such networks – the SAM and CDCM batteries. Some experts reject the notion that A2/AD architectures represent a fundamentally new challenge to Western military freedom of access.[20] However, this report contends that the degree of integration and overlapping coverage of such architectures presents a new challenge.

The US and the UK in particular have assumed dominance in the air and maritime domains over potential adversaries for military advantage since at least the end of the Cold War. The anti-access technologies developed in response can be grouped into three broad historical categories: manually aimed cannons; radar cued and laid cannons; and missiles. Manually aimed coastal anti-ship artillery and anti-aircraft batteries' ability to deter and strike naval and air forces was limited to each crew's ability to spot and identify potential targets, and then the weapons' ability to reach and damage those targets. During the Second World War, radar guidance for both coastal anti-ship and anti-aircraft cannon batteries became commonplace. This not only made them significantly more accurate and lethal at long ranges, but also created a new set of imperatives for naval and air forces attempting to penetrate areas covered by such defences. The radar chains which detected targets and the fire control radars which helped to aim the defensive guns had to be either avoided, jammed or destroyed to reduce the effectiveness of the cannons, which made electronic attack and electronic countermeasures essential for day-to-day naval and air mission planning. The introduction of guided missiles using semi-active radar guidance in the 1960s marked the third generation of anti-access systems. For the first time, both naval and air forces could be reliably threatened beyond the range of heavy cannon fire, and in most cases beyond the effective range of the weapons carried by warships and aircraft themselves. As a result, fixed defence sites shifted from being a threat which needed to be factored into loss rate calculations during operations against enemy-held territories, into a key determinate of campaign viability and, later, theatre entry.[21]

Modern IADS and anti-ship missile complexes are technically still composed of systems which outwardly resemble the missile batteries and command-and-control (C2) architectures which

20. See, for example, John Richardson, 'Deconstructing A2/AD', *National Interest*, 3 October 2016, <https://nationalinterest.org/feature/chief-naval-operations-adm-john-richardson-deconstructing-17918>, accessed 1 March 2022; Michael Kofman, 'It's Time to Talk About Russian A2/AD: Rethinking the Russian Military Challenge', *War on the Rocks*, 5 September 2019.
21. Brungess, 'Setting the Context'.

US-led forces have repeatedly defeated in multiple post-Cold War conflicts. However, these modern A2/AD networks are far removed from their Cold War-era antecedents. The degree of integration and capability overlap between the component systems renders the capability with which states such as Russia, China, Iran, Algeria and Syria effectively deploy a new category of anti-access system.[22] The implications in terms of the increase in the threat level posed and the level of innovation required to reliably degrade them are comparable to the addition of radar guidance for defensive cannon batteries or the introduction of guided missile technology. In addition, the far greater degree of tactical and operational integration possible with digital architectures today, along with the greatly increased effective range of many modern Russian and Chinese missile systems, enables overlapping fields of fire and cooperative leveraging of sensor data between component systems, making each one very difficult to engage or degrade in isolation.

To establish a methodology for degrading an A2/AD architecture it is first necessary to understand how it is integrated, commanded and fought, and to map its critical dependencies. Understanding these points is necessary for appreciating why the system is effective, but also where its points of vulnerability are and where an adversary can apply pressure to gain leverage over the behaviour of the system. This chapter therefore considers the critical components of an A2/AD architecture as they relate to five categories of dependency for the system. These are: the system's sensors and information inputs; its operators and crews; its integration mechanisms; its munitions; and its combat service support requirements. This chapter breaks down each of these to show the layers within each category.

Sensors and Information Inputs

The first consideration with any set of networked military systems is how data is gathered, converted into information and subsequently used to build situational awareness and guide kinetic engagements by the system as a whole. A modern A2/AD architecture such as those deployed by Russia, China, Iran and others gathers data from multiple layers of sensors and uses that data to build the information required for early warning of the approach of potential threats, the identification and tracking of individual targets, and the guidance of missiles against those targets.

The first layer of sensors operates beyond the radar horizon as seen from the ground. This layer can encompass both space-based assets and ground-based over-the-horizon (OTH)radar. Space-based electronic intelligence (ELINT) and synthetic aperture radar (SAR) satellites are particularly useful enablers for maritime A2/AD: the RORSAT and Legenda constellations, for example, were core components of Soviet sea-denial systems[23] and today long-range Chinese

22. Jerome Dunn, 'Lecture at RUSI Missile Defence Conference 2022', London, 23–24 February 2022.
23. Sidharth Kaushal et al., *The Balance of Power Between Russia and NATO in the Arctic and High North* (RUSI Whitehall Paper, 2022), p. 45.

strike assets such as the DF-21D will rely heavily on the Yaogan ELINT and SAR constellations.[24] Given that only China operates large satellite constellations – Russia has struggled to replace the Legenda system with its planned Liana and Persona satellites[25] – suppression of space-based assets should be comparatively simple against most peers. These architectures depend on a limited number of downlinks and can be suppressed from a considerable distance.[26]

This layer also comprises OTH radar. The curvature of the Earth's surface creates a 'shadow' below the horizon as seen from any particular radar or sensor, within which potential incoming threats cannot be directly 'seen' or tracked. The higher a sensor is positioned off the ground and the higher a potential target is (assuming it is an aerial target), the longer the effective detection range can potentially be. However, certain radar bands with long wavelengths and correspondingly low frequencies can look over the horizon by bouncing their emitted energy off the ionosphere.[27] Long wavelengths reduce the effective resolution available in any returns for a given array size, and OTH techniques also encounter issues to do with backscatter, which further reduce the practical resolution and accuracy that is obtainable with such systems. As such, OTH radars are typically used to provide long-range early warning rather than target acquisition, identification or tracking. Traditionally, arrays such as the Russian 5H32-West 'Duga-1' or American AN/FPS-118 OTH-B network were primarily intended to provide advanced warning of incoming nuclear missile and bomber attack waves as part of each of their respective national nuclear C2 structures.[28] However, more modern OTH systems – most notably the Russian 29B6 'Container' – can also provide significantly higher resolution monitoring of airspace activity over thousands of kilometres, and from deep within their own territory.[29]

OTH systems still typically have a resolution measured in kilometres against targets such as ships or aircraft, and so have very limited utility as a means to guide weapons to targets. However, they still make it very difficult for hostile air or maritime forces to assemble into strike groups or packages for operations against a defence network without those movements being detected and roughly tracked. Thus, their integration into IADS and CDCM complexes makes operational surprise difficult to achieve and enables the subsequent layers of sensors, which provide input for the network to be ready and cued towards likely avenues of approach by the time Western forces come within their range.

24. S Chandrashekar and Soma Perumal, 'China's Constellation of Yaogan Satellites and the ASBM – May 2016 Update', National Institute of Advanced Studies, May 2016.
25. Kaushal et al., *The Balance of Power Between Russia and NATO in the Arctic and High North*, p. 46.
26. Christopher Coker, *The Improbable War: China, the United States and the Logic of Great Power Conflict* (Oxford: Oxford University Press, 2015), pp. 151–55.
27. Eric Heginbotham et al., *The U.S China Military Scorecard: Forces, Geography and the Evolving Balance of Power 1996–2017* (Santa Monica, CA: RAND, 2015), p. 157.
28. For example, see Federation of American Scientists, 'AN/FPS-118 Over-The-Horizon-Backscatter (OTH-B) Radar', 29 June 1999, <https://nuke.fas.org/guide/usa/airdef/an-fps-118.htm>, accessed 18 January 2022.
29. Daria Mikhalina, 'Russia's First Over-The-Horizon Radar Has Taken Up Combat Duty', *Zvezda*, 1 December 2019, <https://m.tvzvezda.ru/news/201912180-qwJP2.html>, accessed 18 January 2022.

The second layer of sensors in terms of long-range inputs which provide data to the network are ground- and air-based direct-regard long-range early-warning and target acquisition radars. Examples include the radars carried by AWACS aircraft such as the Russian Beriev A-50M and Chinese KJ-2000,[30] fixed ground-based arrays including the Russian Voronezh-M, -DM and -VP stations,[31] and mobile systems such as the 55Zh6M Nebo-M long-range surveillance and anti-stealth radar complex and 91N6E 'Big Bird' search and acquisition radar which forms part of SA-21 and SA-23 long-range SAM systems.[32] Shorter-range OTH surface search radar such as the Monolit-B and Polsodnukh-E and maritime patrol aircraft including the IL-38 and Tu-142 also fall into this category.[33] The primary function of these systems is to provide the entire defence network with a comprehensive situational awareness picture, acting as the main 'eyes and ears' for all the other more specialised sensors, C2 systems, and the missile batteries charged with actually engaging threats. As such, they need to be actively scanning for a far greater proportion of time than the radars distributed at lower levels of the network and will be situated a significant distance from any frontline; ideally on high ground or airborne to improve performance against low flying or surface targets at long ranges. This makes them relatively easy to locate and track, but nonetheless challenging to attack or suppress comprehensively due to their high-power output levels and typical location deep behind enemy lines and protected by other layers of the network, as well as potentially point defence systems in the case of ground-based radars and combat air patrols in the case of AWACS. Many more modern, digital long-range surveillance and target acquisition radars can also take on fire control responsibilities if necessity dictates, as their resolution and beam focusing capabilities are sufficient to guide semi-active and active radar missiles to targets at significant ranges. However, their core role is as the primary input source for 'big picture' information which is used to coordinate and fight with the network as a whole.

The next layer of sensors is found at the SAM and CDCM battery level, in the form of dedicated target acquisition radars such as the 96L6E 'Cheese Board' used by the SA-21 and fire control

30. On the KJ-2000, see Sidharth Kaushal and Magdalena Markiewicz, 'Crossing the River by Feeling the Stones: The Trajectory of China's Maritime Transformation', RUSI *Occasional Papers* (October 2019), p. 70; Mark Episkopos, 'Russia's A-50U Aircraft Means Business', *National Interest*, 5 November 2021.
31. On the Voronezh and its relationship to systems such as the S-500 and S-400, see speech by Valeri Saar at RUSI 2022 Deep Strike and Missile Defence Conference, London, 23 February 2022. Delivered in person.
32. *Global Security.org*, '55ZH6M "Nebo-M" TALL RACK Mobile Multi-Band Radar Complex', <https://www.globalsecurity.org/military/world/russia/nebo-m.htm>, accessed 18 January 2022; Carlo Kopp, 'Search and Acquisition Radars: NIIIP 5N64S/64N6E/E1/E2/91N6E Big Bird', *Air Power Australia*, updated April 2012, <Search and Acquisition Radars (S-Band, X-band) (ausairpower.net)>, accessed 18 January 2022.
33. Kaushal et al., *The Balance of Power Between Russia and NATO in the Arctic and High North*, pp. 40–55.

radars including the 9S36 used in the SA-17 M-2.[34] For ground-based CDCMs, while radar such as the Monolit-B can provide target acquisition, exploiting the potential of these systems typically requires the use of other spotters such as Ka-31 helicopters, UAVs and low observable surface vessels like the project 22160.[35] Target acquisition radars in this context provide a source of wide-area situational awareness, target tracking, identification and sometimes a measure of backup fire-control capability for a battery. They are the primary local source of big picture situational awareness for a battery and its command vehicle crew if a system is working in isolation. However, when the battery is operating within a modern integrated defence system, its organic target acquisition radar can both feed information to the wider network when actively scanning or remain passive most of the time to make the battery harder for hostile forces to detect, locate, track and either strike, suppress or avoid. The higher layer of surveillance and target acquisition radars within the network can, through such tactics, increase the survivability of forward batteries by reducing their need to illuminate their own target acquisition radars most of the time. In either case, in each battery of CDCMs or SAMs, the organic fire control radars will generally be cued onto targets by either the battery's own target acquisition radar or target data passed to the battery from external sensors elsewhere in the network.[36] Once a fire control radar has acquired the target, it will illuminate it with a beam of concentrated radar energy, which provides high resolution data on target speed, heading, position and signature that can both guide missile shots to target and also be relayed to the rest of the network to enhance the granularity of the overall situational awareness picture.[37] When the network is working as intended, there is also a range of other potential inputs at this more tactical layer, including fighter aircraft equipped with datalinks, sensors mounted on warships and other mobile assets which do not form a core part of the sensor apparatus for defence networks but can contribute when integration pathways and mission capacity allow.[38]

The final and most tactical layer of sensors are those mounted on launch platforms and effectors themselves. Many types of SAMs incorporate transporter erector launcher and radar (TELAR) vehicles which, as the name suggests, mount a fire control radar which gives each launch

34. *GlobalSecurity.org,* '96L6 / 96L6E - CHEESE BOARD Radar', 28 July 2019, <https://www.globalsecurity.org/military/world/russia/96l6.htm>, accessed 2 March 2022.
35. Charles Bartles, 'Improvements to the Onyx Coastal Defence Missile', OE Watch, December 2019, <https://community.apan.org/wg/tradoc-g2/fmso/m/oe-watch-articles-2-singular-format/345363>, accessed xxx; Aleksey Ramm and Bogdan Stepovoy, 'S korablya na «Bastion»: ataka beregovykh batarey stanet vnezapnoy' ['From Ship to Bastion: Shore Batteries Attack Will Be Sudden'], *Izvestiya*, 22 October 2019, <https://iz.ru/930452/aleksei-ramm-bogdan-stepovoi/s-korablia-na-bastion-ataka-beregovykh-batarei-stanet-vnezapnoi>, accessed 29 November 2021.
36. Peter W Mattes, 'What Is a Modern Integrated Air Defense System', *Air Force Magazine*, 1 October 2019, <https://www.airforcemag.com/article/what-is-a-modern-integrated-air-defense-system>, accessed 13 April 2022.
37. Author interviews with SAM operators and visits to inspect systems, July 2021–January 2022.
38. For more information, see Justin Bronk, 'Modern Russian and Chinese Integrated Air Defence Systems: The Nature of the Threat, Growth Trajectory and Western Options', *RUSI Occasional Papers* (January 2020).

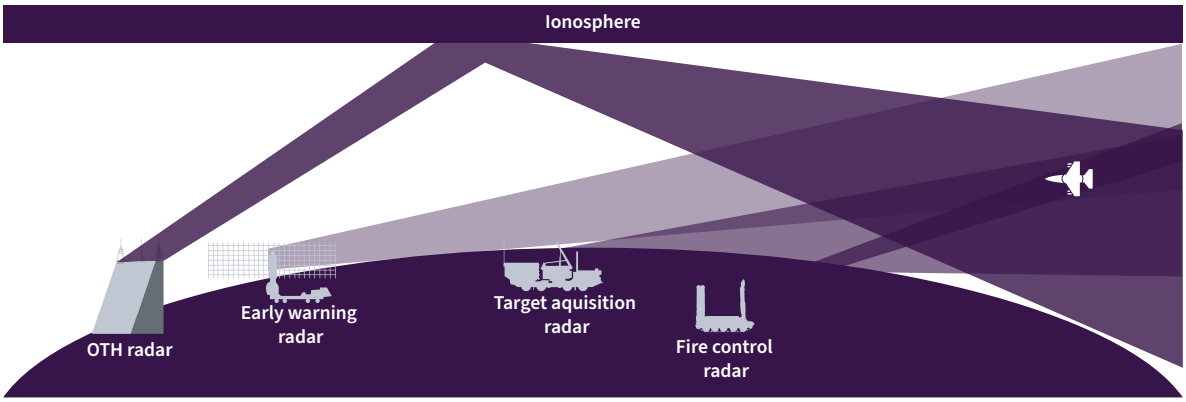
platform an organic engagement capability. The radars mounted on TELARs are typically smaller and offer reduced field of regard, range and performance compared to dedicated fire control radars. However, where systems such as the SA-17 M-2 feature modern passively electronically scanned array (PESA) type radars,[39] TELARs nevertheless represent potentially potent sensors once a target is within their field of view. They are more than capable of guiding missiles to difficult targets in the absence of dedicated fire control radar vehicles, but are also more reliant than the latter for receiving early warning and cueing information from a wide-area surveillance or target acquisition radar to allow them to acquire targets reliably.[40] In the case of sea denial, the final sensor in the kill chain is the active seeker on the missile fired. Most modern ASCMs have active radar seekers, and often possess dual-mode seekers to offset jamming attempts. Missiles in swarms can typically be used cooperatively to compensate for a limited field of view, a tactic that the Soviet Navy pioneered with the P-700 Granit cruise missile.[41] Typically, some missiles in a salvo fly high – expanding their radar horizon and providing data to lower flying sea-skimming missiles. Ballistic missiles, given the heights from which they drop vertically, can cover substantial areas with their seekers – potentially compensating for inaccuracies earlier in the kill chain – although their ability to manoeuvre in terminal sprint to act on data gathered is physically constrained.[42]

When a modern A2/AD architecture is working as designed, it can draw information from multiple overlapping layers of ground-based, airborne and orbital early warning and target acquisition radars. In addition, it can draw on space-based assets, including Earth observation (EO) satellites and SAR satellites, which play a particularly important role in sea denial.[43] This information can then be used to cue multiple layers of standalone and TELAR-mounted fire control radars to guide missiles to targets. As a result, the system can absorb considerable losses in individual radar systems for a prolonged period before overall engagement capability drops significantly. Even once this occurs, the system can retain partial functionality, including by relying on less-than-ideal sources of data. To use an example, the People's Liberation Army Navy (PLAN) is increasingly training maritime militia forces and fishermen to act as mobile

39. *Army Technology*, 'Buk-M2E Air Defence Missile System', 1 May 2014, <https://www.army-technology.com/projects/buk-m2e-air-defence-missile-system/>, accessed 2 March 2022.
40. Author interviews with SAM operators and visits to inspect systems, July 2021–January 2022; Stephen Biddle and Ivan Oelrich, 'Future Warfare in the Western Pacific: Chinese Antiaccess Area Denial, U.S. AirSea Battle, and Command of the Commons in East Asia', International Security (Vol. 41, No. 1, 2016), pp. 7–48.
41. MDAA, 'P-700 Granit/SS-N-19 "Shipwreck"', <https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/p-700-granit-ss-n-19-shipwreck/>, accessed 1 March 2022.
42. Sidharth Kaushal, 'The PLA's Continued Emphasis on Subsonic Anti-Ship Missiles', *RUSI Defence Systems*, 25 February 2022, <https://rusi.org/explore-our-research/publications/rusi-defence-systems/china-military-report-plas-continued-emphasis-subsonic-anti-ship-missiles>, accessed 1 March 2022.
43. Heginbotham et al., *The U.S.-China Military Scorecard*.

sentries. Civilian satellite imagery might represent another data source given the proliferation of these assets to private sector actors.

Figure 3: Sensor Layers in an IADS



Source: Author generated.

Operators and Crews

A2/AD architectures are far more than a set of sensors and missiles. The operators and, more specifically, their behaviours and capacities within that network, are also critical to its performance. However, even before examining the system operators themselves, it is important to note that the choices made by senior commanders and politicians at the strategic level on risk tolerance, force posture and rules of engagement will greatly affect how an A2/AD architecture interacts with the operating environment. Strategic decisions at this level can lead to significantly different active and reactive behaviours than those which a purely technical analysis of the components of the defence network would suggest. For example, a political decision to reserve the authority for the use of lethal force at a more senior level than battery commanders might impose significantly different procedures, greater vulnerability to communications disruption and longer engagement timescales on systems which are technically capable of rapid detection and launch against incoming targets. Furthermore, characteristics and behaviours in a defence network which are dependent on posture decisions made at the senior military and political level can change extremely rapidly if those decisions are superseded by new ones. In the context of sea denial, the fact that some systems, such as the 3M-54 Kalibr, the Kinzhal and the 3M22 Zircon, are dual use and can carry low-yield nuclear warheads means that they may be held in reserve as a means of escalation management.[44] Political decisions regarding how many missiles are available for conventional warfighting will constrain coastal defences.

44. Michael Kofman, Anya Fink and Jeffrey Edmonds, 'Russian Strategy for Escalation Management: Evolution of Key Concepts', CNA, April 2020.

Within the network itself there are three key groups of operators: those who sit in the various C2 centres and mobile nodes; those who sit in the radar, TEL and TELAR vehicles at battery level; and those who operate the supporting logistics and resupply structures which keep the batteries effective over time. The actions of each of these groups are interdependent to a significant degree and are also affected by the strategic level policy choices governing the entire A2/AD architecture.

C2, data fusion and coordination nodes such as the Russian D4M1 'Polyana' vehicle pair typically sit at the regimental or brigade level of an air defence organisation. In the context of sea denial, Monolit-B radar are held at the level of the coastal defence brigades, while longer-range systems report to regional naval commands. In each case, the systems are intended to act as the supporting glue to link and coordinate the activities of type-specific command vehicles such as the 55K6E or the K380P.[45] In such nodes, operator activities are divided up between command tasks governing how the network is fought at the operational and tactical levels, and the more administrative tasks of managing data flows from and to sensor elements and shooter batteries, allocating tasks, permissions and orders to individual components, and monitoring the overall status of those components to ensure that the command level is making decisions based on the best possible information.[46] This is also the practical level at which the broader recognised air picture is intended to be blended with the situational awareness picture generated by the active and passive sensors in the network itself.

The tasks which operators are attempting to fulfil within C2 nodes rely heavily on low-latency connectivity between their fixed facility or mobile post, the various early warning, surveillance and target acquisition sensors providing situational awareness, and the mobile batteries and support elements whose activities and engagements they are attempting to coordinate and optimise.[47] Most tasks within such a vehicle are both technically complex and demanding in terms of workload and the contextual awareness and judgement required to be effective. There are a large number of moving parts within defence networks and when under attack, individual components will be operating at various EMCON states, frequently relocating, potentially under attack, and facing difficult choices to balance vulnerability and combat persistence with potential lethality against incoming threats. Furthermore, a C2 node is likely to be coordinating missile shots from some batteries using radar data and potentially even active fire control guidance from a different one. Exercising command over and technical facilitation of such activities requires a significant level of tactical and technical understanding as well as responsiveness. Therefore, some of the most highly trained and valuable operators throughout an IADS or broader defence network will be found in these command posts. For sea denial, by contrast,

45. Rosoboronexport, 'Polyana D4M1 (9552MI)', Air Defence Systems Catalogue, <http://roe.ru/eng/catalog/air-defence-systems/air-defense-automated-command-and-control-systems/%22Polyana-D4M1%22%20%289S52M1%29/>, accessed 17 September 2019.
46. Author interviews with operators familiar with a range of Soviet and more modern Russian systems, November 2021.
47. Author interviews with operators familiar with a range of Soviet and more modern Russian systems, November 2021.

the importance of fixed, though well defended, naval headquarters to both the coordination of coastal defence assets and integrating data from sources afloat, in the air and on the ground makes these headquarters tactically relevant.[48] The system is still likely to function if the operation of headquarters is hindered either by kinetic means or sheer information overload by, for example, passing decision-making authority down to brigade and battalion level. However, at this juncture, coordinated air-, land- and sea-based salvos become impossible and the system shifts to mounting sequential or dispersed attacks.[49]

At the more tactical level, a battery or battalion command vehicle crew will need to simultaneously be responsible for coordinating tactical engagements, the location, set-up and relocation activities and posture of the battery elements under their command, and potentially integration with other short-, medium- or long-range sensors and SAMs. The span of responsibility for commanders and C2 vehicle crews at this level will be greatly affected by the connectivity and capacity available to the higher C2 echelons within the network at any given time, as well as the broader force posture and Rules of Engagement (RoE). It will also vary significantly depending on the type of SAM system that the battery or battalion operates. Command post units for long-range 'strategic' SAM systems such as the SA-21 or SA-23 are designed, configured and their operators trained to be able to link up and coordinate the actions of the medium- and short-range systems operating within the area that they cover.[50] By contrast, the command vehicle accompanying a medium-range SA-17 or short-range SA-15 unit is unlikely to have this level of assumed responsibility or communications, data fusion and coordination capacity. As such, there is a hierarchy of task complexity, crew training and importance for operators who might nominally fulfil the same role description, depending on which system they are assigned to and what layer of the defence network that system fills.

A general constant is the fact that modern integrated defence systems are designed to degrade gracefully if higher C2 echelons are either destroyed, cut off from communications or otherwise temporarily rendered unable to perform their intended role. In theory, as each echelon of C2 is removed, there are command vehicles and crews able to coordinate the movements, engagements and support operations for their own and any assigned subordinate layers of sensors and shooters. In practice, of course, the ability to effectively perform these functions is limited by the availability of wide area situational awareness, crew size and workload, training level, fatigue state, permissions, and the need to relocate regularly to avoid effective targeting by enemy forces. As such, the further down command echelons that coordination functions can be pushed, the more operators will struggle to meet the requirements of the network and will revert to operating as distributed elements. This will be particularly true for air defence elements operating close to the frontlines or while on the move, as their access to higher

48. Bartles, 'Improvements to the Onyx Coastal Defence Missile'.
49. On Chinese thinking regarding the phases of integration achievable with respect to sea denial, ranging from the ability to launch simultaneous salvos, to coordinated 'overtaking salvos' if the system is partially degraded and finally dispersed attacks if operators are effectively isolated, see Yoshihara and Holmes, *Red Star Over the Pacific*, p. 243.
50. Bronk, 'Modern Russian and Chinese Integrated Air Defence Systems', pp. 9–12.

echelon support will be constrained by available communications channels and emissions control concerns. Furthermore, the behaviours of operators at every level of the system will be significantly affected by the level of perceived capacity of the currently commanding C2 echelon to coordinate and fight the network effectively with sound information and judgement. Decisions as to whether to illuminate battery or battalion radars, whether to fire and in what modes and quantities at enemy assets, and when and where to deploy or relocate can easily cost operators their lives by unmasking them to enemy forces or leaving them exposed without adequate munitions for self-defence. While a defence network is functioning as intended with brigade or even higher-level C2 in place and the presumption that decision-makers have access to excellent tactical, operational and strategic situational awareness and training, decisions are likely to be acted upon without question at the tactical level. However, if effective command is being exercised at a significantly more tactical level, the operators will struggle with crew capacity, communications bandwidth and/or latency and coordinating movements due to having to operate at or beyond the edge of their training envelope. Recent Russian experiences during the early days of the invasion of Ukraine suggest operators at the battery level may make poor decisions which significantly compromise overall effectiveness without adequate higher-level coordination.[51] There is often, therefore, a mutually reinforcing degradation between stresses to C2 and the tactical decision-making of system components.

Within TELARs, vehicle commanders are responsible for crew coordination and (*in extremis*) can coordinate organic engagements using the on-board radar. The rest of the crew operate the fire control radar and perform the launch sequence, feed in external information, check IFF data and drive the vehicle.[52] In older model systems such as the SA-11 these activities were manually coordinated through analogue controls for azimuth and elevation, large numbers of switches and intricate crew procedures were required to complete a successful target acquisition, launch and guidance procedure. Sitting in a cramped self-propelled chassis next to the loud diesel engine or gas turbine needed to power the radar and mission systems will quickly tire out even seasoned crews if alert status needs to be maintained for longer than a few hours at a time, and combat effectiveness may diminish rapidly.[53] Modern versions of such systems tend to have digital interfaces and much more heavily automated controls which significantly reduce the technical skills required of operators and will lessen the impact of fatigue and other human factors on operational effectiveness over time.[54] However, the requirement for seamless crew coordination in order to generate effective capability at the tactical edge remains despite the digitisation of the systems. The psychological and behavioural impact of the knowledge that unmasking to engage targets risks imminent and often fatal retaliation from enemy forces also

51. Justin Bronk, 'The Mysterious Case of the Missing Russian Air Force', *RUSI Commentary*, 28 February 2022.
52. Author interviews with operators familiar with a range of Soviet and more modern Russian systems, November 2021; author experience inside a transporter erector launcher and radar (TELAR) during operation, September 2021.
53. Author interviews with operators familiar with a range of Soviet and more modern Russian systems, November 2021; author experience inside a TELAR during operation, September 2021.
54. Author technical assessment of captured Russian air defence systems in Ukraine, April 2022.

should not be underestimated at the battery level. This fear can be amplified by the loss of situational awareness that occurs when severed from higher echelons.

For those operating the logistical support systems which allow a defence system to continue functioning, the nature of their task will be heavily dictated by the activities of the other elements of the network. In peacetime, or in a relatively static posture, firing units will generally use pre-sited deployment areas close to the depots where additional missile ammunition, fuel and spare parts are stored or staged.[55] However, if the system is being postured to resist potential attack or is actively being engaged, the logistics support personnel will need to either push supplies pre-emptively to batteries or respond rapidly to requests for resupply in the field as firing units, radars and command vehicles go into action and quickly relocate to avoid destruction by enemy forces. The tempo of operations, the posture in terms of ammunition expenditure and relocation frequency will all affect the distances and frequency with which resupply and support activities will have to move out from their depots and staging areas, as well as the risk that those vehicle convoys will be exposed to during such sorties. In terms of individual tasks, the logistics support side of an integrated defence network covers a wide range of requirements, including specialist radar and missile technicians, vehicle maintainers, specialist personnel to operate the reloading vehicles and their cranes which resupply launchers with missile rounds in the field, communications and mission system repair specialists, and a host of other tasks. Their ability to rendezvous rapidly with the batteries during combat operations will also depend to a significant extent on their ability to communicate with those units and the C2 levels above them – which will itself potentially generate a signature which can be exploited by enemy forces to find and attack them. It is also worth noting that combat service support troops may not be as attuned to the requirements of operational security as frontline forces. In some cases, the use of contractors for logistical support will exacerbate this.[56]

Integration Mechanisms

As can be readily understood from the chapter so far, the smooth functioning of a modern A2/AD architecture relies heavily on resilient, low-latency communication links between many geographically dispersed mobile and fixed assets across multiple echelons. The preferred Soviet and now Russian method of intra- and inter-element communication is via buried landline links which can be accessed through standard field cable ports at pre-sited firing points in friendly territory. Such cables provide the lowest latency available which is critical for allowing third-party targeting and weapon guidance between different sensor and shooter components, and also provides a robust capability in the face of hostile electronic warfare interference. Signals

55. Author interviews with operators familiar with a range of Soviet and more modern Russian systems, November 2021.
56. David Axe, 'The Russian Army Depends on Civilians to Keep it Supplied. This Could Be a Problem in Ukraine', *Forbes*, 14 January 2022, <https://www.forbes.com/sites/davidaxe/2022/01/14/the-russian-army-depends-on-civilians-to-keep-it-supplied-this-could-be-a-problem-in-ukraine/?sh=5b0899672e37>, accessed 28 April 2022.

battalions for laying these cables are a critical component of the logistics support to tactical elements of the system.[57]

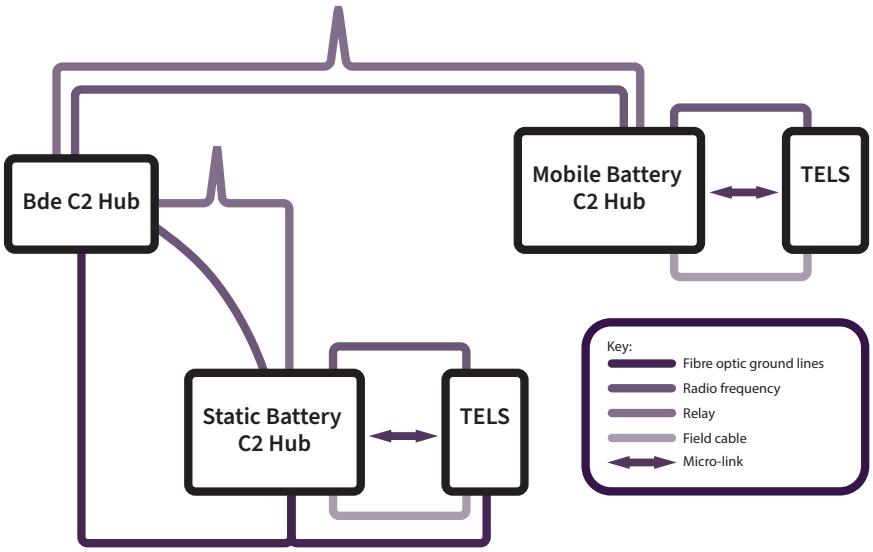
Vehicles within batteries are also able to use directional microwave-wavelength datalinks within line-of-sight when operating away from pre-prepared firing locations and when dispersed beyond the reach of field cables.[58] Directional systems are difficult to jam and relatively difficult to detect from standoff ranges, but they offer reduced bandwidth and come with line-of-sight limitations compared with plugging into landline networks. However, they do enable a battery C2 vehicle to coordinate the actions of its subordinate radars and TELAR/TELs within the broader network, provided that the C2 vehicle itself has access to a physical or other datalink connection with higher echelons of the system. Both Russian and Chinese made systems have the capability to fall back on less secure or lower bandwidth communications methods such as VHF radios, but these would likely be badly affected by a range of electronic warfare techniques on both sides of any likely conflict. They also offer significantly reduced capacity to support higher-level integration techniques such as cooperative engagements.[59] Electronic warfare techniques are also disproportionately effective in isolating tactical components, since these are closer to the front and can have their receivers suppressed, cutting them off from access to higher-level data, even if higher echelons can still receive data from the battery.[60]

One of the key dependencies in terms of integration is on the availability of real-time information on the location and activities of friendly or allied forces. For example, an individual SAM battery or even battalion might have a potentially superb capability to detect and engage air targets using the target acquisition and fire control radars held within the unit. However, if regular contact with higher C2 nodes is not possible then the operators would quickly encounter difficulties verifying that a detected contact was not a friendly or neutral asset, especially if the nation in question fields systems with old or lacks IFF systems.[61] Depending on the rules of engagement, this would either increase the danger of friendly fire or restrict the potential

57. Author interviews with operators familiar with a range of Soviet and more modern Russian systems, November 2021; technical assessment of captured Russian air-defence systems in Ukraine, during fieldwork, April 2022.
58. Author interviews with operators familiar with a range of Soviet and more modern Russian systems, November 2021; technical assessment of captured Russian air-defence systems in Ukraine, during fieldwork, April 2022.
59. Sam Cranney Evans and Thomas Withington, 'Russian Comms in Ukraine: A World of Hertz', *RUSI Commentary*, March 2022.
60. As experienced by Ukrainian air defenders using Russian-designed systems in the early stages of the Russian invasion, see Jack Watling and Nick Reynolds, 'Operation Z: The Death Throes of an Imperial Delusion', RUSI Special Report, April 2022, p. 2.
61. A Russian assessment of the Nagorno-Karabakh conflict, for example, noted that Armenia shot down five of its own aircraft after losing much of its command-and-control architecture in the opening stage of the conflict, see CAST, 'Vishla Kniga CAST "Burya na Kavkaz"' ['CAST Book "Storm in the Caucasus" Published'], 8 September 2021, <https://cast.ru/news/vyshla-kniga-tsast-burya-na-kavkaze.html>, accessed 24 April 2022.

capability of the SAM unit because they would not have access to an up-to-date recognised air picture for deconfliction purposes.

Figure 4: Sample of Methods of Network Connection



Source: Author generated

Missiles and Effectors

Modern IADS and CDCM complexes are made up of a variety of systems which can fire a range of missile types from very large, long-range and expensive weapons such as the 400km-class 40N6 fired by the SA-21 or P-800 Oniks and 3M22 Zircon that are currently fired or soon to be integrated on the Bastion-P to cheaper, shorter-range weapons such as the 9M317 missile fired by the SA-17 M1/2, or the KH-35 CDCM fired from the Bal coastal defence complex.[62] Long- and medium-range SAM systems rely on semi-active or active radar guidance, but short-range systems may use a range of radar-guided, infra-red (heat-seeking) guidance, laser beam riding, wire guided and optically guided missiles and firing modes. Semi-active radar guidance requires the target to be constantly illuminated by a fire control radar during terminal guidance, to give the missile seeker a source of reflected radar energy on which to home in. Track-via-missile-type systems work on a similar principle, but instead of processing the radar reflections and adjusting course itself, the missile uses a datalink to transmit what the seeker head sees

62. Jenevieve Molenda, 'Russian Army Accepts 40N6 Missile for S-400', Missile Threat, CSIS Missile Defense Project, 18 October 2018, <https://missilethreat.csis.org/russian-army-accepts-40n6-missile-for-s-400/> accessed 19 January 2022; *Global Security.org*, 'SA-17 GRIZZLY / Buk-M2', 13 September 2021, <https://www.globalsecurity.org/military/world/russia/sa-17.htm>, accessed 19 January 2022. On Bastion-P and Zircon, see Pavel Baev, 'Russian Nuclear Modernization: Real Issues and False Posturing', IFRI, 2019, p. 17.

back to the SAM system. The system then processes the data, which generates precise course corrections and broadcasts them back to the missile. Both systems have drawbacks, including the need to illuminate the target from a ground-based radar for extended periods, which makes them easier for hostile forces to detect and attack. Modern semi-active systems can employ tactics to reduce the need to illuminate the target from launch to impact, such as providing initial and mid-course updates on the target position by radio command link to the missile, and only illuminating the target during the terminal phase of the missile's flight. However, these still require a target acquisition radar or other sensors to be providing the system with high-resolution data about the target's location and track throughout the engagement.

By contrast, missiles with active radar homing seeker heads or infra-red seekers require only sufficient guidance information from launch systems to place the target within the acquisition range and field of regard of their own seeker, and from then on will guide themselves to the target with no further input from the launch system. There is less variation in the maritime domain. CDCMs such as the KH-35 and P-800 typically have active seekers and, increasingly, receive midcourse guidance and updates from GPS, GLONASS and Beidou, meaning that they can typically be used on a fire-and-forget basis.[63]

Western air and missile defence systems such as the Patriot PAC-2/3 and NASAMS, as well as most non-Western medium- and short-range systems tend to be equipped with a single type of missile. However, long-range Russian and Chinese systems such as the SA-21 and HQ-9 series of strategic SAMs feature TELARs with enclosed missile tubes which can carry and launch multiple types of missiles. For example, an SA-21 TELAR might have two 250km-class 48N6 series missiles taking up two of its launch tubes alongside eight cheaper, shorter-range and more agile 120km-class 9M96 series missiles quad-packed into the other two.[64] This arrangement allows these long-range SAM systems to save their missiles for targets that require their reach and performance, while using more plentiful and cheap ones for targets that are closer to the launchers. One of the important differences between older generations of A2/AD systems and the latest integrated architectures is in the much greater capacity of the latter to allocate fire missions to the most efficient potential shooters within range of a given target, and thus minimise the potential ammunition wastage and avoid unnecessary unmasking of the higher end assets which carry the most potent long-range missiles.

The ability of a modern IADS to fire multiple different types of missiles, sometimes from the same SAM system, greatly complicates efforts by opposing air forces to mitigate the threat that they pose at the tactical level. This is because semi-active, track-via-missile, active radar homing and infra-red seeking guidance all present aircraft with different levels of warning that they have been targeted and require different tactics and countermeasures to try and defeat once a missile is in the air. Taken on its own, each type of SAM system can be fought with tactics designed to exploit its weaknesses and neutralise its strengths. However, when different

63. Kaushal, Macy and Stickings, 'The Future of NATO Air and Missile Defence', pp.10–20.
64. *Global Security.org*, 'S-400 SA-21 Triumf – Missiles', 10 April 2019, <https://www.globalsecurity.org/military/world/russia/s-400-missiles.htm>, accessed 19 January 2022.

types of systems are combined in a layered, coordinated network involving short-, medium- and long-range missiles and sensors using a variety of guidance methods, the threat level is greatly increased and tactics that might reduce vulnerability to one system can increase the threat posed by others.

Combat Service Support

The combat persistence of an integrated defence system depends on a wide range of factors, but key bottlenecks can nevertheless be identified. In the absence of significant attrition against key nodes, radars and launchers, persistence will still be limited by the available stocks of missiles, supplies of fuel, spare parts and key operators. There is a significant temporal component to these different persistence bottlenecks.

For instance, the combat persistence within a tactical engagement is likely to be limited by the supply of ready-to-fire missiles loaded on the TEL and TELAR vehicles in the batteries which are within range of the target strike group or strike package. Reloading TELs and TELARs with missiles carried by reloading vehicles deployed with or near to the battery can often be accomplished in around 20–30 minutes depending on the system and crew.[65] However, especially in the air domain, this is still likely to be too slow to allow the reloading process to be completed in time to be used in the same tactical engagement which consumed the ready-to-fire supply. This is one temporal aspect of combat persistence, and one which allows attacking forces to estimate the number of ready rounds which a defence network can fire before a significant tactical window opens up as most launchers are reloaded. Commanders at the battery level up to division or army group command posts have a responsibility to make decisions on the balance between firing more missiles to increase the probability of kill (Pk) against each target and engage a greater proportion of a large incoming force, and tactics such as 'shoot-look-shoot-look' methods to conserve ammunition and thus increase tactical combat persistence. Equally, the supply of missiles also acts as a determinant of persistence in a longer timeframe, in terms of the number of rounds available in stockpiles and depots at various distances from the frontline, the number of resupply vehicles and crews available, and the attrition rate and tactical constraints imposed on that resupply apparatus. There is, therefore, an operational and strategic combat persistence bottleneck for defence systems based on the total usable stockpile of missiles available for the frontline to draw on during sustained combat operations.

In a similar vein, the availability and capacity of operators is a persistence bottleneck in both a tactical and the operational/strategic timeframe. At the tactical level, vehicle and sensor operators will become exhausted and need replacement or a stand-down period after a given number of hours at readiness to fire. The rate of fatigue will be higher in systems such as self-propelled SA-17 TELARs where operators work in cramped, noisy and more dangerous conditions than in systems such as Polyana C2 nodes where operators sit in more spacious, environmentally controlled and comfortable conditions further from the frontline. The proportion of total

65. Author interviews with operators familiar with a range of Soviet and more modern Russian systems, November 2021.

assets needed to generate the required level of coverage within the network will determine the impact and accumulation rate of crew fatigue in this sense, as well as what alert state can be maintained for sustained periods. At the operational and strategic level, attrition through enemy action against key nodes such as target acquisition radars and C2 nodes would have an outsized effect on overall combat persistence and effectiveness over time, compared to similar loss rates among TELAR operators, for example.

There is a slight but important difference between domains with regard to where operator pressures are likely to be most acute. The operation of key sensors, such as the Monolit-B of a Bastion-P system and the control of launchers, is held at the level of the brigade and naval headquarters respectively. This fairly top-heavy control structure makes it particularly viable to overload the central decision-making systems of a sea denial system, although it removes some pressures from lower-level operators. The challenge of coordination and deconfliction between air, maritime and coastal assets and the need to rapidly push data from long-range sources out to relevant shooters makes the task of headquarters particularly labour intensive and difficult to prosecute if placed under pressure.[66] Another difference is that whereas key sensor operators in air-defence architectures tend to be further removed from the frontline, helicopter borne ISR and other assets critical to coastal defences place a significant demand on crews and operators that can lead to fatigue and a degradation in effectiveness.

Fuel and spare parts availability and supply for vehicles are also an essential component of the combat persistence of an integrated defence system, as are food and water for crews. While this is the case for most military capabilities, the task of fulfilling these requirements for a sustained period of combat operations is complicated by several features of integrated defence systems. The first is that the sensor and shooter elements must be able to maintain consistent coverage due to the reactive and defensive nature of their task. The second is that survivability against SEAD/DEAD efforts by enemy forces requires the various elements of a defence system to avoid giving away their position as far as possible, and to relocate regularly both as a precautionary measure and after each engagement. The short- and medium-range elements of most defence networks in particular tend to be tracked to allow movement over rough ground comparable to armoured forces, and relatively compact, which limits the amount of fuel and spares that can be carried on each vehicle. Both increase the requirements for regular resupply and maintenance, but the regular movements of resupply and maintenance vehicles will create a signature which enemy forces can exploit to track or discover those systems. Again, commanders face a continuous trade-off as to how they balance optimising their survivability through concealment, emissions control and regular relocation movements with the desire to limit consumption of fuel, spares and the consequent need to call in and rendezvous with support elements in the field.

66. Kaushal et al., *The Balance of Power Between Russia and NATO in the Arctic and High North.*

II. Targeting A2/AD Architectures in Conflict

HAVING CONSIDERED THE structure of A2/AD architectures, their capabilities and dependencies, this chapter considers how to go about degrading them to enable theatre access. In doing this it is first necessary to have a clear appreciation of the expectations of what can be achieved and what constitutes a desirable end state. The chapter therefore begins by outlining the levels of system effectiveness. The second section examines the principles for activity attacking an integrated system if incremental effects are to achieve more than attritional results. The third section considers the primary targets in the system and the mechanisms for engaging them.

Levels of Systems Degradation

While there is no paucity of military literature on degrading an opponent's systems, the concept of systems degradation and systems theory tends to be viewed very narrowly by militaries. A good deal of the literature on cybernetics by early theorists such as Norbert Wiener laid out general principles regarding the degradation and collapse of systems that have not often been retained in military thinking.[67] Specifically, in both Western and non-Western military thinking, systems destruction tends to be conflated with finding the 'exhaust shaft on the death star': the destruction or disruption of key nodes which will cause the collapse of the system as a whole. While identifying critical nodes in a system is indeed important, in systems theory it is subordinate to a wider phenomenon: the feedback loop.[68] Because the interaction of the parts of a system creates an emergent phenomenon – something more than the sum of its parts – its behaviour is more complex than would be assumed if analysis was confined to assessing each component in isolation. Take, for example, the oft-cited example of a financial bubble: something that is the aggregate effect of small changes in the behaviour of individual actors that produces a disproportionate distortionary effect across the financial system as a whole. The success or failure of a system depends not on the destruction of key nodes in a modern-day blitzkrieg, but rather by the imposition of inefficiencies, frictions and the achievement of behavioural effects across the system that collectively have a non-linear impact on its functioning.

In practical terms, A2/AD architectures have optimal and sub-optimal operating protocols. For example, coastal defence systems can opt for dispersed attacks (hit-and-run raids with few missiles), sequential attacks and massed salvos coordinated from a range of ground, sea

67. Norbert Wiener, *Cybernetics: Or the Control and Communication in the Animal and Machine* (New York, NY: Quid Pro, 2013).
68. Wiener, *Cybernetics*, pp.100–150.

and subsurface assets.[69] From the point of view of overwhelming an opponent's systems, massed salvos are the most logical choice. However, actions by the attacking side might lead a defending force to opt for sub-optimal response methods. For example, if defenders believed that communications across their system exposed them to adversary ELINT targeting, they may opt to limit their transmissions and thus forgo the benefits of seamless integration within the wider network. Similarly, if a force believed its capacity for either classifying targets or conducting battle damage assessment was compromised, it might be incentivised to avoid launching massed salvos for fear of expending its magazines without achieving sufficient effects. A lack of trust in one's own systems, magnified by an opponent, can often cause pathological behaviour, as exemplified by Iranian and Syrian air-defence units destroying allied and civilian aircraft respectively in 2018 and 2020.[70] Another example of the impact of operator perceptions is the relative caution that the very presence of CDCMs has induced in the deployment of naval assets.[71] This is in spite of the fact that when they have come under direct attack, large surface vessels have often defeated CDCMs.[72] Nonetheless, it is now felt necessary to deploy assets in larger groups to account for the risk posed by CDCMs, which strains force structures, readiness and the flexibility of the naval instrument.[73] One might also consider the inordinate caution showed by Soviet submariners after the revelations of the Walker spy ring.[74]

The thread uniting all these examples is that a change in subjective risk perception led to alterations to individual tactical decisions, which changed the behaviour of operators and, thus, limited the effectiveness of the A2/AD architecture. In the air domain, defenders might opt to engage targets as individual systems using 'pop-up' tactics if emitting radars or command posts communicating with units are likely to be readily identified and promptly struck by an attacking force. If operators can be induced to distrust their systems – and this distrust can be exploited and magnified – this can lead to individual changes in behaviour that can have aggregate system-wide effects. Similarly, the allocation of air-defence assets could be shaped by a wider range of factors. For example, a major feature of Russian thinking about aerospace attack and defence is a (perhaps exaggerated) memory of NATO's strike campaign against Serbia which, per Russian thinking, paralysed the nation's critical military and civilian infrastructure

69. Wayne P Hughes Jr, *Fleet Tactics and Coastal Combat*, Second edition (Annapolis, MD: Naval Institute Press, 2000).
70. Barbara Starr, Ryan Browne and Nathan Hodge, 'Syria Accidentally Shot Down a Russian Military Plane', *CNN*, 18 September 2018; Matthew S Schwartz, 'Iran Report Details Chain of Mistakes in Shooting Down of Ukrainian Plane', *NPR*, 12 July 2020, <https://www.npr.org/2020/07/12/890194877/iranian-report-details-chain-of-mistakes-in-shooting-down-ukrainian-passenger-pl?t=1646152693530>, accessed 1 March 2022
71. Bryan Clark, Mark Gunzinger and Jesse Sloman, 'Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance', CSBA, 2017, pp. 5–6.
72. J C Schulte, 'An Analysis of the Historical Effectiveness of Anti-Ship Cruise Missiles in Littoral Warfare', thesis, Naval Postgraduate School, September 1994.
73. Clark, Gunzinger and Sloman, 'Winning in the Gray Zone', pp. 5–6.
74. Peter Hennessy and James Jinks, *The Silent Deep: The Royal Navy Submarine Service Since 1945* (London: Penguin, 2016).

from standoff ranges.[75] If Russia needs to divide assets between the defence of infrastructure and forward forces, an information campaign to exploit Russian fears of an imminent NATO attack on its critical national infrastructure, coupled with the posturing of assets equipped with prompt strike capabilities could lead to a sub-optimal allocation of air-defence assets, potentially denuding the forward edges of an IADS.

In effect, the aggregate impact of a range of actions on how a system *behaves* is of greater significance than the destruction of individual system nodes. This is not to ignore the importance of mapping the nodes that comprise the system, but merely to point out that operational paralysis through the judicious targeting of points of failure in systems warfare – both Western and non-Western – is generally only an ideal. In practical terms, a more useful objective is to shift system behaviours to degrade its ability to function as intended.

When one considers the objectives therefore in targeting an A2/AD architecture this may be framed as degrading the system sufficiently to bring about three stages of behavioural change, each of which reduces the threat and increases access to the operating environment. The first level of behaviour may be understood as the system working optimally as an integrated and mutually supporting network, with overlapping situational awareness, motivated crews and sufficient stockpiles of munitions. Under these circumstances the system can be wielded proactively to collaboratively engage targets and thereby prevent access to the area being protected or at least impose a heavy level of attrition on enemy assets operating within their range. As pressure is imposed on different parts of the network, however, the system must begin to manage its signature, conserve ammunition, and increase its tempo of displacement. All these activities increase the strain on crews and constrain overall system output. As more activity is reported, information must be passed between more nodes, while movement induces fewer channels for communication being available. At a certain level of pressure, the system is likely to degrade gently to what might be considered a stressed state in which fewer assets are available to engage targets and operators may choose not to engage marginal targets of opportunity, or at least conduct engagements sequentially rather than en masse. As attrition and pressure mounts further, uneven supplies of munitions and fuel, degradation of the radar picture and the loss of key command links begins to break apart the integration of the system. At this point, many of its components will begin to operate as independent entities, rather than collaboratively. This may be considered the system functioning in a degraded state. Its components are liable to begin to conduct pop-up engagements but are no longer able to coordinate their actions as a multi-layered network. While dangerous, the scope to isolate and overwhelm each threat increases the level of suppression of the system as a whole. As the willingness of isolated launchers to illuminate and engage diminishes, the level of suppression increases. The object of degrading an A2/AD architecture, therefore, is to stress the system into this third behavioural pattern and thence to sustain its suppression as the theatre is penetrated.

75. Dave Johnson, 'Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds', Livermore Papers on Global Security No. 3, Lawrence Livermore National Laboratory Center for Global Security Research, February 2018.

Principles Underpinning System Degradation

In order to bring about the degradation of the system, it is necessary that effects are consistently applied in accordance with key principles. Before detailing the methods for degrading the system therefore it is worth outlining how those methods ought to be orchestrated. The three guiding principles for planning the degradation of A2/AD architectures are simultaneity, persistence and at an escalating tempo. The thread that runs through these principles is that a system should be prevented from operating on its own terms at every stage of competition, with the methods of achieving this spanning pre-conflict erosion to overwhelming the system as the tempo of activity escalates. Pre-conflict activities will be addressed in the next chapter.

Simultaneity

This is perhaps the most critical of the three guiding principles, because modern A2/AD architectures – layered, mutually supporting elements comprising a wide variety of different systems and nodal points with significant redundancy – have a high degree of inherent capacity to deal with pressure against individual component parts or processes. Success in forcing a significant degradation of capacity requires either overwhelming force or, more practically for most states, the ability to simultaneously apply pressure from multiple attack vectors against specific elements of the system. Very often this will generate multiple dilemmas for the operators at the tactical level between guarding against simultaneous but different kinds of threat. Simultaneous actions should therefore aim to bring about conflicting imperatives.

The imposition of multiple, concurrent dilemmas on a system is a critical precondition to operational shock: the degradation of a systems' functions to the point where it no longer fulfils its assigned task, even if its components have not been individually attritted.[76] Examples of this might include the Soviet destruction of the Kwantung Army in 1945 where multiple convergent attacks effectively led to the army's decomposition into individual formations which, while tactically formidable, lost their ability to function at the operational and strategic level.[77] At sea, one might consider how the Reagan-era maritime strategy, which saw a combination of more aggressive Atlantic ASW and forward submarine patrols to menace Soviet SSBNs, had the effect of dislocating Moscow's planning for undersea warfare.[78]

The principle of simultaneity revolves around presenting a system with multiple vectors and tiers of attack. For example, sectored radar systems can be held at risk if attacks can be conducted from more than one vector, as Saudi defenders discovered during the strikes on Abqaiq and

76. Shimon Naveh, *In Pursuit of Military Excellence: The Evolution of Operational Theory* (New York, NY: Frank Cass, 1997).
77. Naveh, *In Pursuit of Military Excellence*, p. 238.
78. John B Hattendorf and Peter M Swartz (eds), *US Naval Strategy in the 1980s: Selected Documents* (Newport, RI: Naval War College Press, 2008).

Khurais.[79] As the defenders' radar was set up to intercept threats from Yemen, they were not prepared for a salvo from the north. Similarly, attacks with four loitering munitions from multiple angles have been demonstrated to overwhelm even the most modern point defence systems.[80] Although the sectored nature of radar systems can be overcome through networking, this still requires the division of assets to cover multiple threat vectors if, for example, fires from both land and sea can strike targets. This in turn raises the possibility of assets being spread thin and thus overwhelmed on any one vector.

Converging attacks across multiple tiers represent a parallel challenge. Because the components of a system typically contend with specific threats, the coordinated employment of multiple threat types can overwhelm a system or exploit the seams within it. For example, in 2016, a small North Korean UAV was discovered crashed near the AN-TPY2 radar on which the US THAAD batteries in South Korea depend.[81] The UAV had overflown the radar without being detected and classified as a potential threat and, had it been armed, could have damaged it. To be sure, opponents can and do develop layered systems against multi-tiered threats. Russia, for example, has developed both robust EW capabilities and lower tier defences such as the SA-22 Pantsir-S to cope with UAVs. However, the requirement to add complexity to a system by, for example, coordinating upper and lower tier interceptors or hard and soft kill measures while avoiding complications such as fratricide is testing. By way of an analogy, PLAN scholars conducted an exercise to model how to overwhelm an Aegis destroyer – itself effectively an IADS at sea.[82] Their model suggested that approximately seven missiles – six cruise missiles on different flight paths and one ballistic missile – would overwhelm the command system of the destroyer if they arrived nearly simultaneously, due to the concurrent tracking and engagement challenge posed.[83] The greater the complexity of one's attacks, and the higher their tempo, the greater the likelihood of a collapse in a system's capacity to switch focus rapidly enough to cope with new threats. As such, for example, the risk posed by an attack comprising cruise missiles, ballistic missiles and UAVs is not so much that each threat cannot be dealt with by a layered IAMD system but that coordinating an efficient and coherent response to such varied threats concurrently is almost impossible. When dummy attack runs, jamming, severing of communication links, mining of resupply routes using infiltrated saboteurs, and other effects are added to the kinetic attack, the effect on the defender can magnify as cognitive load, concurrent tasks and conflicting imperatives generate slow and sub-optimal responses. When planning attempts to strike targets within an A2/AD architecture, therefore, attacks should

79. Presentation by Uzi Rubin at the RUSI Space and Missile Defence Conference 2020, London, 27 February 2020.
80. Kaushal, 'The PLA's Continued Emphasis on Subsonic Cruise Missiles'.
81. Tom Karako, *Distributed Defense: New Operational Concepts for Integrated Air and Missile Defence* (Washington DC: Center for Strategic and International Studies, 2018), pp. 1–10.
82. Yang Zhongxin et al., 'Analysis of Anti Ship Missile Saturation Attack Capability of the Arleigh Burke Missile Destroyer', *Modern Defence and Technology* (Vol. 30, No. 3, 2002), pp. 1–5, <http://www.defence.org.cn/aspnet/vip-usa/uploadfiles/2006-1/20061313144410.pdf>, accessed 4 May 2022.
83. *Ibid*.

comprise multiple simultaneous and converging actions from as many domains as possible, including cyber and information effects.

Persistence

Persistence is also a vital principle for successful degradation of A2/AD architectures. This is because the challenge posed by any attempt to quickly achieve permanent destruction of the defence network is likely to be beyond the military resources or political permissions available to commanders in most scenarios. As such, the inherent threat from these A2/AD architectures will remain a major planning and operational constraint for some time. This means that the ability to achieve simultaneous effects against enough of the system to cause its capability to degrade must be sustainable over time rather than a collection of one-shot capabilities which can be marshalled for a single overwhelming DEAD strike. Furthermore, many of the most important pressure points on the system – especially cognitive load and strain on operators – will dissipate if pressure is eased but can magnify as the duration of the threat persists. The system will reorganise itself to fix damaged network connections, close gaps in radar coverage, and can thereby move up as well as down the levels of effectiveness previously discussed. Persistently harassing the architecture prevents its recovery and maintains suppression.

It may seem that there is a conflicting imperative between the need to conduct simultaneous activities in all domains to achieve effective returns on resource investment in terms of the effect on the system and the need to persistently operate for a sustained period. One activity is resource intensive, the other demands that resources can be preserved. The key point here is to demonstrate the potential to strike at multiple depths and from multiple domains persistently, while following through with actual attacks when they can be synchronised. For example, loitering munitions are a serious threat to many components in an A2/AD architecture. They are also expensive and a force will have a limited number of them.[84] If a force has conducted a successful initial strike that – alongside other attack vectors – used loitering munitions, a fact amplified in information exploitation activities, enemy operators know that they are a potential hazard in the environment and will be looking for them. If the initial attack is followed up with persistent but intermittent flights of cheap UAVs flying low-altitude, pre-programmed routes, but without a seeker capability, the enemy must investigate whether or not these are loitering munitions. If they choose to ignore them without investigation, they risk being surprised. If instead – as they will – the operators exert considerable energy into tracking and classifying low-flying, small and difficult to detect targets, they will be tired, distracted and stressed for a sustained period. This will also limit their capacity to do other things. The persistent push by naval vessels and aircraft into range of their systems, but not into the no-escape zone, similarly creates a continual pressure, setting a pattern that can be broken when the next salvo of simultaneous actions is pressed home. Another example might be following up a special forces

84. Justin Bronk, 'Swarming Munitions, UAVs and the Myth of Cheap Mass', in Justin Bronk and Jack Watling (eds), *Necessary Heresies: Challenging the Narratives Distorting Contemporary UK Defence* (London: Routledge, 2021), pp. 49–60.

raid against a system with the tripping of perimeter sensors using cyber capabilities so that the defenders are forced to react in anticipation of multiple dispersed follow-up raids.

Another way in which persistent effect can be delivered is through the use of long-range strike systems to hold large parts of the force – including multiple echelons – at continual risk. Even if these are rarely fired, the fact that they can be disperses effort and produces a continual planning constraint that over time can become a cognitive barrier to generating certain options on the part of the defender. By their very presence and theoretical capacity to strike both tactical and strategic target sets, the deployment of such strike assets may force resource trade-offs on the part of defending forces. The ability to target multiple echelons to which components of an A2/AD system correspond simultaneously, as well as to attack the external targets which the system either depends on or is obliged to provide defensive coverage for is thus important in presenting persistent pressures to the defender. The activation of peripheral cyber penetration in higher echelon networks – even if they were of negligible impact on the system's functionality – for instance, can similarly force the defender to assure their networks, which can be a laborious task for a dispersed, deployed system. If the defender decides not to assure its network then information effects can subsequently ascribe system failure to such cyber penetrations, persistently eroding trust among the defenders in between kinetic strikes.

Escalating Tempo

This reflects how as the A2/AD architecture degrades, the efficiency of the system decreases and the threat it poses is diminished. The attacker can therefore increase the tempo of effect delivered as the relative resource intensity required to bring about results shifts in their favour. This requires changes to permissions and authorities that recognise the levels of degradation thus far achieved. Failing to capitalise on the degradation of the network risks it being reformed. Thus, as the attacker determines that the network has been degraded, they must follow this degradation with a change in their rules of engagement, planning assumptions, risk tolerance and objectives.

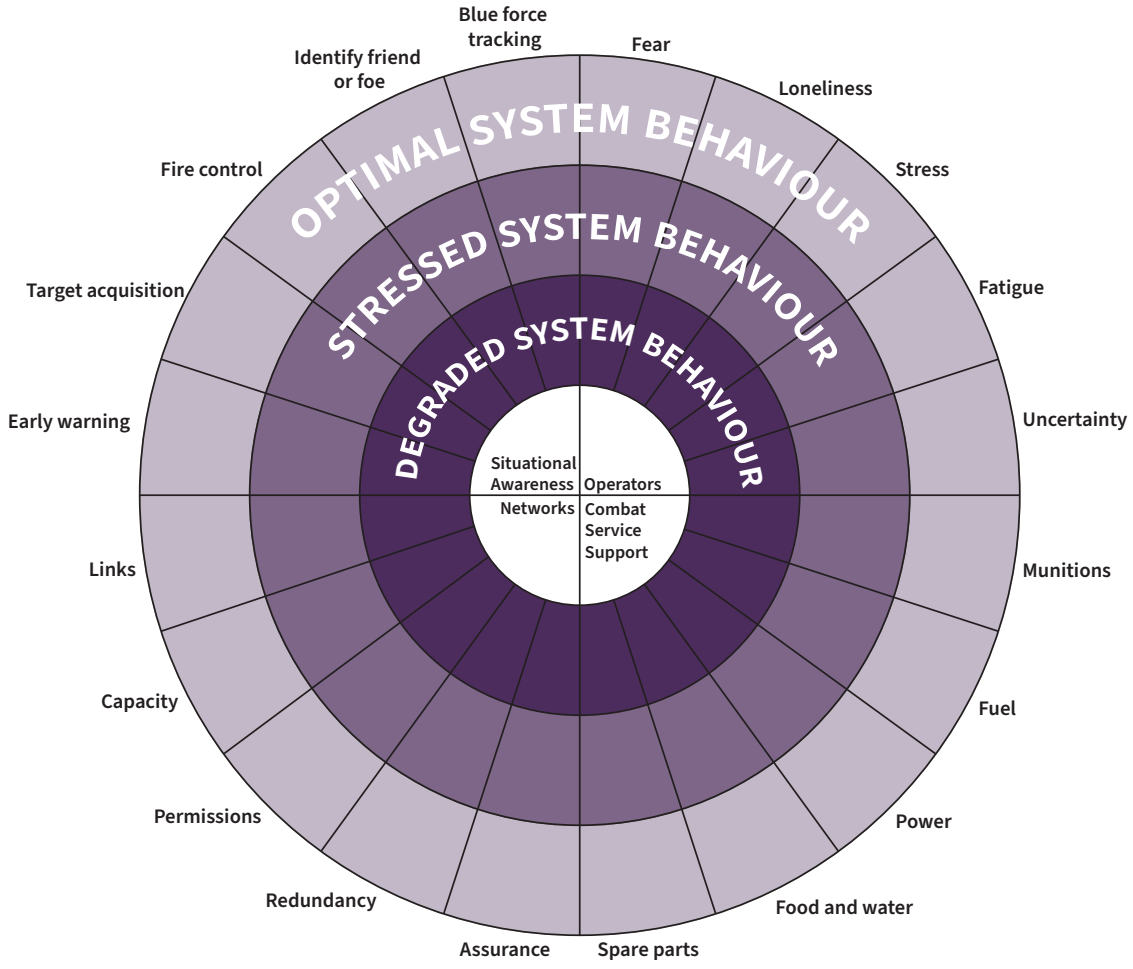
The escalation of tempo is not just about preventing the enemy from recovering, but also because the intention of degrading an A2/AD architecture is to enable theatre entry and ultimately the use of close air support, naval strike and resupply in aid of securing key objectives. This must be accomplished within a short timeframe. Thus, advances made in penetrating the enemy's defences must be followed up, exploited and capitalised on. Suppressing the A2/AD architecture is not therefore an end in itself but a prerequisite of wider operational success. As has already been explained, however, suppression is very unlikely to mean total destruction. Pop-up threats will still pose a significant problem for amphibious shipping, air resupply, or for aircraft optimised for ground attack supporting land forces.[85] If the force is not to experience significant attrition in this phase, harassment and suppression of the A2/AD architecture must continue until theatre entry has been secured. Having established these principles to building a joint effects campaign against an A2/AD architecture, and defined the end-state sought, it is

85. As seen during the early phases of the Russian invasion of Ukraine, February–March 2022.

now necessary to consider the range of effects that can be applied against the groups of targets outlined in the previous chapter: the system's situational awareness; personnel; connectivity; and endurance.

Primary Target Categories and Potential Effectors

Figure 5: Effects and Targets



Source: Author generated

Information Inputs

A key starting point in any effort to degrade the effectiveness of an A2/AD architecture is to target the key mechanisms through which it gathers information in order to build situational awareness and control engagements. This is perhaps easier to accomplish in the maritime domain due to the limitations imposed by the radar horizon, which mean that even if placed in elevated positions, systems such as the Bastion-P CDCM complex cannot classify and target

surface vessels using their organic radar at ranges beyond 40–80 km.[86] At longer ranges, these systems rely on support from airborne assets such as the Ka-31 helicopter or the Forpost UAV that are significantly more vulnerable to jamming or destruction.[87] The Russian navy also plans to use vessels such as the Project 22160 Corvette in an ISTAR role.[88] Though stealthy, these vessels are lightly armed and might be destroyed by a number of means. The more pressing question for navies is not how to destroy sensors which provide fire control for CDCMs, but how to do so without incurring disproportionate costs. Shooting down a helicopter, for example, with an interceptor from an air-defence destroyer is both costly and liable to reveal the position of the destroyer. A variety of tools, from forward-positioned littoral forces with soft kill tools, or unmanned surface or subsurface vessels operating in an anti-air or anti-surface role might fulfil this function.

At longer ranges, anti-ship ballistic missiles are likely to rely on satellite constellations supported by OTH backscatter radar. China's DF-21D, for example, will receive target coordinates by triangulating information from its NOSS satellites and its OTH radar at Jiangfan in order to cue in the SAR satellites that form part of its Yaogan constellation.[89] Even with effective cueing, this could take several hours and the disruption of space-based assets through electronic attack could make this harder still. States such as Russia, which have less well-developed space-based ISR, given the lack of progress on its Liana and Persona ELINT and EO constellations, will likely need to rely on maritime patrol aircraft, including the IL-38N. Russia, despite claims made by its military, fields only 16 operational IL-38Ns,[90] which are also needed for a range of other tasks and are themselves vulnerable to being shot down by task group missiles or supporting combat air patrols. The task of complicating information gathering is thus likely easier against ASCMs than it is against a modern IADS.

The primary early-warning, wide-area surveillance and target acquisition radars within an IADS are not as easily suppressed, since they do not need to be forward positioned to detect targets except for those flying at very low altitudes. That said, the need to actively transmit to build up active situational awareness for the broader IADS will allow relatively rapid triangulation of the locations of the main surveillance and target acquisition radars by an attacking force.

For large fixed OTH arrays such as the Russian 29B6 Container, which provides advanced warning of any attacking force's rough movements, long-range precision strike using Tomahawk land

86. Range determined by the height above sea level of the radar and ship superstructure respectively.
87. Michael Kofman, 'Russian Maritime "A2/AD": Strengths and Weaknesses', *Russia Military Analysis*, 29 January 2020, <https://russianmilitaryanalysis.wordpress.com/2020/01/29/russian-maritime-a2-ad-strengths-and-weaknesses/>, accessed 1 March 2022.
88. Kaushal et al., *The Balance of Power Between Russia and NATO in the Arctic and High North*, p. 46.
89. Heginbotham et al., *The U.S China Military Scorecard,* pp. 157–65.
90. BMPD Journal, 'Na Severnom flote vosstanovleny dva aviatsionnykh polka' ['Two Naval Aviation Regiments Restored to the Northern Fleet'], 3 December 2019, <https://bmpd.livejournal.com/3860313.html>, accessed 10 May 2021; Frederick Westerlund, Johan Ingval and Susan Oxenstierna, *Russian Military Capability in a Ten Year Perspective 2019* (Stockholm: FOI, 2019), p. 71.

attack missiles (TLAMs) fired from naval assets, or Storm Shadow air-launched cruise missiles, could technically provide a potent attack vector. However, in practice, political constraints would likely prevent kinetic strikes on these assets since they are generally not only situated deep within a hostile state's territory but in the case of Russian systems also form a key part of the nuclear early-warning chain. This means that the escalation dynamics around any attack on these systems are highly unpredictable and potentially mutually apocalyptic.

On the other hand, the fixed and mobile wide-area surveillance and target acquisition radars which feed an IADS with its primary situational awareness inputs are critical points in the network and need to be put under sustained pressure during any SEAD/DEAD operation. This is partly because suppressing or destroying these key sensors offers perhaps the most dramatic potential gains in terms of IADS capability degradation out of any target set. However, it is also because as the primary source of operational situational awareness, any successful effort to manipulate the data which these radars are seeing will have outsized effects across the rest of the network. Most modern target acquisition radars, such as the Russian 91N6 Tomb Stone, RLM-M Nebo-M and 9S15M Obzor-3 and Chinese Type 305A/B, are mobile, and as such are difficult to reliably hit with weapons fired from significant standoff ranges given the time in flight over the considerable distances that must be covered.[91] To be sure, this assumes that operators are behaving efficiently, but given the centrality of both air defences and sea denial systems to the warfighting plans of peers, the assumption that the troops manning these capabilities are effective is a sensible starting point, with viable attack options expanding as operator behaviour deviates from best practice. Even under optimal operational conditions there is still potential value in such attacks as part of a wider effort to put pressure on the system since if multiple target acquisition radars have to pack up and drive to alternative sites to avoid incoming missile strikes, they will be unable to perform their function during transit and so gaps in the wide-area coverage of the network as a whole may be opened. Furthermore, forcing these high-level assets to move between pre-identified deployment sites may create opportunities for other attack vectors. Examples could include laying SCATMIN fields by rocket artillery along likely transit routes or timing sorties by penetrating stealth assets such as F-35s to hunt them down during the window in the network's most potent frequency-agile sensor coverage created by the standoff missile launches. While escalation concerns or layered point defence systems might make kinetic strikes against these radars difficult in some circumstances, they are a high-gain target for protocol-based electronic attacks, for example. This is because if it is possible to induce these key information nodes to feed false or confusing data into the wider network, it will create significant confidence, assurance and capacity issues for system operators in subordinate layers of the system. Such an effect would be multiplied if it could be exerted at the same time as more traditional attacks.

When an IADS is functioning as intended, the battalion and battery-level target acquisition and even fire control radars also contribute to the overall situational awareness picture of the network. However, their effectiveness as a source of wide-area situational awareness within

91. For example, see *GlobalSecurity.org*, '64N6 / 91N6E - TOMBSTONE / Big Bird', 23 April 2018, <https://www.globalsecurity.org/military/world/russia/tombstone.htm>, accessed 2 March 2022.

the network will depend to a significant extent on what type of SAM complex the unit in question is operating, as well as where in the battlespace it is sited. When able to rely on situational awareness data from higher echelons to cue their organic fire control radars for engagements, the organic target acquisition radars at battery level may well choose to reduce their signature by remaining passive for most of the time. Thus, attacks on higher echelon surveillance and target acquisition radars will have the effect of forcing those at battery level to illuminate and make themselves easier for attackers to identify and target, especially since they are likely to be located relatively close to the frontlines. This might also be achieved if an opponent manoeuvres beyond the range of effective integration. Air-defence assets with ground forces may face this, as will maritime assets, with the PLAN in particular struggling with the challenge of C2 at expeditionary reach.[92] Radar operators in medium- and short-range SAM units are open to a wider range of attack vectors than those sitting at higher echelons due to their proximity to enemy forces and the need to illuminate to control engagements in the face of enemy action. They are also unlikely to have the same degree of protection against incoming munitions from short-range point defence systems as higher echelon radar systems. As such, their capabilities can be degraded through multiple, ideally simultaneous, points of pressure. At the most traditional and simplistic level, loitering munitions and more traditional missiles, such as the AGM-88 HARM fitted with anti-radiation seekers that home in on radar emissions, can be fired either reactively or pre-emptively to force operators to choose between illuminating their radars to engage incoming threats and risk destruction or stay passive to stay safe but be unable to effectively engage other targets.[93] Even a few loitering munitions in the battlespace can force radar operators to waste considerable search and interrogation capacity chasing fleeting radar returns among the ground clutter. This may be inconsequential until it coincides with infiltration by stealth assets on the periphery of that radar's potential detection radius or a salvo of traditional munitions launched from outside the battery's range.[94] The use of decoys and stand-in jammers alongside kinetic munitions can also impose considerable sensor confidence or saturation challenges on SAM battery sensors, which face the choice of potentially wasting their ready-to-fire missiles on false targets or poor-Pk shots or risking destruction by not engaging said potential threats.[95] If situated close enough to the frontlines to protect the forward echelon of troops, short- and medium-range SAMs may also become seriously vulnerable to destruction by artillery fire called in by special operations forces or standoff/penetrating stealthy ISTAR assets. Since most are only lightly armoured and the radars that they carry are vulnerable to blast and splinter damage, this is a major potential weakness at the forward edge of an IADS in a joint engagement context.[96] The trade-offs between keeping a

92. Kimberly Jackson et al., *Command and Control in U.S Naval Competition with China* (Santa Monica, CA: RAND, 2018); Thomas Withington, 'When They Sounded the ALARM', *Armada International*, 4 March 2021.
93. Dan Hampton, 'The Weasels at War', *Air Force Magazine*, 1 July 1991.
94. Withington, 'When They Sounded the ALARM'.
95. Tyler Rogoway, 'Recent MALD-X Advanced Air Launched Decoy Test Is a Much Bigger Deal Than it Sounds Like', *The Drive,* 24 August 2018.
96. This was demonstrated repeatedly in the opening advance by Russian ground forces during the invasion of Ukraine, as Russian columns frequently outran the coverage of their primary air-

system survivable and ensuring that it meets its goal can lead to cross-component friction if the forces a SAM is meant to be protecting believe they are not being supported. One might think of Admiral Richmond Turner's withdrawal of the USMCs air cover in the Battle of Guadalcanal as an example of how a supporting force, attempting to protect itself, can find itself at loggerheads with those it is meant to be protecting.

Attrition of standalone radars at battery level on the edges of an IADS is likely to be relatively easy to achieve over time for a joint force, at least in comparison to the objectively higher-value radars held at higher echelons. Due to the presence of numerous TELARs, it is unlikely that such efforts can have a decisive effect on their own, but pressure on each part of the sensor network will increase the pressure on those at other echelons to illuminate in a sustained way and on aggregate will increase vulnerability and reduce effectiveness. Furthermore, forcing the system to adapt as radars at various echelons are destroyed, suppressed or forced to relocate will also increase the reliance on low-latency communications between the remaining active sensors, the C2 nodes and fire control/launch units at the battery level. Concurrent pressure on these communications links would thus increase the degradation impact of radar suppression, spoofing and destruction across the network. Such pressure on integration links is likely to be an objective of any SEAD/DEAD campaign since these links represent another key target set.

Connectivity

As terms such as 'integrated air and missile defence system' imply, integration across multiple layers of sensor, C2 and shooter elements is the key that allows modern A2/AD architectures to project such a qualitatively greater threat than previous generations of systems. It follows implicitly that if an attacking force can disrupt the connectivity which allows the architecture to function as a coordinated whole, its combat effectiveness will rapidly degrade.

There are critical integration nodes which, if at all possible, should be identified and targeted, even if the cost is likely to be high in terms of potential losses incurred in return. These are the top echelon mobile C2 nodes such as the Polyana-D4, which acts as a data fusion and coordination hub for strategic level ISR, very long-range SAM complexes and joint force integration and the 55K6 and 9S457 command vehicles embedded within very long-range SA-21 and SA-23 units, respectively.[97] These nodes will be difficult to identify and target from standoff compared to the radar nodes, which must actively transmit, or even the TELs and TELARs, which unmask themselves when they launch missiles, since when connected up to ground links they can operate without generating a significant signature. They also resemble trucks and/or tracked utility or support vehicles when on the move so are difficult to pick out. However, if these nodes can be found and destroyed, they are not only a critical node that would then be out of action but are also comparatively scarce assets which are difficult to quickly replace. Even more importantly, if these targets can be destroyed kinetically, the likelihood is that their crews

defence assets, leaving them vulnerable to attack by Ukrainian aircraft and UAVs. See Bronk, 'The Mysterious Case of the Missing Russian Air Force'.

97. For more details, see Bronk, 'Modern Russian and Chinese Integrated Air Defence Systems'.

of highly trained operators and senior commanders will be killed or wounded in the process – thus depriving the defence system of an asset that is even harder to replace or backfill than the vehicles and their equipment.

A less challenging but iteratively potentially highly effective vector for targeting the system's connectivity first requires mapping pre-positioned SAM sites. These are cut and laid long ahead of conflict and can often be identified by their tell-tale layout of tracks, enabling the SAMs to move quickly from their hides to firing positions (figure 3). Across these sites will be attachment points where field cables can be plugged into ground laid cable networks. The ground laid cables are hard to detect, but by mapping the SAM sites it becomes possible to understand what is being connected. Terrain features and observing them during exercises can also provide an indication of where pre-positioned links are for radar, since these sites will be occupied during training. The number of terrain features that give good radar coverage will be limited and these can also be mapped pre-conflict to determine likely targets. For example, terrain elevation along Iran's coastline means that the portions of the coast that can actually be used to position CDCMs and their supporting radar are more limited than a glance at the map might suggest.[98]

Figure 6: Example of a Pre-Prepared Long-Range SAM Site

Source: Google Earth Image capture from presentation given by Igor Sutyagin at RUSI, May 2017.

Once a list of likely locations has been identified, it may become possible to infiltrate teams into these areas before they are occupied and either sabotage the connection boxes or sever the ground cables. Ideally this can be done in a manner that produces a major troubleshooting effort, such as putting adhesive into the female socket for the field cable connector. Where lines of connection can be determined through covert reconnaissance pre-conflict, or through

98. Caitlyn Talmadge, 'Closing Time: Assessing the Iranian Threat in the Strait of Hormuz', *International Security* (Vol. 33, No. 1, 2008), pp. 82–117.

standoff techniques, these can be bombed using long-range precision strikes and thereby damaged. Alternatively, such links can be sabotaged by penetrating reconnaissance troops. Such activities can also contribute to terrain analysis, which can illuminate details regarding where systems such as radar can be effectively placed.

The purpose of destroying ground links is to force the systems to revert to their alternative or contingent communications procedures. Not only does this reduce the available bandwidth and increase their signature, but it also makes them vulnerable to more standoff techniques. Radio communications between dispersed units can be subjected to jamming. This could constitute longer-range electronic warfare, which must be directional and must therefore maintain alignment, or dirty jamming, which needs to be done from a shorter range but can have an area effect and therefore does not require the current location of a vehicle to be precisely identified. The purpose of such jamming is to overload the receivers on the communication system, thereby isolating the vehicle from inbound communications. This could be achieved from dedicated land platforms, ships with electronic warfare suites, pods on aircraft, or in the case of dirty jamming could be delivered as a sub-munition with rocket artillery, distributed by UAV, or placed by penetrating reconnaissance teams. These effects can only be maintained for a limited period of time. Directional jamming will not work once the adversary has displaced, unless their location can be tracked, and will be constrained by the endurance of the platform delivering it. Dirty jamming is limited by the available power supply. One advantage of deployable jammers is that the enemy must either move their position or else find and disable the devices, which is exceedingly burdensome on personnel. The use of distributed arrays of jammers can account for target movement in certain circumstances.[99]

Micro-links and other line-of-sight connections are difficult to jam, but their short range means that they only enable connectivity within rather than between tactical units.[100] However, for short windows these capabilities can be disrupted by targeting the site with white phosphorous or other multi-spectral smoke that breaks the line of sight between vehicles. Such effects may only be short in duration but if deployed immediately preceding an attack could disrupt the mutual support within a tactical unit. For those vehicles that might be pushed forwards, such as SA-17, sponsoring railway workers and others who might get access to them to surreptitiously damage the somewhat fragile micro-link antennae could also increase the level of friction within unit communications.

Another class of attack against the communications of an A2/AD architecture targets the assurance of its data. Suppose, for example, a penetrating reconnaissance team could find a buried cable, running from a forward tactical unit back into hostile territory. By attaching a device to this cable, it may be possible to inject information into it. Israel has repeatedly done

99. Clark, Gunzinger and Sloman, ‘Winning in the Gray Zone’.
100. Author interviews with operators familiar with a range of Soviet and more modern Russian systems, November 2021.

this to Hizbolluh's ground laid fibre optic cables which it uses for C2.[101] Although Hizbullah runs line checks that have detected these devices, the use of booby traps and other techniques can slow and disrupt assuring these cables. Moreover, corrupted data needs only to be pushed into the system for a short period to cause serious problems as misleading information cascades through the network. If links are subsequently severed this can leave isolated parts of the network holding residual corrupted data. This sort of misleading information creates trust issues throughout the system and therefore degrades confidence and dependence on communications, often requiring that messages be received from multiple channels, and thereby slowing the efficiency of the network. At sea, states such as Russia have deployed hydrophone arrays and both underwater and surface sensors powered by underwater autonomous nuclear turbine generator unit (ATGU) stations, linked to ground control centres by cables in the Arctic.[102] These sensor arrays can enable a range of A2/AD assets on the ground, surface and subsurface. Like their ground-based counterparts, these systems could be sabotaged covertly – which is a viable activity both in peacetime and conflict since sabotaging them entails no incursion into Russian waters.

The integration of the network – central to the effectiveness of the integrated architecture that has made A2/AD a significant threat – also exposes it to vulnerability. The digitisation of the system means that rather than operators reading the direct returns from their systems they instead monitor data that is being presented following an automatic interpretation of the sensor picture. Furthermore, the integration of mobile systems into fixed installations means that there are permanent targets for penetration that provide reliable access points to the network. Another manner in which the assurance of the network can therefore be compromised is either its penetration pre-conflict through cyber attack, or the use of protocol-based electronic attack to generate mistranslations of sensor input received to data displayed for the operators. The former requires years of pre-planning. The latter relies on similar penetration of the architecture but can be applied in real time. Both offer the opportunity to insert misleading information into the integrated network. The resulting need to assure the picture given can lead to paralysis and increase the vulnerability of the system to jamming by forcing operators to check returns on their screens. The primary effects of such activities are more psychological than physical, disrupting the confidence of the operators in the integrity of their systems.

Operators

There are two key categories of operator activities which can be actively pressured and influenced by an attacking force. The first are C2 activities – essentially the commanders sitting at key nodes at each layer of the system and how they are able to process the situation and activities of their subordinate elements and of the wider system above them. The second category of processes

101. Ronen Bergman, *The Secret War with Iran: The 30-Year Clandestine Struggle Against the World's Most Dangerous Terrorist Power* (New York, NY: Simon & Schuster, 2008), p. 367.
102. *GlobalSecurity.org,* 'Garmoniya / Harmony – RUSOSUS', 30 July 2021, <https://www.globalsecurity.org/intell/world/russia/harmony.htm>, accessed 2 March 2022.

are more generic operator behaviours – how the crews of radars, launchers, sustainment and logistics vehicles and other network components go about fulfilling their roles within the system.

The coordination and data-processing requirements are somewhat different in nature for commanders of air defenders and coastal defence forces. An IADS must rapidly not only detect but also classify, positively identify and assign shooters to targets across multiple tiers and channels. Some exotic threats, such as hypersonic glide vehicles and quasi-ballistic missiles, may even straddle the boundaries between multiple tiers. The primary C2 challenge in an IADS is in ensuring that the appropriate batteries within it are provided with sufficient real-time information about the wide-area picture of the battlespace and the planned activities of friendly forces to be able to confidently engage sometimes very fleeting targets of opportunity or defend themselves against potential attacks at short notice, while also ensuring deconfliction between the various elements and unplanned activities by friendly or neutral air assets. The use of decoys and electronic warfare techniques by attacking forces will considerably increase the difficulty of this challenge, especially if other factors can prevent or delay the movement of higher-level situational awareness to the tactical edges of the defence system.[103] Stealth assets, which are difficult but not impossible to detect and track, can also greatly increase the situational awareness challenge by forcing defenders to either ignore fleeting contacts or divert significant capacity towards attempting to 'join up the dots', to the detriment of wider stealth assets.[104] Although decoying and spoofing are possible in both the air and maritime operating environments, in the air domain the potential effects of decoy use and signature reduction or modification techniques are enhanced by compressed decision-making times. The potential to temporarily saturate a defence system's capacity to distinguish between legitimate threats and false targets is thus likely higher in the context of air defence networks than sea denial ones. Commanders may be influenced into making different judgements on how to prioritise different trade-offs by various pressures, including losses inflicted by attacking forces in previous engagements, targeted information operations or false data injected into key information-gathering nodes such as radars. Notably, A2/AD systems may use civilian and dual-use radar. The Russian IADS in the Arctic, for example, uses the Sopka-2 – a civilian airspace monitoring radar – for early-warning purposes.[105] Similarly, Hizbullah's 2006 attack on the INS *Hanit* was conducted using data from a civilian coastal radar. Though such systems add redundancy, they may also be easier to penetrate and spoof using means such as cyber penetration. The behaviour of commanders will be both affected by and critical to determining how the whole network reacts to such dilemmas over time.

The behaviour and perceptions of commanders can also be influenced by forcing them to make imperfect and inherently costly trade-offs between the system fulfilling its role of engaging incoming threats and the likely rate of attrition suffered by forward batteries and sensors. For example, an attacker might fire a number of anti-radiation missiles (ARMs) and loitering

103. Martin Streetly, 'Airborne Deception', *Armada International*, 22 September 2021.
104. For more information, see Justin Bronk, 'Russian and Chinese Combat Air Trends', *RUSI Whitehall Report 3-20* (October 2020), pp. 3–6.
105. Kaushal et al., *The Balance of Power Between Russia and NATO in the Arctic and High North*, p. 90.

munitions, as well as decoys and stand-in jamming munitions in support of an incursion into the IADS by an airborne strike package. In such a case, it would be difficult for the system to determine with much certainty which targets posed an imminent threat and there might also be far more radar contacts than ready-to-fire missiles. Command decisions would be required to determine the rules of engagement for the various layers of the system – how many missiles to fire, which target types to prioritise and which to ignore.

Command decisions would also affect how much risk the frontline radar and TELAR operators were exposed to from ARMs and loitering munitions when they unmask to illuminate targets and fire missiles before attempting to reposition. Outcomes (or perceived outcomes) in any one engagement will likely have a significant impact on commanders' decision-making processes when faced with similar dilemmas in subsequent engagements. The level of trust in the various command echelons' judgement and true situational awareness among operators at the battery level will similarly be affected by the real or perceived outcomes of such choices. As such, there are a variety of ways in which initial operations might be tailored to increase the likelihood that commanders misinterpret and react in a sub-optimal way to future attacks and/or reduce frontline trust in the capacity of the wider network to keep them alive or effective. A wave of lethally effective loitering munitions and kinetic stand-off munitions such as the UK's SPEAR 3 used to punish the defences which unmask to engage a subsequently feinting strike package in one engagement might, for example, encourage commanders or operators to assign far greater lethality to decoy munitions accompanying a real strike package in a subsequent engagement.[106] If activities can introduce contradictory information and create temporary isolation from higher nodes within the system, commanders will also become stressed due to the need to process too much information and coordinate more assets than the system was designed for them to handle while under significant time pressure and having to make choices which will have life and death consequences.

Sea denial systems typically face a different C2 challenge: coordinating assets from across domains and managing salvo tactics. While the active defences on ships can usually cope with sequential attacks, simultaneous salvos are likely to pose a greater challenge. Simultaneity, however, requires agile communication across the system, and between assets that may be held under distinct command chains. Understanding the decision-making points through which resource allocation decisions between, for example, the coastal defence troops, naval flotillas and air assets are made could thus substantially erode the potential for convergent strikes at sea. For the attacker, deploying naval assets in a manner that forces the defender into applying sensors from multiple domains also ensures that the defending C2 system must coordinate a complex combination of assets.

In effect, then, the C2 challenge facing air defenders and coastal defence assets are almost divergent. Coastal forces need to win what Wayne Hughes dubbed the 'battle of the first

106. George Allison, 'What is SPEAR 3 and Why Is it Important?', *UK Defence Journal*, 16 March 2017.

salvo'[107] and thus need to process and disseminate data and to coordinate launch decisions across services in a way that could exceed their actual capabilities. An IADS, by contrast, may be able to gather and disseminate information with relative ease, but is subject to data saturation and thus C2 degradation precisely because rapid data accumulation with insufficient time for analysis encourages mental short-cuts and sub-optimal decisions among command teams.

At the operator level, there are three main vectors on which operator behaviour can be shaped – fear, uncertainty and decision-making capacity. All of these will be further magnified by fatigue if pressure can be maintained over a sustained period, forcing operators to stay at their posts and potentially in harm's way for long periods. Changes in operator behaviour can have disproportionately large effects. For example, during Operations *Northern Watch* and *Southern Watch*, Iraqi SAMs operators were highly reluctant to illuminate their fire control radars for the required duration during engagements – resulting in them inflicting significantly less attrition on coalition aircraft than they might have.[108] Belief that operating one's own system would reveal the operator's position resulted in the system operating far short of its potential efficiency. The death of a Serbian general who ordered a battery he was visiting to maintain illumination is a good example of how cognitive effects can cascade across a system. On the one hand, his bravery was honoured by his comrades. On the other, his death reinforced the sense that illuminating meant death and Serbian air defences were therefore rendered ineffective by how they were employed, rather than simply by the scale of threat imposed by NATO.[109] Indeed, in Serbia, NATO pilots reinforced their kinetic effects with information operations, passing the codeword for HARM launch on open channels, which led Serbian SAM operators to shut down their systems and thereby also lose the ability to detect that they were being played. Revelations that make an organisation's practices public can serve a similar role. Following the hacker group Shadow Brokers' leak of exploits to software used by the National Security Agency, the organisation saw a degree of generalised uncertainty regarding safety across the organisation while the system itself was forced to undergo a revision of its tactics, techniques and procedures – all of which greatly hindered its operations.[110]

The risk tolerance of operators and commanders alike can be shaped to induce different behaviours. For example, when in a frame of losses – perceiving that their situation is deteriorating – commanders may take unnecessary risks to attempt to redress the situation. This was true in the case of the Soviet submarine commander who, having been hounded by US ASW assets at the height of the Cuban Missile Crisis, nearly ordered the launch of a nuclear

107. Wayne Hughes and Robert Girrier, *Fleet Tactics and Naval Operations* (Annapolis, MA: US Naval Institute Press, 2018), p. 294.
108. Peter Bartos, 'A Day on Northern Watch', *Air Power History* (Vol. 54, No. 1, 2001), pp. 1–16.
109. Benjamin S Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment* (Santa Monica, CA: RAND Corporation, 2001).
110. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London: Profile Books, 2020), p. 410.

torpedo.[111] Conversely, encouraging a perception of high losses and low effectiveness among operators is likely to lead to actions such as short illumination periods during radar-guided engagements or blind launches, which enhance individual survivability but greatly decrease operational effectiveness. Another effect of increased risk perception and fear among operators might be to induce systems to relocate more frequently to avoid being targeted. This will not only increase fatigue over time and reduce combat effectiveness but will also greatly complicate the supply of combat service support and create new potential opportunities to detect, track and attack the systems while on the move. The Russian armed forces demonstrated this in Ukraine – securing the cellphone data of frontline Ukrainian troops and using targeted and false messaging to get them to take unnecessary risks, such as breaking cover, in pursuit of personal survival.[112] Risk behaviour can be shaped in a number of other ways. For example, when confronted with losses, most individuals show a preference for high-value gains to recoup their losses, even when presented with the option of lower-value but more certain results.[113] As such, the creative use of decoys might incentivise disproportionate resource expenditure if it simulates higher-value targets because operators or commanders may take risks which they otherwise would not in pursuit of what appears to be major gains.

On the other side of the coin, under conditions of persistent pressure, individuals can fall into a state of learned helplessness and decision paralysis due to a perceived loss of subjective control over their circumstances. Uncertainty can be a function of a variety of factors, some of which have been discussed already. In addition to contradictory information, the isolation of certain components of a system from others can increase the informational demand on individual operators, who now have to carry out tasks, such as IFF interrogation, manually. Similarly, fears regarding penetration or disinformation can slow an organisation by forcing it to introduce layers of verification to compensate for uncertainty. This is illustrated in literature on insurgent groups, which often become significantly more cautious in their behaviour when they think they have been penetrated;[114] such behaviour usually degrades effectiveness even if it keeps operators alive. In the context of an A2/AD system, similar principles might be served through different means. If, for example, operators within a system were given some evidence that the other side knew who they were, or if evidence of previously successful deception were provided, this might alter their willingness to communicate across the system or act on orders without subsequent verification. For example, during the Ardennes offensive, once news spread that Otto Skorzeny's forces were dressed as Americans and operating behind allied lines, it had the effect of causing wider disruptions given the need to verify the identities of troops moving

111. Robert Krulwich, 'You (and Almost Everyone You Know) Owe Your Life to This Man', *National Geographic*, 25 March 2016.
112. Lucas Scarasso, 'Text Messages from Hell: Restraint and Information Warfare', Modern War Institute, 21 April 2020.
113. Daniel Kahneman and Amos Tversky, 'Prospect Theory: An Analysis of Decision Under Risk', *Econometrica* (Vol. 47, No. 2, 1979), pp. 263–92.
114. Jacob Shapiro, *The Terrorist's Dilemma: Managing Violent Covert Organizations* (Princeton, NJ: Princeton University Press, 2013), p. 40–55.

throughout the allied rear.[115] Information regarding successful SIGINT could be selectively leaked to achieve similar effects across an integrated defence system.

There is another potential way to exert pressure on a defence network via the introduction of uncertainty that is worth noting. In the context of a growing emphasis on automation and AI, preparatory activities in peacetime can inject significant levels of potential uncertainty. Specifically, by intentionally feeding incorrect data regarding one's own tactics into an opponent's systems. Automated systems are only as good as the data on which they are trained, and so can be influenced by subtle tailoring of peacetime activities that occur in sight of hostile intelligence collection or surveillance capabilities, or through mutual partners who might share information with opponents. While there is nothing new about tactical or operational deception, the volume of information and the timeframes over which it needs to be fed into an adversary system may necessitate more persistent deception than was previously the case. Increasing levels of automation hold the promise of potentially greater payoffs in terms of disruption and uncertainty if such effects are successful.

Finally, one might consider the tendency of individuals operating under conditions of stress and uncertainty to fall back on heuristics: mental shortcuts which serve to simplify complex cognitive tasks. This will increase the susceptibility of operators to deception, task overload and oversight of key threats within a complex picture. All other things being the same, the more under stress a system is, the more rigidly it will adhere to its standard procedures, and so the more likely it is to be inflexible under changing circumstances. As such, the more pressure a system is put under the less likely major reallocations of resources between different tasks and adroit changes of tactics become.

In summary, if operators within a defence network can be made to feel isolated, threatened, fatigued, placed under a high decision-making tempo and mistrustful of their own systems, the likely result will be a series of incremental shifts in behaviour that collectively add up to a major degradation of operational effectiveness.

Combat Persistence and Combat Service Support

The final major targeting vector for applying pressure on an A2/AD architecture is its capacity to sustain combat effectiveness over time. The first and simplest way to degrade the persistence of a defence system is to run it out of ready-to-fire missiles without those missiles inflicting significant harm on attacking forces. To do this, an attacker must persuade or force the command system or battery-level operators to launch large numbers of missiles against illusory, unimportant or expendable targets, or real targets which present the defences with a very low probability of kill per shot.

115. Jeffrey Jarkowsky, *German Special Operations in the 1944 Ardennes Offensive* (Fort Leavenworth, KS: US Army Command and General Staff College, 1994), p. 87.

There are several tactics and approaches which might succeed in drawing large numbers of missiles from launch rails for little practical gain. As with many of the other attack vectors alluded to in this chapter, most are likely to be far more successful if employed as one of many concurrent pressure points on the defence network than if they are employed in isolation. For example, large scale use of decoy UAVs, USVs or missiles which mimic the movement, radar and emission signature of real aircraft or ships will be much more likely to consistently draw hostile missile launches if they are employed in combination with actual strike sorties and long-range stand-off weapon salvos. The combination of lethal real targets and false signatures will either force the defences to waste a large number of missiles on harmless targets or take significant risk by ignoring targets which are not considered high confidence and thus increase the likelihood that many real threats penetrate the defences and inflict major damage. If they are cautious and as a result lose significant numbers of radars and other assets to real threats that were not engaged in time, behavioural changes are likely to lead to subsequent waves of decoys or false targets injected by protocol-based electronic attack being more successful in convincing the defenders to waste missiles. Over time, such operations can lead to a sustained fall-off in combat effectiveness as the defensive architecture begins to run short of high-value, long-range missiles and commanders and operators modify their launch tactics and rules of engagement to conserve remaining ammunition supplies.

Figure 7: The 202nd Air Defence Brigade in the Western Military District in Russia reloading S-300V SAMs in 2012.

Source: Vitaly V Kuzmin, Wikimedia Commons, 2 February 2012, <https://en.wikipedia.org/wiki/Cold-weather_warfare#/media/File:202_Air_Defence_Brigade_-_missile_loading_-2.jpg>, accessed 4 May 2022.

In either case, each time the defence system is successfully induced or forced to launch a significant proportion of the ready-to-fire missiles covering a given area, there will be a short but potentially exploitable window of degraded combat effectiveness while reloading of the TELs and TELARs takes place. The reloading operations will themselves create additional vectors for applying further pressure. Resupply efforts generally fix both reloading and receiving vehicles in place for 15–20 minutes at a time, which makes them more vulnerable to detection and attack.[116] Furthermore, the movements of resupply convoys generate a distinctive signature for long-range sensors such as GMTI radars, which can be analysed to give away battery locations, patterns of movement over time and the resupply routes themselves for future targeting and exploitation.[117] Special operations forces, infiltrating attack aviation formations, long-range artillery or conventional airstrikes all offer theoretically plausible means to target resupply and maintenance support convoys during periods when the system has been degraded by over-expenditure of ready-to-fire ammunition. If it can be demonstrated or at least convincingly messaged to operators that resupply operations expose them to additional risk, they may become more hesitant to fire missiles in large numbers in order to minimise the frequency of such rendezvous.

The radars and mission systems on mobile SAM complex units also require a steady supply of fuel to generate onboard power if they are deployed away from fixed pre-prepared firing points where external ground power is available. Thus, exerting continual low-level pressure on a network to force systems to remain at alert for long periods, especially in conjunction with long-range stand-off attacks which force them to operate in dispersed locations and relocate often, will impose a significant logistical burden on the combat service support apparatus. An SA-11 TELAR, for example, carries sufficient fuel for around seven hours of operation with the mission systems and radar ready.[118] This shortens rapidly if the system must displace. Operators and commanders alike may have to start making hard decisions over whether to prioritise using fuel for regular relocation movements or to preserve operational capability, especially if fuel convoys can be tracked and interdicted in the outer reaches of the network. The key point for the attacker is in sequencing their actions so that they have the assets in place to exploit and target the necessary actions of the defender in the wake of the previous engagement.

116. Author interviews with specialists familiar with a range of Russian air-defence systems, November 2021.
117. Thomas Newdick, 'The Army Lays Out Plans for its New Intelligence Gathering Jet', *The Drive*, 15 June 2021.
118. Author interviews with operators familiar with a range of Soviet and more modern Russian systems, November 2021.

III. Sustained Targeting: Preparing for Theatre Access in Competition

THE TARGETING METHODOLOGY outlined in the previous chapter highlights the importance of incremental advantage built up through the simultaneous application of pressure against the situational awareness, integration, crew performance and endurance of the target systems. Securing those incremental gains and having the confidence to push the risk envelope in harassing the target system depends on an adequate technical understanding of the radars, missiles and personnel being targeted. The consequences of failing to have a sufficient understanding can be fatal. Early jamming pods deployed by the US Air Force on a number of platforms, including the U-2 spy plane, far from protecting the aircraft, acted as homing beacons for the missiles fired at them.[119] Similarly, the Luftwaffe's failure to identify radar stations as a point of fragility in Britain's defences during the Battle of Britain meant that aircraft and pilots were expended on targets of secondary importance.[120] Since the RAF lacks the mass to suffer any significant combat losses, committing large strike packages into contested air spaces demands a high degree of confidence as to the performance of their equipment against the threats in the operating environment.

Conversely, when the Israeli air force conducted a strike against a Syrian nuclear facility in 2007, they appeared to Syrian air defences as friendlies, entering and departing Syrian air space unmolested. Whether achieved through a cyber attack or protocol-based electronic attack,[121] this was enabled by Israel building up a detailed understanding of the target system over a long period and thereby tailoring a means to evade it with a high degree of confidence. Whether such a feat is repeatable will depend on the speed at which an adversary can identify how the penetration was accomplished and patch or shield the vulnerability, but it may not need to be repeated.

The lesson from these examples is that to cold target an A2/AD architecture is to accept a severe disadvantage and take considerable risk. Activity that reduces the threat before conflict pays dividends in ensuring that the force is prepared should the requirement to penetrate the system arise. Whereas Chapter II considered how to degrade A2/AD architectures, this chapter outlines the activities necessary to make that targeting as effective as possible. Within British doctrine

119. Ben Rich and Leo Janos, *Skunk Works: A Personal Memoir of My Years at Lockheed* (London: Time Warner, 1995), pp. 147–81.
120. Sam Tangredi, *Anti-Access Warfare: Countering A2/AD Strategies* (Annapolis, MA: US Naval Institute Press, 2013).
121. Thomas Rid, *Cyber War Will Not Take Place* (New York, NY: C Hurst and Co, 2013), p. 54.

this concerns how UK forces can operate to compete, setting favourable conditions should they be required to undertake warfighting.

As with Chapter II, this one is framed around the ends being sought. The targets remain the same, but the mechanisms and associated activities differ. In many instances these activities create additional effects in conflict or are required to deliver the effects already described in Chapter II. The ends sought in competition may be broken into three broad lines of effort. The first is to continually seek access to understand the systems. The second is to constrain the development and deployment of A2/AD architectures. The third is to use collaboration to expand the avenues into theatre and therefore increase the threat surface of the system. These lines of effort are considered in turn.

Understanding A2/AD Architectures

As has already been discussed, having a detailed understanding of A2/AD systems is vital. To achieve this, it is necessary that the force is able to pursue multiple means of gaining access to, penetrating and collecting on the systems under as many different conditions as possible. To achieve this the force can conduct a range of activities from covert and overt collection to the stimulation of systems and the procurement or seizure of targets of opportunity for study.

Covert Collection

Covert collection involves the secret collection of information on how A2/AD architectures work. This can be achieved through the use of cyber penetration of the manufacturer to obtain detailed plans as regards the design and technical specifications of the systems – much as Chinese hackers did with the PAC-3[122] – or the cyber penetration of the C2 systems themselves. Covert collection may also involve traditional espionage targeting the engineers and scientists involved in the development of these capabilities, with cases such as the success of the Walker spy ring illustrating just how pivotal the information from such sources can be.[123] Collection can also be facilitated by the infiltration of testing areas, or the locations near where these systems operate, and the placement of spectrometers and other collection assets able to monitor the signature and emission patterns of the systems. This may involve the use of Special Forces to emplace monitoring devices.

Overt Collection

Overt collection differs in that the adversary may well know that they are being targeted and collected on. For example, during the Cold War the Soviets and the US Navy waged a quiet 'Third Battle of the Atlantic' against each other in which each side attempted to collect data on the other.[124] Collection can be achieved through the close proximity of ELINT and SIGINT aircraft

122. *BBC News*, 'Chinese Hackers Compromise US Weapons Systems Designs', 28 May 2013.
123. Hennessy and Jinks, *The Silent Deep*.
124. Owen R Cote Jr, 'The Third Battle', Newport Papers No. 16, US Naval War College, 2003.

including RC135 or close proximity of naval assets with sophisticated collection capabilities such as the Type 45.[125] It must be noted that if a system illuminates while these assets are in the area they may do so in a mode that differs from their standard procedures in war. In this way it is possible for the defender to deceive the attacker into believing they have mapped the signature of the platforms when in fact they have not. However, there are also instances where it is possible to monitor these systems as they engage real threats. Russian systems in Syria or Armenia, for example, have to illuminate to conduct point defence against threats from non-state actors flying UAVs at Russian bases.[126] The invasion of Ukraine has provided a wealth of intelligence collection on Russian SAM systems operating both on Ukrainian soil and in Belarus.[127] British warships and aircraft can remain in or over international waters and conduct overt collection on these incidents, while covert collection can support collection of signatures as regards C2 procedures within the network.

System Stimulation

This may be used to proactively cause target systems to illuminate to enable collection. The sponsoring of groups flying UAVs over defended airspace, or the infiltration of teams to proactively conduct such an action, could cause a range of responses that can be monitored using both covert and overt collection, with the difference between the response to the two also observed. Instances of exported systems can provide a valuable opportunity for systems stimulation because they are less likely to be able to rely on wider system components to avoid illuminating and because the escalation threat of operating against these systems may be reduced. This is especially the case as regards systems employed by non-state actors such as the Wagner group.[128] Against these systems aggressive harassment using fast air, or electronic warfare from ship-based or infiltrated systems, can be employed to monitor effects, given that the capacity for the manufacturer to record the effects is lessened by the layers of separation. In the case of non-state actors, the capacity to record such effects can be further reduced by the subsequent destruction of the system. The threat, moreover, encourages the system to be turned on with all of its functionality.

Stimulating communications between components of the system and the wider network is also of value when the system incorporates non-state actors for another reason. The employment of non-state elements as spotters and, perhaps, shooters for A2/AD architectures is increasingly visible. China, for example, has equipped all new People's Armed Forces Maritime Militia vessels

125. Author interview with Thomas Withington, electronic warfare expert, on the subject of peacetime monitoring of Chinese A2/AD, London, 18 February 2022.
126. Presentation by Uzi Rubin at the RUSI Deep Strike and Missile Defence Conference 2022, London, 23 February 2022.
127. Tim Robinson, 'Air War over Ukraine – the First Days', Royal Aeronautical Society, 2 March 2022.
128. Joseph Trevithick, 'The United States Smuggled a Russian-Made Pantsir Air Defense System out of Libya', *The Drive*, 27 January 2021.

with the HN-900 antenna, which supports a PLAN network comparable to Link-11.[129] There is also anecdotal evidence of Chinese fishermen identifying foreign naval assets for the PLAN using satellite phones.[130] Elsewhere, Russia has containerised the Klub-K cruise missile for possible use on civilian vessels.[131] The tendency to use civilian assets as spotters and shooters provides both risks and opportunities. On the risk side of the equation, it is vital to gather precise data on which civilian assets are supporting A2/AD architectures, given that erroneously killing civilians can be strategically disastrous – witness, for example, the Dogger Bank incident.[132] At the same time, however, civilians may represent a weak link in A2/AD systems if they are more amateurish in maintaining emissions control and communicate more readily with military assets than they should, creating the opportunity to expose more valuable targets through SIGINT. Stimulating communications between the military and civilian layers of the system is thus important both to avoid embarrassing mishaps in wartime and because the potentially most undisciplined operators of an A2/AD network should be targets for stimulation.

Covert stimulation can also be used with EW assets to assess how the system reacts to different signals being directed into its sensors. Given that many different frequencies can be generated and directed at a system, such collection does not necessarily give away useful information about tools aimed at overcoming the system.

Procurement

Procurement is a means of securing the actual threat systems or at least components of them or the services of operators in order to conduct examination and testing of them in a manner where adversaries cannot observe the experiments. Physically possessing these human and material components allows for actual systems and methods for warfighting – from jamming pods and electronic attack systems to tactical plans – to be tested against their intended targets.

Procurement can occur either quasi-overtly or covertly. Quasi-overt procurement might involve encouraging the defections of personnel with their platforms through the promise of reward and resettlement. Examples of successes for such policies would be the case of a Soviet Union pilot of the MIG-25 – then a very poorly understood aircraft – flying his plane to Japan in the

129. Ryan D Martinson, *Echelon Defense: The Role of Sea Power in Chinese Maritime Dispute Strategy* (Newport, RI: US Naval War College, 2018), p. 72.
130. Wang Chunyan, 连云港警备区结合渔业生产加强海上防卫警戒 民兵出海，渔船成为流动岗哨 ['Lianyungang Garrison Unites Fisheries Production to Strengthen Maritime Defense Awareness: When the Militia Goes to Sea, Fishing Vessels Become Mobile Sentries'], *China Military Online*, 8 December 2015, <http://www.81.cn/mb/2015-12/08/content_6805466.htm>, accessed 28 April 2022.
131. *Globalsecurity.org*, 'Klub-K Container Launched 3M-54 Klub / Caliber - SS-N-27 Sizzler', <https://www.globalsecurity.org/military/world//russia/club.htm>, accessed 28 April 2022.
132. Peter Schneider, 'Dogger Bank Incident', in Rudolf Bindschedler et al. (eds), *Encyclopaedia of Disputes: Installment 10* (Amsterdam: Elsevier, 1988)

hope of making a life in the US in 1976.[133] Generally, operators are likely easier to exfiltrate than systems, meaning that this approach may in many cases fall closer to collection than procurement. However, this depends on the particulars of the case. A policy of encouraging defection could raise risks to deploying assets in areas such as Kaliningrad, which directly border Western states and might at a very minimum foster a culture of distrust in operators that could hinder organisational effectiveness.

The process of covert procurement involves the setting up of front companies to procure systems or some of their components. In some cases, countries have gained access to key military data by exploiting national loopholes on exporting components that count as dual-use technology – for example, China securing German diesel electric engines for its warships and submarines in the 1990s.[134] Generally, it is unlikely to be possible to do this against the manufacturer of the system, but it can sometimes be done via those to whom systems are sold. Covert procurement can also be used to gain access to or possession of damaged components from combat zones.

The conduct of covert procurement requires the ability to straddle the licit and illicit arms trade. In many instances it also requires access to obfuscated finance. One advantage to covert procurement is that because procurement may come from a third-party recipient, it can be difficult for an adversary to know that their system has been compromised. For example, if China or Russia were to export a later generation MANPAD to Iran, and this were supplied to the Houthis, the procurement of that system by a front company working through another Yemeni actor could enable the recovery of the weapon without China or Russia appreciating that the weapon had fallen into the hands of an adversary.

Seizure

Seizure of A2/AD components, by contrast, is likely to be noticed by a competitor. When A2/AD components are used by non-state actors – as in Libya – opportunities may arise to work by, with and through local partners to capture intact platforms and to thereafter fly them out of the country for analysis. This may require the identification of possible targets and the building of specific missions alongside local partners, or it may arise from incidental captures with a requirement to rapidly provide transport. For the latter targets of opportunity it is necessary to have procedures to quickly assign the airlift and the necessary funds to facilitate capture. Seizure of such equipment has two effects. In the first instance it provides a platform for testing. In the second, because the capture will likely be noted by the designer, it provides an opportunity to reduce confidence in the system by advertising the fact that it is compromised and that defeat mechanisms may have been developed. This can also feed into constraining the proliferation of the system as confidence in its effectiveness can be undermined.

133. Cory Graff, ‘This MiG Super Fighter Terrified NATO: Then a Soviet Pilot Stole One’, *Popular Mechanics*, 16 November 2021.
134. Amanda Rivkin, ‘German Engine Technology Found in Chinese Warships – Report’, *DW*, 11 June 2021.

All of these lines of effort contribute to having a robust understanding of the threat systems, how they technically work, and for designing effective countermeasures and effectors. To achieve this, however, it is necessary to have a robust system for information management to cohere the data gathered from a wide range of collection activities. This database must not only comprise a repository for technical data for the design of countermeasures, but also include what the adversary knows is compromised, the conditions of collection and the human behaviours that were observed. Although access to the repository may be limited, those planning campaigns should be able to arrange for detailed briefings that assess the developed picture of the adversary defensive architecture in its entirety, rather than narrow technical briefings compiled in silos and relating to individual components of the A2/AD architecture.

Collaborative Engagement

The UK, as a medium power, must be wary of escalation dynamics in competition, and of its limited mass in warfighting. Working with and through partners and alongside allies can mitigate against these risks but requires prolonged engagement to effectively yield results. Collaboration may be pursued along four distinct lines of effort: ensuring access; enabling action; building preparedness; and assuring resilience.

Collaborating for Access

This may be understood as a means of increasing the opportunities for collection against hostile systems. This involves building relationships with groups and partner states who are anticipating having to operate against the components of A2/AD architectures. By way of an example, Vietnam fields the K-300 Bastion-P to defend islets in the South China Sea, and Ukraine fields the S-300P.[135] Engaging a non-adversarial third party can represent a useful avenue to insights on both systems themselves and the tactics, techniques and procedures imparted to local operators by Russian advisers. Of course, mutual partners may withhold such information for fear of losing access to adversary systems, but this is not always the case, especially for nations which are more invested in their ties with the West for security reasons. Understanding of when and against what they intend to operate can inform the timing and placement of collection devices without exposing the UK to escalation risk. The UK will have to engage in transactional exchanges with these partners, but where there is common interest there is also a basis for sharing results. There is also value in collaboration to enable covert collection. For instance, assisting a Kurdish group in strengthening its anti-tank capability may facilitate moving teams into a geography where they can emplace sensors to monitor systems of interest. Ultimately, collaboration for access must be divided between allies, where preparation for integrated operations means using common data files and significant sharing of intelligence and capability, as with the US through F-35s, partners with whom there are transactional exchanges, and groups that are used inadvertently to gain proximity to target systems. Defence attachés can

135. *Navy Recognition*, 'Vietnam People's Navy Deploys Bastion-P Mobile Coastal Defence Systems in Drills', 17 August 2016.

play a role in securing this kind of access, but they are not the only groups that can do so; in principle, advisory and support missions can also build bonds of trust to facilitate access.

Collaborating for Action

This may straddle the divide from competition to warfighting but must be premised on relationships built before the outbreak of hostilities. In competition, action to seize or stimulate threat systems may be undertaken indirectly through inducements to partners. In warfighting, the promotion of partner forces acting to target key systems, harass logistics, conduct sabotage against communications links, and harass sensors could expand the threat vectors against which an adversary must guard. By way of example, the need to position air-defence radar to meet a southern Houthi threat exposed Saudi Arabia to a direct attack from Iran on Abqaiq and Khurais.[136] The Houthi's willingness to take responsibility provided Iran with (implausible) deniability.[137] In a sub-threshold scenario the non-combatant evacuation of Lebanon or humanitarian operation into western Yemen could be greatly aided by having local partners equipped and prepared to fly loitering munitions into the anti-ship missile sites within their area of operation. This would not necessarily bring retaliation against UK forces but would enable their access and therefore their ability to assist said partners in assuring their own security. Another example would include sabotage of Russian logistics in Belarus through networks cultivated by Ukrainian intelligence.[138]

Collaborating in Preparation

This differs from seeking partners for offensive action in that it primarily concerns defence against incursion by a hostile power. Russian ground forces, for example, aim to maintain links between their forward air defences and strategic air defences. While targeting the radar themselves is highly dangerous given the force protection surrounding them, the field lines and other infrastructure between nodes is easier to reach. For those countries that are concerned with preparing resistance to incursions, educating the population – especially where there is conscription – about the appearance and significance of key vehicles and the means by which their integration and resupply can be impeded may significantly reduce the effectiveness and security of forward-deployed elements. Increasing the impact of autonomous and disaggregated action by informing the population of high-value targets can also act as a deterrent and constrain adversary planning, increasing the commitment of infantry that must be assigned to the protection of ground lines of communication. The exploitation of civilian quadcopters and other devices to harass, distract and otherwise degrade the effectiveness of components can also be valuable. While Russia maintains substantial rear area security forces, the concentration of these forces around key assets could in and of itself provide insights on their location to

136. Presentation by Uzi Rubin at the RUSI Space and Missile Defence Conference 2020.
137. *Ibid*.
138. Liz Sly, 'The Belarusian Railway Workers Who Helped Thwart Russia's Attack on Kyiv', *Washington Post*, 23 April 2022.

aircraft and other higher-end tools. As manoeuvre elements provide rear-area security from their own second echelon elements, this also decreases their capacity for penetration.[139]

Collaborating to Build Resilience

This builds on the preparedness of populations under threat of offensive hostile action by taking disaggregated resistance and articulating how it can be coordinated with wider campaign efforts. The ubiquity of telecommunications and photography in current conflict zones means that it is difficult for an occupying force to suppress the transmission of data from a combat zone.[140] Ensuring that those posting images of what is around them can do so in a manner that is most useful as regards the timely identification and targeting of high-value targets, however, requires that the population understands what it is observing.[141] There is increasing evidence that crowdsourcing data from both local populations and those across the West can increasingly be integrated with other forms of ISR.[142] One might consider the recent case of the University of Missouri's attempt to use a combination of deep neural networks and amateur analysts to map Chinese SAM sites.[143] Assisted by deep convolutional neural networks, which narrowed their search parameters, amateur analysts were only 5% less accurate than their professional counterparts on average.[144] Enabling civilian access and awareness of these openly available tools is both easy and potentially highly effective. Reprisals can of course restrict this behaviour, but because posting has become a universal phenomenon it would be resource intensive to prevent at scale. Ensuring that citizens understand how to make information available and useable by those seeking to liberate their territory can significantly expand the robustness and extent of sensor coverage across an operating environment, especially in urban and densely populated areas where standoff military sensors struggle to distinguish ground targets from civilian clutter.

Constraining A2/AD Architectures

The constraint of A2/AD architectures involves limiting where they are to be found, their density and levels of integration, and their attractiveness to third parties. Targets in achieving this objective include: the manufacturers of A2/AD components; the potential customers for A2/AD

139. Lester Grau and Charles Bartles, *The Russian Way of War* (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), pp. 190–200.
140. R A Marcum et al., 'Rapid Broad Area Search and Detection of Chinese Surface-to-Air Missile Sites Using Deep Convolutional Neural Networks', *Journal of Applied Remote Sensing* (Vol. 11, No. 4, 2017), pp. 2–31.
141. Shaun Walker, '"Barbarians": Russian Troops Leave Grisly Mark on Town of Trostianets', *Guardian*, 5 April 2022.
142. Matthew Ford and Andrew Hoskins, *Radical War: Data, Attention and Control in the Twenty-First Century* (London: Hurst, 2022).
143. Marcum et al., 'Rapid Broad Area Search and Detection of Chinese Surface-to-Air Missile Sites Using Deep Convolutional Neural Networks'.
144. *Ibid.*

components; military planners who may wish to deploy A2/AD components; and the operators who may eventually have to fight them.

Manufacturers

The capacity of manufacturers to produce the radar and missiles in sufficient quantities to support large integrated A2/AD architectures, and the proliferation of their products through foreign military sales, can be targeted in a range of ways. In the first instance, these companies depend on expertise to innovate and sell their products. In a competitive international market for talent the access of these companies to that expertise can be constrained by making the consequences of working for them unattractive. Monitoring those who work in design and engineering or sales for manufacturers of components of concern and promoting the denial of their access to the states of allies and partners, can restrict both how they go about their work and the attractiveness of taking up posts at these companies. Targeting these individuals for intelligence collection when they travel, gathering information on the irregularities in which they engage as part of the corruption that taints much of the arms trade,[145] and deniably releasing details of these activities to law enforcement agencies and local journalists, can place them under threat of arrest and thereby constrain their travel and opportunities.

Such methods mean that companies producing A2/AD components will become increasingly unattractive to talent that is not ideologically committed to working for the hostile state. Some may be attracted by increased pay, but this imposes an increased cost for talent on the manufacturer. Such measures are unlikely to greatly diminish the availability of domestic talent. However, they can significantly constrain access to international talent, and to the networks of facilitators employed by arms companies that enable export. The most effective campaign targeting talent within missile development is arguably that undertaken by Israel against German scientists working for the late President Gamal Abdel Nasser of Egypt.[146] The Israeli campaign not only entailed coercion and the kinetic targeting of scientists, but information efforts targeting the German government and the publication of scientists' activities to make working for Egypt dangerous and unattractive. Although threatening scientists is highly escalatory and could only be pursued under grave circumstances, the UK did adopt an aggressive approach towards potential suppliers of Exocet missiles to Argentina during the Falklands War.[147] There are many other ways in which working for particular companies can be made unattractive, without the threat of lethal force, which may be pursued under less extreme circumstances.

145. Andrew Feinstein, *The Shadow World: Inside the Global Arms Trade* (London: Penguin, 2012); Oleksandr Danylyuk et al., *The Geopolitical Goal of the Arms Trade of the Russian Federation* (Kyiv: Centre for Defence Reform and Potomac Foundation, 2019).
146. Roger Howard, *Operation Damocles: Israel's Secret War Against Hitler's Scientists, 1951–1967* (Borough: Pegasus Books, 2013).
147. Richard Aldrich and Rory Cormac, *The Black Door: Spies, Secret Intelligence and British Prime Ministers* (London: Harper Collins, 2016), pp. 353–86.

In certain cases, the manufacturers of key components may have underlying weaknesses that can be exacerbated. For example, Russia's Elektropribor, which manufactures key components of the KH-47M2 Kinzhal, is on the verge of bankruptcy due to corruption and poor management practices.[148] Exploiting potential labour disputes or targeting banks that choose to finance the firm could be avenues to exacerbate its issues, as could simply publicising these weaknesses to prospective foreign customers should Russia put the Kinzhal on sale. Alternatively, banks that conduct transactions with such firms and make payment for goods possible can be targeted with sanctions – making payment in hard currency difficult. This option was considered, though not applied, by the US as a response to India's purchase of the S-400.[149] It would likely have succeeded in at least significantly complicating the transaction, with the choice not to apply it being driven by diplomatic considerations.

With regard to Russian weapons systems at least it is also worth emphasising the extent to which their A2/AD components – and indeed all Russian complex weapons – are dependent on sub-components manufactured outside Russia, in the US, the UK, Germany, the Netherlands, Israel, Taiwan, South Korea and Japan, among other countries.[150] The oscillator for the computer supporting the radar on the TOR-M2 short-range air-defence system, for example, is made in the UK.[151] Through the process of building an understanding of A2/AD components it is likely that many vulnerable supply chains will be identified, which can either be denied through export controls or used as an opportunity to corrupt the system by tainting the supplied components.

Manufacturers can also be targeted by promoting the sale of cheaper and adequately effective alternatives to their intended markets. For example, several post-Soviet states have the capacity to manufacture missiles for earlier generations of Soviet air-defence systems. For many countries these earlier generations of SAMs can be run much more cheaply than advanced modern designs. They are also often adequate for the needs of the countries concerned. Ethiopia – for example – needs to be able to hold fourth-generation fighters flown by neighbouring countries at risk.[152] By supporting partners who can sell less capable but cheaper solutions that meet a country's needs, it becomes possible to both spoil the market for target companies and to help countries feel secure without having to invite hostile air defenders onto their territory or building architectures that threaten geographies well beyond their borders.

148. Sidharth Kaushal, 'Putting the Russian Hypersonic Threat in Perspective', *RUSI Commentary*, 28 September 2021.
149. Manu Pubby, 'India Likely to Pay for Russian Arms in Euros to Avoid U.S Sanctions', *Economic Times*, 1 July 2019.
150. Watling and Reynolds, 'Operation Z'.
151. Technical assessment of a recovered TOR-M2 in Ukraine, reviewed by one of the authors during fieldwork in April 2022.
152. *Military Watch Magazine*, 'Ethiopia Strengthens Air Defences with High End Russian Hardware – Pantsir Combat Vehicles and More', 19 March 2019.

Customers

The impact on potential customers of A2/AD architectures must primarily be cognitive. The aim must be to convince states that acquiring these systems is not a cheap means of achieving security but is instead a significant choice as regards strategic alignment, makes them a more likely target rather than protecting them from hostile attention, and that the systems themselves are unreliable and of limited effectiveness unless fielded in a density that is beyond the means of most medium powers. To examine these in reverse order, the amplification of effective strikes on such systems – such as Turkish strikes on systems in Libya and Syria, Israeli strikes on systems in Syria, and Russian air-defence losses during the invasion of Ukraine – can be used to demonstrate that they are not an effective defence when fielded in limited numbers.[153] On the more aggressive end of the scale, the use of offensive cyber penetration, or physical sabotage of demonstrator systems where opportunities arise, can produce failed tests and launches that bring the reliability of these systems into question. Moving long-range but narrow beam electronic warfare systems to bear on test radar can similarly ensure that they behave in an unpredictable manner when being used for demonstration purposes.

Demonstrating to a state that such systems make them a target and framing the choice to procure them in terms of strategic alignment is best left to diplomats but represents a key line of effort. Saudi Arabia's flirtation with the procurement of S-400, for example, must be understood by Riyadh not as a casual augmentation of their layered defences.[154] Instead, introducing a threat system, with Russian engineers, into an airspace where it can collect on Patriot batteries and on US and UK aircraft that might be helping to deter aggression from Iran, massively increases the cost and complexity of allied operations in the air space. For Saudi Arabia to do this must be understood as potentially invalidating commitments to defend them from Iran and comprising a strategic breach with its Western allies. This should not be represented as a punitive response. Instead, it is simply the case that the presence of such systems threatens the security of the forces that would otherwise be helping the Saudi government. It is for a similar reason that the presence of S-400 on Turkish soil must lead to major constraints on what NATO allies will share with Turkey and what systems can be exported to them. That Turkey flies its own NATO jets over these systems, which must be supported by Russian engineers, provides a huge intelligence opportunity for Russia and expands the risk for NATO aircraft should they need to operate against these systems.[155] Turkey must therefore not be allowed to procure F-35s and the reason for that prohibition must be made clear. Turkey must be an example to others of the consequences of alignment. Of course, Turkey also has a potential opportunity to bring itself back into alignment by allowing NATO to compromise the S-400 systems on its soil.

153. Ragip Soylu, 'Russia-Ukraine War: Turkey's Bayraktar TB2 Drones Proving Effective Against Russian Forces', *Middle East Eye*, 28 February 2022.
154. Linda Kay, 'Saudi Eyeing Russian S-400, Pantsir-S as U.S. Air Defense Systems Ineffective Against Yemeni Missiles, Drones', *Defense World*, 11 November 2021.
155. Joseph Trevithick, 'Turkey Tests F-16s and F-4s Against S-400 Radars in Defiance of U.S. Sanctions Threats', *The Drive*, 25 November 2019.

Studies on measures such as the Countering America's Adversaries Through Sanctions Act suggest that while they have not necessarily led to a diminution of sales by Russia to traditional partners, they have had a chilling effect on potential new customers of Russian equipment.[156] As such, it is on prospective adversary partners as opposed to those with longstanding defence ties that efforts must be focused. When approaching traditional partners of states exporting A2/AD components, by contrast, attempting to wean them off purchases may be less useful than trying to use opportunities for cooperative engagement with them for information gathering.

Planners and Operators

The risk of compromise if more advanced A2/AD components are forward deployed must be factored in to the judgement of military planners in those states who operate these systems. Demonstrating, or suggesting through false information, that systems have been accessed or compromised because of their forward deployment increases the risk of distributing them and therefore limits where they will be used. Alternatively, this will increase the force protection that must accompany deployed units and therefore drive up the resource commitment to deploy. There is also the point that if compromise is considered a risk in foreign military sales, this will likely see more limited versions of a system exported. This requires changes to design and a parallel production line. It increases friction and reduces customer satisfaction, knowing that they have an inferior product. Where this reduction in export capability is rushed it can also be possible to regain the full functionality of the system through software changes, for example, and thereby to still learn a great deal about the base system from the less functional export version.

Messaging that systems have been compromised, amplifying the defeat of export systems used in conflict, and deniably promulgating false trails of information as to how systems were defeated, all have the effect of limiting the confidence of operators in their systems. This can also lead to the employment of unnecessary or unhelpful tactics in actual combat, as crews try to mitigate against perceived or poorly understood threats. This is particularly doable in the wake of conflicts such as in Nagorno-Karabakh. While Russia has conducted detailed after-action reviews of the performance of its systems in isolation,[157] their capacity to understand the full range of capabilities that Azerbaijan and Turkey used against them is incomplete. This, therefore, becomes an opportunity to provide misleading information.

Command and Control in Competition

Just as the suppression and degradation of A2/AD architectures in conflict requires the simultaneous and persistent fusing of effects along multiple lines of effort to achieve tangible results, activities in competition are most effective when combined. It is the collection effort to understand the components – both overt and covert – that allows for information to be

156. John Parachini, Ryan Bauer and Peter Wilson, *Impact of the U.S and Allied Sanction Regimes on Russian Arms Sales* (Santa Monica, CA: RAND, 2021).
157. CAST, 'Vishla Kniga CAST "Burya na Kavkaz"' ['CAST Book "Storm in the Caucasus" Published'].

disseminated, undermining confidence in these systems among operators, planners and customers. Similarly, it is through collaboration that the stimulation of the systems can often most effectively be achieved to optimise collection. As has been described in this report, this will require the collaboration of intelligence agencies, diplomats, cyber forces, special forces, conventional forces and the defence industry. In conflict, joint interagency approaches are forced by the pervasive atmosphere of crisis. In competition, with opportunities potentially short, it becomes difficult to maintain sufficient situational awareness between independent units to effectively cohere activity. For this reason, within the British system, the appointment of a campaign director, empowered as a senior responsible officer, to cohere these activities, would be essential to the effective pursuit of preparing the ground to successfully degrade A2/AD architectures in conflict. This individual would need to be read into the multiple lines of effort and empowered to shape planning for other activities so as to achieve opportunistic convergence. There is also the need for pre-authorisation of budget and the ability to deploy at short notice to pursue opportunities as they arise. Without a centralised approach to campaign coordination, the speed of collaboration would likely be too slow to capitalise on relevant opportunities.

A secondary line of effort, not under the responsibility of the SRO for competition, would be the cohering of the intelligence picture, based on collection activities and the assessment of the threat, to build and maintain effective joint training, tactics and procedures to enable the suppression and degradation of A2/AD architectures in conflict. The capacity to design joint exercises and the authorities to experiment between rather than be led by each frontline command would be critical to innovating in a manner that would enable success in conflict. It is also important that the targets and what can be done to incrementally degrade them is shared widely so that units within an operating environment can practise mission command to contribute towards the systems degradation outlined as the objective in Chapter II.

IV. Battle Damage Assessment and Campaign Waypoints

CHAPTER II OF this report set out a methodology for degrading A2/AD architectures by disintegrating their layers, exhausting the force, blinding its systems and overwhelming its personnel. This could be achieved through the persistent, simultaneous application of joint effects through a non-linear tempo of blows above a critical mass. The aim was to translate physical actions targeting the system into behavioural changes in how the system behaves as a whole, in order to open up access to the theatre. A fundamental challenge in this task is to assess when the defensive network has been pushed into a new behavioural state. How, for example, is a headquarters to judge whether operators in SAMs have been worn out to a point where their responsiveness has significantly diminished? How is it to be determined that engagement permissions have been delegated from higher echelons to battery commanders? Finally, how confident is the attacker that a target SAM has been destroyed? Battle damage assessment is fundamental to the effectiveness of the degradation of A2/AD architectures because understanding when certain thresholds have been crossed as regards the performance of the target system must inform how resources are committed against it, and the risk profile of specific missions. This chapter considers the requirements for accurately monitoring the progress of a campaign and the decision points that commanders will have in expanding or restricting the licence of the joint force to engage.

There is also an important question as to who makes the judgement on changes in the risk posed by the A2/AD architecture, and whether they are sufficiently trained to do so. Then-Rear Admiral Sandy Woodward, commander of the Carrier Task Group that retook the Falklands, in many respects demonstrates the problems that can arise when one domain expert judges the risk across multiple domains of operation. He rightly viewed the UK's centre of gravity as the carriers and in balancing risk between the domains under his command, placed their protection highest in his order of priorities. At the same time, however, he was willing to commit the Harriers – an indispensable part of the carriers' weapons system – into attacks where the probability of losing the aircraft was high, the likelihood of success small, and the impact of success negligible.[158] In doing this he routinely overruled the RAF and Fleet Air Arm officers under his command.[159] If – as is necessary – multi-domain activity is to be orchestrated, it must be directed centrally. Although units operating under mission command may exploit opportunities to advance the campaign, the major set pieces that will have an appreciable effect on the A2/AD architecture will require centralised synchronisation. This means that whoever is in this position will be a joint commander but will have a single service background. Ensuring that they are appropriately

158. Jerry Pook, *RAF Harrier Ground Attack Falklands* (Barnsley: Pen & Sword, 2007), pp. 177–81.
159. Lawrence Freedman, *The Official History of the Falklands Campaign: Volume II* (New York, NY and Abingdon: Routledge, 2005).

cognisant of the risk to each component within the force will be vital to ensuring that scarce assets are not overcommitted too early when conditions have not been appropriately set. It is also important that these commanders are aided by information to judge the risk. Again, therefore, an effective methodology for battle damage assessment is vital, as is the appropriate provision of staff in support of the commander to ensure access to relevant technical expertise.

Assessing System Degradation

Conducting an assessment of whether an opponent's system has been degraded or dislocated is fraught with subjectivity and error and provides an opponent with opportunities to reinforce one's own preferred beliefs. Take, for example, Admiral Chester Nimitz's decision prior to the Battle of Midway to selectively reveal the locations of two carriers – seemingly out of position – to Admiral Chuichi Nagumo's task force.[160] This reinforced Japanese assessments that they had achieved operational surprise and contributed to lax tactical scouting on the day of the battle. The commander of an A2/AD architecture might, similarly, have reasons to feed into perceptions that the system has been degraded so as to invite risky behaviour on the part of Western forces. For example, committing large numbers of fourth-generation aircraft before an IADS has been sufficiently attritted or placing vessels within CDCM range while a system can launch coordinated salvos might prove catastrophic. As such, effective methods for assessing system degradation are vital. There is an argument that the skills that support systems analysis are the domain of the deep specialist, who may not necessarily rise up a military career path. However, it is worth noting here that specialists can in principle be drawn from other branches of government or beyond government to support these efforts, which might also contribute to their being able to impact assessments on equal terms with commanders. In principle, for example, branches of the military could maintain organisations that serve as a pool of specialised individuals with clearances who could be bolted into a headquarters in conflict. The US Air Force and wider military's use of RAND in the form it existed during the Cold War is an example. The very fact of many RAND analysts being civilians from beyond the command structure was an additional advantage which lent them an ability to argue certain points with senior leaders.[161]

Pattern of Life Analysis

If one wishes to assess whether a system is operational, has degraded gracefully, or is at a tipping point, it is necessary to compare the behaviour of its constituent elements to a baseline. To this end, pattern of life analysis of system behaviour under optimal conditions can be juxtaposed with actual operator behaviour. For example, a tell-tale sign might be operators moving their vehicles erratically in ways not consistent with pre-conflict pattern of life analysis. Erratic or last-minute changes of plans typically reflect system degradation and cognitive collapse; witness,

160. Anthony Tully and Lu Yu, 'A Question of Estimates: How Faulty Intelligence Drove Scouting at the Battle of Midway', *Naval War College Review* (Vol. 68, No. 2, 2015), pp. 1–15.

161. Fred Kaplan, *The Wizards of Armageddon* (Redwood City, CA: Stanford University Press, 1991), pp. 223–81.

for example, Soviet decision-making during the early days of Operation *Barbarossa*[162] or Qusay Hussein's frequent changes to the defensive plans for Baghdad in 2003.[163] Unusual behaviour could also reflect generalised uncertainty among operators.

The volume of communications within and across echelons could be another marker of systems degradation. The lower the confidence of operators, the less likely they are to communicate in ways that support integrated defensive operations. For example, an air-defence system operating optimally would see strategic SAM systems placed at the rear of an opponent's formation operate their radar, while systems further forward remained turned off. It would also see relatively low levels of radio communication, because operators can rely on ground-based datalinks. As operators were forced to move, one would expect to see higher volumes of radio frequency communication. Moreover, if efforts in areas such as EW severed the links between forward positioned systems and those in the rear, one would expect to see their radar light up more frequently as operators were forced to rely on their own organic capabilities. In a sea denial context, if coastal vessels clustered in specific zones, this would reflect them attempting to deconflict with shore-based batteries, indicating that the two components of the system could not be rapidly coordinated. This in turn would indicate a reduction in the system's capacity to launch massed salvos.[164]

System Stimulation to Test Hypotheses

Stimulating activity within a system serves purposes beyond immediate targeting, it is also an important means of assessing the state of the system as a whole at any given point. For example, should operators within a system mount sporadic or poorly coordinated responses to a perceived threat – as Iranian operators did in 2020 following the death of Qasem Solemani and subsequent Iranian attacks on US forces – this can be revealing.[165] Similarly, if CDCMs fire sporadic or limited salvos against maritime threats, this could be indicative of a shift in the state of the system as a whole. Stimulating the system can be accomplished through decoying, though in practice it often puts at least some assets of real military value at risk. The commander of a theatre access operation will need to assess precisely how many assets they are willing to risk in this role. Assets of low value may not stimulate a response, regardless of the system's functionality, while putting higher-value assets at risk could provide better information, albeit at a higher risk.

Stimulating individual components of a system can also reveal the degree to which it has been compromised. To return to the example of Midway, US cryptographers assessed the

162. Chris Bellamy, *Absolute War: Soviet Russia in the Second World War* (London: Penguin, 2008), p. 110.
163. Michael Gordon and Bernard Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York, NY: Atlantic Books, 2006), pp. 92–100.
164. Bruce Bechtol, *Red Rogue: The Persistent Challenge of North Korea* (Washington, DC: Potomac Books, 2007), pp. 72–77.
165. Schwartz, 'Iranian Report Details Chain of Mistakes in Shooting Down Ukrainian Passenger Plane'.

success of their penetration of Japanese communications by having the garrison at midway broadcast a supposed water supply shortage and observe whether this detail emerged in Japanese intelligence reports.[166] In an A2/AD context, one might assess the degree to which communications between operators were compromised by similar means, perhaps through the selective leaking of supposed losses.

Data Fusion

A major source of error in battle damage assessment is reliance on a few, potentially compromised, sources of data. For example, at Gallipoli, British assessments that the Royal Navy had cleared nearby minefields and silenced major Turkish artillery positions were driven by the excessive use of information from maritime reconnaissance planes to inform judgements.[167] Where possible, then, multiple sources of data should be used to conduct verification. Local friendly populations and special forces could, for example, augment efforts at battle damage assessment using data gathered through air- and sea-based sensors. This might be particularly useful with regard to identifying decoy targets, which opponents such as the Serbs used to good effect in the Balkan wars of the 1990s and which Russian forces are likely to field.[168]

When assessing the psychological state of the defenders, cross-validating accounts of defectors where possible with pattern of life behaviour might provide a better account of systemic degradation than any one source. Finally, where possible, multiple types of sensor should be used to verify the status of specific targets. The breadth of the available data and the number of potentially contradictory sources on which the commander can rely will be vital to avoiding the over-optimism or groupthink which characterised failures such as Gallipoli and Japanese operations at Midway.

Assessing Unit-Level Tactical Results

Having indicators for system behaviour is critical for assessing risk, but it is also necessary to log what has actually been physically done to an architecture. There are therefore a range of battle damage assessments that must be completed in relation to each tactical engagement.

Direct Observation

The simplest way to ascertain whether a target has been struck is through direct observation. There are a number of ways in which this can be accomplished.

Many strike assets have two-way datalinks that provide information on whether they have struck their target. This is the case for most modern anti-ship and land-attack cruise missiles,

166. Tully and Yu, 'A Question of Estimates'.
167. Jonathan Schroden, 'Straits Comparison: Lessons Learned from the 1915 Dardanelles Campaign in the Context of a Strait of Hormuz Closure', CNA, September 2011.
168. Martin Andrew, 'Revisiting the Lessons of Operation Allied Force', *Air Power Australia*, 27 January 2014.

for example. In other cases, using an expendable asset for battle damage assessment might be viable. For example, during the Nagorno-Karabakh conflict battle damage assessment for the Azerbaijani Harop strike on an Armenian S-300 system was carried out using a Bayraktar UAV.[169] More capable assets are also being considered for battle damage assessment functions by many nations. For example, the Chinese GJ-11 stealth UCAV is considered a likely candidate platform, with which the Chinese strategic rocket force can monitor its effectiveness.[170]

HUMINT from assets on the ground may provide another means of assessing whether targets have been struck. In certain cases, if platforms once struck are left in place for long periods of time, granular satellite imagery using assets such as SAR satellites can also be of use. Targets such as naval vessels, given their size and conspicuousness, will be the easiest components of an A2/AD system against which to perform battle damage assessment. Assets destroyed by operators within line of sight, such as Ka-31 helicopters, will similarly pose a relatively simple challenge. The task is at its most complex on the ground, particularly because the individual means of achieving direct observation can be countered. Datalinks can, for example, be jammed and HUMINT assets compromised. Nonetheless, a broad suite of means for collecting data can produce redundancies. It is also worth noting that not all components of one's system for assessing battle damage will necessarily be able to communicate at the same pace, meaning that commanders will likely have to make key judgements about when to trade operational tempo for certainty.

Indirect Observation

Behaviour associated with the sustainment of losses can also provide indirect insights. For example, the movement of assets from other military districts or regions might provide insights into the degree of attrition suffered at the front. Similarly, the movement of vehicles to tow or repair damaged assets could provide information.

At strategic depth, losses at the front will create patterns of behaviour to replace them, which can be mapped and assessed. Cyber incursions or conventional espionage into inventories and actors within the adversary's industry might reveal details regarding resource expenditure and the demands for loss replacement. The mobilisation of additional personnel might similarly reflect an attempt to replace losses at the front. In many conflicts, the creation of ad hoc training centres to fast track individuals into certain skill categories has been an indicator of severe attrition of the pre-existing pool of trained personnel. This was the case for Imperial Japan during the Second World War, after its pool of skilled pilots began to diminish.[171] The movement of people to new specialisms and career paths within an organisation and the creation of training infrastructure near the front might, then, be a tell-tale sign of operator

169. Can Casapoglu and Sine Özkaraşahin, 'The Hunt for Armenia's S-300: Assessing Azerbaijan's Most Sensational SAM System Hit in the Ongoing War', EDAM, 1 November 2020.
170. Kaushal and Marciewicz, 'Crossing the River by Feeling the Stones', p. 72.
171. Milan Vego, *The Battle for Leyte, 1944: Allied and Japanese Plans, Preparations, and Execution*, (Annapolis, MA: US Naval Institute Press, 2014), pp. 43–75.

losses. If granular information regarding operators themselves is known, sources such as communications between the state and their families, pay-outs to relatives of the deceased or information in local obituaries might also provide insights into whether casualties were inflicted on key personnel.

Notably, with a few exceptions, much of what constitutes indirect observation will be conducted by national intelligence assets but will comprise a critical part of a commander's battle damage assessments. It is thus vital to both maintain lines of communication between intelligence and commanders in the field and that clear criteria direct intelligence-gathering towards providing tactically actionable information.

Conclusion

THIS REPORT HAS sought to explain the strategic threat posed to UK freedom of manoeuvre by modern anti-air and anti-ship weapons complexes collectively described as A2/AD architectures. It has set out to explain how these systems work and why they are different to previous generations of defensive weapons. The report has attempted to outline a methodology for degrading A2/AD architectures and the preparatory work necessary to be able to carry out such operations. This leads to some clear recommendations for how the UK should go about addressing this challenge.

The first requirement is for a Senior Responsible Officer to be appointed to cohere the collection of information on and the joint force training to fight against A2/AD networks. This officer must have a key collection target list and contacts across the joint force and other government departments. They must be able to identify opportunities that emerge either because of adversary activity or UK operations and have the resources and authority to support the exploitation of those opportunities.

Second, there must be a joint and interagency repository for the information collected and a team dedicated to understanding this data as it relates to a system in use, rather than as a series of technical components. At present, analysis of technical specifications is largely retained within the Defence Science and Technology Laboratory for producing technical countermeasures. Assessments of adversary systems within defence intelligence is largely held at a platform level and expertise on enemy doctrine and concepts of employment are in a different silo. The result is that tactical commanders likely to face these systems often receive disjointed briefs that do not provide a comprehensive operating picture.

Third, there is a need for joint exercises for theatre entry, and for the challenge in these exercises to effectively represent the threat. Owing to the limitations on joint training areas large enough to allow for play over realistic ranges, let alone the use of electronic warfare, and the collection opportunities such activities would provide for adversaries, these are likely not viable. Instead, tactical exercises across the joint force on unit contributions to effects against A2/AD components should be carried out. Given the lack of expertise on these systems at unit level, these exercises should be designed by a director with access to the data repository. Where joint activity can be conducted, however, is in simulated command post exercises to help educate joint commanders about the different risks across the force when confronting these systems. Assuring theatre entry should be a key component of professional military education.

As regards targeting A2/AD systems, the methodology outlined in this report advocates two distinct phases of operation: competition and conflict. The former provides the necessary technical knowledge to be effective in the latter.

In competition, the aim must be to maximise collection opportunities, lay the groundwork for theatre access by building networks for collaboration, and constrain the deployment and export of threat systems by discrediting their effectiveness and threatening their integrity. This requires joint interagency collaboration to conduct stimulation of threat systems, covert and overt collection, procurement and seizure. Collaboration can be used to cause realistic stimulation, or to lay the groundwork for degrading the effectiveness of systems in conflict. Cyber penetration and electronic collection against targets of opportunity is particularly critical outside conflict. The whole force should see it as part of their mission to exploit opportunities to facilitate this activity during their other operations.

In conflict a commander must first draw together their forces and have each subordinate component layout what they believe they can contribute as regards effects to the systems threatening theatre entry. These options should be presented with their lead times, repeatability and projected magnitude and persistence of effect. These effects should target the A2/AD architecture's information inputs, its personnel, its networking and its endurance. The effects might be summarised as:

Table 2: Effects and Target Sets

Deny, Disrupt or Corrupt *Information Inputs*	**Induce *Personnel* to Experience**	**Deny, Degrade or Corrupt the *Network***	**Deny or Disrupt Access to *Supplies* of**
Early Warning	Fear	Links	Munitions
Identify Friend or Foe	Loneliness	Capacity	Fuel
Fire Control	Stress	Redundancy	Power
Target Acquisition	Fatigue	Permissions	Food and Water
Blue Force Tracking	Uncertainty	Assurance	Spare Parts

Source: Author generated.

Against these effects, the commander should synchronise joint force activity so that the adversary system finds itself persistently under threat but is struck simultaneously by multiple and therefore mutually reinforcing and cascading effects. Furthermore, these simultaneous packages of effects should build as the system degrades. Thus, the initial coordinated defeat of a tactical component of the system should be reinforced with information operations across the system to shape the behaviour of personnel and thereby enable a more widespread disruption of the network, further exposing isolated components to synchronised attack.

At a system level the aim should not be the destruction of the A2/AD architecture, because, while desirable, this is likely infeasible within a relevant timeframe and with the likely combat mass available. Instead, the aim should be to shift system behaviour from an integrated fighting system to an isolated set of components, which can thereafter be suppressed. The commander should therefore aim to shift the system from optimal operations to strained operations to degraded operations. Effective behavioural indicators to overlay on to tactical battle damage assessments must be used to judge how permissive the operating environment has become and

therefore the risk parameters of wider activity. These operations must be conducted quickly; they are vital in order to enable theatre access, but they will not deliver victory by themselves.

Finally, it must be stressed that for a relatively small force such as the UK the inability to absorb losses significantly constrains options for penetrating A2/AD architectures. In this context, it is necessary to have a large number of decoys and to be able to clutter the environment, or else to consciously accept a considerable level of risk. This means that there must be a sizeable stockpile of munitions, decoys and effectors. Investment in capability without sufficient munitions to deliver a critical mass of effect is largely pointless as regards operational outputs. Determining what constitutes a critical mass of munitions and decoys must be determined through the simulation of joint engagements. Testing single systems in isolation tends to produce overly large requirements for the number of munitions employed. This – again – reinforces the importance of simulations in a synthetic environment that accurately replicates the enemy system.

About the Authors

Jack Watling is a Senior Research Fellow for Land Warfare in the Military Sciences team at RUSI.

Justin Bronk is a Senior Research Fellow for Airpower and Technology in the Military Sciences team at RUSI.

Sidharth Kaushal is a Research Fellow for Sea Power in the Military Sciences team at RUSI.

Annex: Russian Air and Coastal Defence Systems

SA-21/23 – Russian Designations S-400/S-300V4

These are very long-range SAM systems based on wheeled or tracked vehicle chassis. They are typically deployed as batteries which incorporate a command vehicle, target acquisition radar vehicle, a primary fire control and engagement radar vehicle, several TEL and/or TELAR vehicles to carry and fire the missiles, and relocating vehicles carrying spare missiles in their canisters. Batteries sit within a larger battalion, regiment or brigade structure which includes not only multiple batteries but also strategic radar assets and higher-level command vehicles. Each TEL or TELAR can carry and launch a number of different missile types including very large 250 km- or even 400 km-class weapons, as well as smaller and cheaper 120 km- or 60 km-class ones for closer targets.

Source: Dmitriy Fomin, Wikimedia Commons, 6 May 2018, <https://commons.wikimedia.org/wiki/File:S-400_Triumf_(27102989027).jpg>, accessed 5 May 2022.

SA-17 – Russian Designations 9K37M1 Buk-M1 or 9K317M Buk-M3

These are advanced medium-range mobile SAM systems based on tracked chassis and designed to be able to keep pace with advancing ground forces units over rough terrain. They are intended to be used in batteries which incorporate a command vehicle, target acquisition radar vehicle, TELARs and reloading TELs. Each TELAR is designed to be capable of conducting independent engagements as a single vehicle, although its performance will be far more limited compared to when operating as a battery or within a larger IADS. The 9K37M1 variant has a maximum engagement range of around 50 km, and the newer 9K317M has a claimed maximum range of 70 km. The SA-17 can also engage ground or maritime targets in an emergency.

Source: Dmitriy Fomin, Wikimedia Commons, 6 May 2018, <https://commons.wikimedia.org/wiki/Category:2018_Victory_Day_in_Moscow#/media/File:BUK-3M_(27053439937).jpg>, accessed 5 May 2022.

SA-15 – Russian Designation 9K331 Tor-M1

The SA-15 is a highly mobile short-ranged SAM system designed to move with and protect Russian ground forces units close to the frontlines. It is a tracked, self-contained system designed to operate as a single vehicle. The system was primarily developed to counter enemy attack helicopters and to intercept incoming missiles and other projectiles. As a result, it has a comparatively high-frequency radar with very limited range, but excellent track resolution and very rapid detection rates even against small targets. The effective range of the SA-15's missiles against aircraft is around 12 km. The operating frequency of its radar and the mobile, self-contained nature of the system make it particularly challenging to detect, track and locate. It also ensures that if an aircraft accidentally finds itself in engagement range, it will have very limited warning time before missile impact.

Source: Vitaly Kuzmin, Wikimedia Commons, 2010, <https://en.wikipedia.org/wiki/Tor_missile_system#/media/File:Tor-M1_SAM_(2).jpg>, accessed 5 May 2022.

SA-22 – Russian Designation Pantsir-S1/2

The SA-22 is a short-range mobile SAM and anti-aircraft gun system. It is a self-contained system mounted on a wheeled chassis and designed to provide both local air defence for Russian ground forces units, and also protection against incoming missile strikes for more valuable long-range systems like the SA-21 and SA-23. The Pantsir has suffered numerous losses in combat against both the Israeli Air Force and Turkish Air Force in Syria, as well as in Libya and Ukraine – most notably against Bayraktar TB2 UAVs with light anti-tank missiles. It is assessed as significantly less capable than the SA-15 but can still pose a serious threat to aircraft caught unawares in its effective range of around 10 km for the missiles or 3 km for the cannons.

Source: Dmitriy Fomin, Wikimedia Commons, 6 May 2018, <https://commons.wikimedia.org/wiki/Category:Pantsir-S1#/media/File:Pantsir-S1_(SA-22_Greyhound)_(41204907934).jpg>, accessed 4 May 2022.

SS-C-5 - Russian Designation K-300P Bastion-P

The Bastion-P is a Russian coastal defence complex. It is capable of launching the supersonic P-800 Oniks (SS-N-26 Strobile) cruise missile, which is capable of fulfilling both anti-ship and land attack missions. The Oniks has a top speed of Mach 2.8 and carries a 300 kg armour-piercing warhead. Its navigation system relies on a combination of inertial guidance and GPS/ Glonass in midcourse, and an active seeker in the missile's terminal phase. The P-800 has an operational range of 400 km and its extended range version, the P-800M, is effective at ranges of 800 km. A typical battery of Bastion-P includes four launchers, four transloaders and two or three command and support vehicles. The average coastal defence brigade has four batteries under its command, though this may vary by brigade. The system can be cued in by data from Monolit-B over the horizon radar (organic at brigade level), but can also receive cueing from sources such as the Ka-31 helicopter and small vessels, including the Project 22160 corvette acting as spotters.

Source: Russian Ministry of Defence, Wikimedia Commons, 22 June 2021, <shorturl.at/egvHZ>, accessed 5 May 2022.

SS-C-6 - Russian Designation Bal

The Bal coastal defence system is an antecedent to Bastion-P, which is being gradually phased out in favour of the latter system. That said, it still makes up roughly half the missile capabilities of units such as the Baltic-based 25th Coastal Missile brigade. The system fires the KH-35 anti-ship missile, a subsonic missile that was designed to be analogous to the Exocet with a 145 kg HE warhead and a range of roughly 130 km. Its extended range variant, the KH-35UE has a range of up to 300 km. The missile relies on a combination of inertial guidance in midcourse and an X-band active seeker in terminal phase to navigate towards its target. Like the Bastion-P, Bal systems are operated in batteries of four lanchers and transloaders, and two or three command and support vehicles all based on the MZKT-7930 8x8 truck chassis. The command vehicle has a 3TS2E Garpun radar, but the system likely relies on assets held at brigade level or by other parts of the force to operate at long ranges. In effect, then, it is a less sophisticated antecedent to the Bastion-P. Like its newer counterpart, the Bal CDCM system has been used in land-attack roles, in addition to its primary anti-ship function.

Source: Pliskin, Wikimedia Commons, 6 July 2013, <https://commons.wikimedia.org/wiki/File:BAL-E003.jpg>, accessed 5 May 2022.