**Royal United Services Institute**
for Defence and Security Studies

Conference Report

# RUSI Missile Defence Conference 2022

Sidharth Kaushal

# RUSI Missile Defence Conference 2022

Sidharth Kaushal

RUSI Conference Report, August 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 Conference Report, August 2022. ISSN 2397-0286 (Online).

**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)

# RUSI Missile Defence Conference 2022

ON 23 AND 24 February 2022, RUSI held its 23rd Missile Defence Conference. Participants considered how integrated deterrence against long-range precision strike might be delivered at a NATO level. Discussions were framed around the Russian long-range precision strike threat, which has supplanted other threat vectors as NATO's pacing challenge. Over the course of the conference, several key themes emerged:

- The air and missile threat environment is becoming more complex as the discrete categories that guided defenders are becoming increasingly blurred by new capabilities.
- To meet this, NATO integrated air and missile defence (IAMD) will need to be nested within a multidomain concept of operations which similarly blurs previously well-defined barriers within NATO systems.
- This approach will need to embrace strike, active defence and resilience in a synergistic way.
- This in turn will require both technical adaptations – in particular, leveraging domains such as space – but also vital organisational adaptations to create structures capable of supporting multidomain approaches to IAMD.

## The Evolving Threat Environment

In the first panel of the day, we heard how adversary approaches to both strike and IAMD will challenge our own concepts of operations. Dr Uzi Rubin, the former director of the Israel Missile Defense Organization, argued that until relatively recently threats could be neatly categorised on the basis of altitude and speed. There was a clear distinction, for example, between high-flying fast targets like ballistic missiles and lower-flying targets like cruise missiles. This in turn enabled a technical approach to the problem based on a subdivision of the threat into tiers, with different systems enabling intercepts against different tiers. This paradigm has been challenged in several ways. First, the emergence of capabilities such as hypersonic glide vehicles (HGVs) and quasi-ballistic missiles like the Russian 9M723, all of which fly at varying altitudes at very high speeds. HGVs, in particular, pose a challenge to old paradigms given their speed and extreme manoeuvrability. Moreover, low-altitude threats such as UAVs are becoming more complex and can be equipped with a range of propulsion systems. The result is a more congested low-altitude space in which UAVs and cruise missiles operate in tandem. The cumulative effect of these shifts has been to substantially challenge an air and missile defence paradigm that was based on building specific systems to meet specific challenges.

The second major facet of the threat environment, described by Major General Valeri Saar, former Chief of the Estonian Air Force, is the fact that adversaries such as Russia are developing their own highly robust IAMD networks to limit the effects of NATO strike capabilities. Russia's ballistic missile defence (BMD) system will see its older A-135 interceptors replaced with newer variants, and upgrades made to its C2 systems. The new S-500 Prometheus, which will be equipped with four different radars for BMD and air defence missions, will also be critical both as a means of intercept against targets like hypersonics and ballistic missiles but also as a data integrator and C2 node for other systems like the S-300 and S-400. General Saar noted that the slow reaction times of the Soviet BMD system against targets like the Pershing missile were viewed as a critical vulnerability during the Cold War, so including a command layer to overcome this challenge is likely a Russian priority. Systems like the Kontainer over-the-horizon radar will provide the first layer of the Russian network, followed by S-500 and the subordinate systems under its command which will track threats which change their altitudes.

The offensive threat posed by Russia is intrinsically related to its IAMD systems. The existence of Russian defences precludes an exclusive reliance on deterrence by punishment. This lends itself to damage limitation approaches in which offensive actions can be contemplated by Russia because NATO retaliation against them can be mitigated if not entirely precluded. A robust IAMD capability underpins an aggressive strike posture. Indeed, the fact that countries such as Russia and China view the risk posed by NATO and Western missile defences in precisely this way – as noted by RUSI's Veerle Nouwens in the same panel – is a partial insight into how they intend to use their capabilities.

As discussed in this panel, the evolving threat environment leaves NATO policymakers with two options. First, they could attempt to replicate the Russian approach to IAMD which tends to emphasise defence against the full spectrum of threats and multifunctional capabilities. For example, systems like S-400 and S-500 typically carry a range of interceptors to enable them to engage a variety of targets. Some Western assets, particularly maritime ones, already do take this approach to IAMD. Second, they could prioritise the most challenging threats for investment in active defences, while in other areas deterrence, strike or resilience might be used to meet the missile challenge.

## Doctrinal and Organisational Requirements for Effective Deterrence

Currently, as discussed by Radoslava Stefanova, head of NATO's IAMD section, the NATO approach is to attempt to find the right balance between deterrence and defence. Within this context, IAMD plays a crucial role, albeit one that is still distinct from BMD, which is a permanent mission with a distinct set of enablers and permissions. NATO currently provides a C2 structure for national IAMD capabilities with the aim of ensuring a federated framework into which national assets can 'plug and play'. Furthermore, NATO aims to ensure deterrence against missile threats across the spectrum of competition through activities such as air policing in peacetime along with BMD missions, and by generating IAMD from national assets in wartime. Beyond this are the human and organisational elements of IAMD, in particular exercises which align national

tactics, techniques and procedures. Exercises such as *Steadfast Defender* play an important role in this, as do those led by individual countries, such as the US-led *Formidable Shield*. Aligning these exercises and their outputs was identified as a key task for NATO going forward, especially as not all national assets are perfectly interoperable. A particularly challenging aspect of the issue is that some NATO members still use Russian systems like the S-400. Other priorities for the emergence of a more integrated Alliance capability, identified by Raytheon's John Baird and Lockheed Martin's Chris Harrison, were commonality in areas such as software and the technical interoperability that could serve as a stepping stone for eventual integration.

In the day's session on concepts of operations and capability generation, Brigadier Robbie Boyd, former military advisor to the Chair of the NATO Military Committee, suggested that NATO could find itself owning and jointly funding a wider range of strategic enablers. Pointing to the Allied ground surveillance system operating from Naval Air Station Sigonella, Boyd noted that a shift from a capability-driven approach to a threat-driven one could create greater opportunities for the joint funding of strategic enablers, many of which currently depend on the US. In the same panel, Professor Julian Lindley-French suggested that delivering the enablers needed to both leverage current systems and future capabilities such as AI will be critical to allowing the Alliance to fight increasingly high-tempo wars.

There is, however, a challenge that extends beyond adequately resourcing IAMD as currently understood which was underscored by a number of speakers. Reiterating a point made in the first session, Jerome Dunn, currently of Booz Allen Hamilton, described the challenge facing militaries as being one of liberating information from the networks built to handle them. Dunn described the current architecture of IAMD systems as being essentially linear, with certain sensors and command nodes being linked to certain effectors, meaning that opponents can target specific points of failure with capabilities that the system was not designed to defend against. An example of this is the Houthi attacks on the radar of Emirati Patriot batteries – essentially unpicking a battery's single point of failure with a slow, low target it was not built to intercept. The solution, Dunn noted, was creating integrated networks that can use data from mission-agnostic capabilities. For example, during a recent IBCS test, the US army conducted an intercept of a cruise missile from tracks it received from a USMC G/ATOR radar and an F-35, neither of which is a dedicated missile defence asset but which collectively could meet this mission. The technical dimensions of this need not be unduly complex, Dunn noted, arguing that both military testing and work on data integration in the commercial sector illustrates the viability of this vision.

However, there are substantial organisational implications with such an approach, both for IAMD and command more broadly. If capabilities, such as an F-35, can serve multiple missions, then the question of how they are tasked becomes a challenge. For example, if an F-35 on a SEAD mission spots a ballistic missile launch, should it shift emphasis to tracking the launch and transmitting data or continue on its existing mission? As Rear Admiral Archer Macy, former director of the US Joint Integrated Air and Missile Defense Organization, noted, this will require a shift in the philosophy of staffing and command that Western militaries have inherited from the Napoleonic era. He suggested that the unification of strike and IAMD under a single effects

coordinator, themselves working to the intent of an overall campaign coordinator, might represent a first step in facilitating effective resource allocation. A commander's intent might, for example, need to be more broadly defined at a campaign level, with priority accorded to specific tasks rather than being signposted as an asset's core function.

Further discussion focused on the incorporation of other instruments into IAMD. These instruments include technical capabilities such as strike and cyber but also national-level resilience. Major General John Mead, Deputy Chief of Staff for Plans at JFC Naples, highlighted the ability to draw on both kinetic long-range precision fires and less kinetic means of disruption as central to deterrence. At the strategic level, the ability to hold certain capabilities at risk can be used to deter the use of enemy assets or force their withdrawal. Consider General Saar's example of the way in which Pershing and the threat it posed to Soviet C2 set the conditions for the withdrawal of Soviet SS-20 missiles and the signing of the INF Treaty. The integration of offence and defence also has tactical implications. As General Richard Formica, former head of the US Army's Space and Missile Defense Command, noted, the sheer size of adversary missile arsenals makes an approach centred solely on active defence unviable. For example, Russia has fired over 2,000 cruise and ballistic missiles at Ukraine to date. As such, 'thinning the herd' of incoming missiles by proactively engaging launch platforms is also a tactical imperative. However, Sally Walker, former Director Cyber at GCHQ, noted the risk of using a homogenous template based on military capabilities such as cyber assets. Walker noted that cyber assets work on very different time scales to capabilities such as fires, with vulnerabilities in an opponent's system often cultivated decades in advance, with a persistent risk of discovery or patching. This is not to say that integration is impossible. Russia, for example, conducted coordinated cyber attacks and kinetic strikes on Ukraine's early warning systems and communications architecture early in the current conflict. The issue, however, is that one should not assume that these capabilities can be responsively called on over the course of a conflict like fires – the vulnerabilities that enabled their use will be discovered. Rather, they might be useful as part of an initial broadside in tandem with strike, but their value may diminish as a conflict wears on.

The second major area for integration is resilience. As noted by Brigadier General Dr Mier Elran, former head of Israel's home front command, the challenge posed by adversaries is not merely large numbers of precision strike capabilities but increasing numbers of low-cost assets from MLRS to UAVs. This will be a particular risk for NATO's eastern members who, even in the event of successful deterrence, could find themselves coping with a substantial humanitarian disaster should they face the levels of MLRS use seen in Ukraine. For Israel, which has faced a substantial and growing MLRS and UAV challenge from its north with very limited strategic depth, the solution to the challenge has been integrating active and passive defence. Hardened shelters, resilient infrastructure and an information architecture that shares details of incoming missile volleys with both citizens and key civilian agencies such as fire brigades have been crucial to ensuring that the threat can be met at a reasonable cost. As Elran noted, there are other low-cost means to defeat threats – the use of directed energy is viewed as having particular promise in Israel – but civil resilience is a sine qua non. Moreover, the existence of resilience measures can also remove pressures to act pre-emptively to reduce risks to civilian populations.

## The Technological Element

Underpinning the developments described by the attendees will be a series of technological shifts. Space, now defined as an operational domain by NATO, will be central to much of this. As Lt General Henry Obering, former director of the Missile Defence Agency, noted, developments in areas such as edge processing and neural networking are making concepts of operations previously considered technologically infeasible conceivable. For example, he noted that one of the causes of the failure of the US Brilliant Pebbles satellite programme was that the C2 demands of the programme could not be met by a centralised node. Today, however, it is viable to consider peer-to-peer information sharing by constellations of small satellites acting as the functional equivalent of single apertures to track targets such as hypersonics.

The importance of space was reiterated by Air Vice-Marshal Paul Godfrey, commander of UK Space Command, who noted that the vision laid out in the UK's Space Strategy seeks to embrace many of these principles. In addition to its ISR function, space will also be central to delivering the levels of data latency needed to enable a multidomain system of systems.

The second key enabler for a multidomain approach to IAMD, as noted by BAE's Amelia Gould, is shared standards of data and appropriate training models. The ability of industry to leverage data more effectively will be critical to generating models that operators can trust, which in turn will be vital to the decision-making speeds that Lindley-French and others identified as central to contemporary and future operations. This will require protocols for sharing data that is considered highly sensitive.

Finally, at the level of effectors, Dr Tom Karako, director of the missile defence programme at CSIS, highlighted the importance of multi-mission effectors. Pointing to the example of the SM-6, which can serve both air defence and land attack roles, Karako highlighted the fact that multi-mission capabilities will be vital to ensuring that platforms can serve the vision of integrated offence and defence highlighted by other speakers. However, multifunctionality will come with its own problems in terms of specialisation and, potentially, cost – meaning that an understanding of where to specialise and where to emphasise multifunctionality will be critical to procurement.

## Conclusions: Towards an All Domain Approach

The core challenge highlighted at the conference was integration – of technical capabilities and across the levers of national power. This will likely entail a shift from an approach based on specialised capabilities to one in which versatility is the key value of an asset. This will require substantial investments in key enablers, many of which cannot be met by NATO members on a national basis. This raises the question of whether joint funding of capabilities at the Alliance level will need to proceed on a more expansive basis.

Beyond this, key operational decisions will need to be made regarding where a full-spectrum defence is necessary and where the Alliance should rely on other means of coping with threats – whether by deterrence or resilience.

A further consideration for the Alliance is how the doctrine and command structures within which national capabilities fit should adapt to the requirements of a future operating environment in which neatly delineated mission taskings may no longer be viable.

These challenges will likely be met on both national and Alliance level and meeting them is critical to ensuring integrated NATO deterrence against precision strike in the decades to come.

***Sidharth Kaushal*** *is Research Fellow for Seapower in the Military Sciences team at RUSI.*