Breaking the kill chain: Rethinking soft kill in anti-ship missile defence

A more diverse, complex, and proliferating anti-ship missile threat set is creating more stressing challenges for ship self-defences, and asks new questions as to the contribution of soft-kill mechanisms. *Richard Scott* reports

Anti-ship cruise missiles (ASCMs) have long been recognised as a significant threat to maritime forces. Their potency was first demonstrated in October 1967 with the sinking of the Israeli destroyer *Eilat* by P-15 Termit (SS-N-2 'Styx') missiles, and the half century since has been punctuated by a number of deadly strikes on both naval and commercial vessels: the Indian attack on shipping in Karachi harbour in December 1971; Israeli actions against Syrian and Egyptian naval forces during the 1973 Yom Kippur war; Argentine attacks against the UK Royal Navy (RN) task force in the 1982 South Atlantic conflict; and the Iran-Iraq 'Tanker War' in the Gulf between 1984 and 1988.

What is also becoming clear is that the ASCM is increasingly transcending definitions of conventional and asymmetric warfare. Proliferation to proxies and non-state actors has become a reality, evidenced by the attack on Israel's Sa'ar 5 missile corvette INS *Hanit* by Hezbollah off Lebanon in July 2006, and the destruction of the United Arab Emirates' fast catamaran *Swift* off Yemen by Houthi forces in October 2016. Both attacks are believed to have involved missiles sourced via Iran.

Anti-tank guided weapons (ATGWs) fired from the coast also pose a threat to vessels close inshore. This was demonstrated by a July 2015 attack by Islamic militants against an Egyptian patrol craft off North Sinai; footage showed an AT-14 'Spriggan'/9M133 Kornet-E missile – or an Iranian clone thereof – being launched from a coastal hilltop and then flying out to strike the vessel.

Soft-kill countermeasures have long been a key part of the anti-ship missile defence (ASMD) armoury. As early as February 1966 the RN had raised an urgent requirement for the development of shipborne 'Window' – chaff by another name – rocket and launcher systems, assigned the code names KNEBWORTH and CORVUS respectively, to provide electronic countermeasures (ECM) against Soviet anti-ship missiles employing active radar homing.

A chaff round is fired from a Mk 36 decoy launching system aboard the DDG-51 guided-missile destroyer USS Barry (DDG 52) during the Valiant Shield 2016 joint training exercise. (US Navy)

1704718

Such expendable decoy systems were thrust front and centre of ASMD in the wake of the destruction of the Eilat in October 1967, and again after the 1982 South Atlantic conflict. The loss of major units to active radar homing ASCMs resulted in rapid response programmes to engineer more effective ship self-defence systems, with significant emphasis placed on the deployment of off board countermeasures to distract or seduce radio frequency (RF) seekers.

First-generation chaff systems were designed to counter the relatively simple active radar homing systems – characterised by wide-range gates – associated with 'Styx' and its ilk. However, the subsequent proliferation of more modern sea-skimming ASCM types, employing increasingly complex RF seekers with very narrow range gates and various electronic counter-countermeasures processing techniques, was to present a new challenge. These threats were the catalyst to the development of increasingly automated soft-kill systems, improved chaff payloads, rapid response corner reflector decoys, and a new breed of active off-board countermeasures devices.

The emergence of guidance methods and seeker technologies exploiting other parts of the electromagnetic spectrum has similarly resulted in the development of matching soft-kill responses. These include infrared (IR) decoys to seduce IR seekers, and multispectral obscurant payloads designed to counter electro-optical (EO) guidance systems.

However, there is a recognition that continuing developments in ASCM technology mean that maritime forces are today confronted by an increasingly diverse and complex threat set. Furthermore, the advertised development of a new breed of hypersonic weapons – such as Russia's 3M22 Zircon – will present ship defences with an altogether more stressing challenge in the years ahead.

Accordingly, there is a debate under way as to what contribution soft kill will play in future ASMD, and how its deployment and function will integrate with, and balance against, hard-kill responses. Attendant to this discourse is how soft kill can break the classic find, fix, track, target, engage, and assess (F2T2EA) kill chain.

[Continued in full version…]

Understanding the threat

As well as integrating human skills with technology resources (sensors, weapons, communications, and command facilities) in a measured and coherent manner, the success of ASMD also depends on a detailed understanding of the threat. "Co-ordination of these skills and capabilities, along with insight into the threat, are essential components of success, which can only be realised through comprehensive analysis, modelling, simulation, and training – with subsequent mission rehearsal – to develop robust tactics, techniques, and procedures [TTPs] for the efficient proactive and reactive use of integrated hard-kill and soft-kill effectors," Hogben observed. "These must all be used with cognisance of the operating environment, including an assimilation of meteorological and geographical impacts made on weapon and sensor systems."

He continued, "We must employ TTPs to break the [F2T2EA] chain effectively [either at the earliest opportunity, or alternatively at that point in the kill chain is most efficiently exploited]. A modern anti-ship missile may have a supersonic flight envelope, enhanced with a counter-countermeasures and a hard-kill evading final terminal weave, but it may need precise information to find its target or have a slow fly out trajectory from launch before transitioning to its cruise profile, both of which offer opportunity for less complex effectors to defeat it.

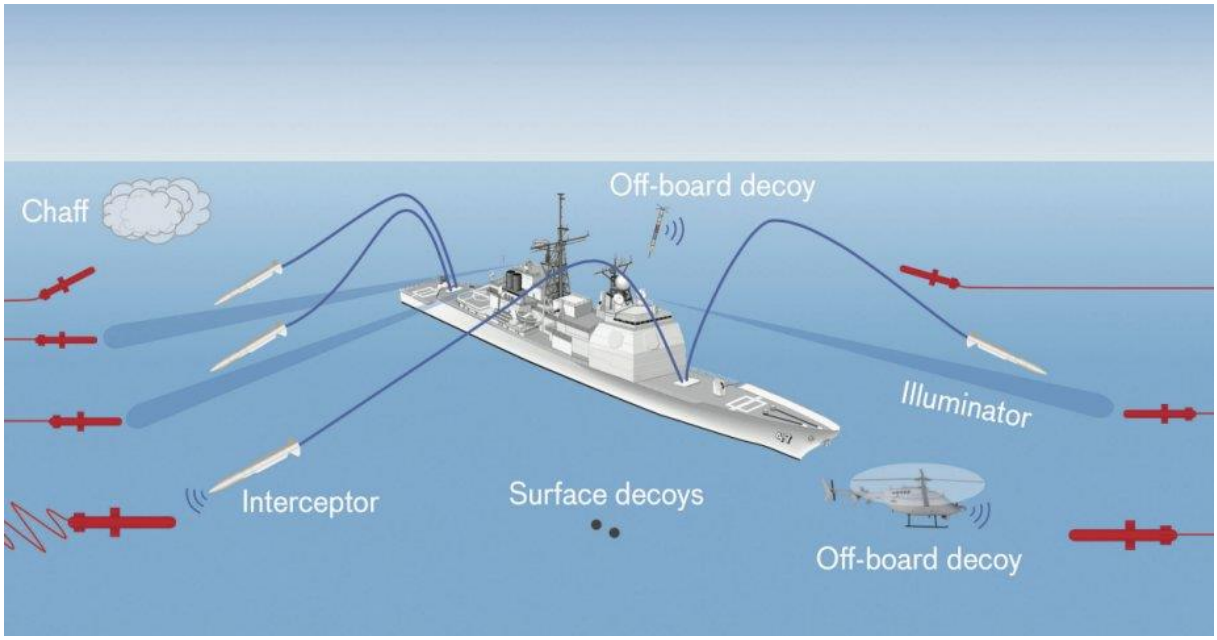
"We must also think about efficiency. A surface-to-air missile is very expensive. So why not use a [lower-cost] decoy [where possible] to conserve hard-kill resources?"

Part of the problem, in Hogben's view, is that there is increasingly a lack of appreciation as to the part to be played by soft-kill countermeasures. "Technological understanding has stagnated in the last decade or so as hard-kill solutions have become the default effector of choice against anti-ship missiles," he said. "Operational risk has increased as a result, while the understanding of how soft kill can contribute to ASMD has diminished significantly."

Operational risk in this particular context reflects two factors. First, a changing threat environment characterised by the proliferation of increasingly capable and relatively cheap ASCMs (the economics of Chinese volume production are estimated to achieve a near 10:1 cost-equivalence ratio when compared with the unit production cost for a Western surface-to-air missile). Second, the lack of depth in the defensive magazine available to the maritime commander.

"Soft kill offers the potential to provide alternative means to defeat the modern threat, quite possibly supporting a hard-kill effort. At the same time, there is a 'deeper' magazine of defensive effectors available to the command to defeat the prolific legacy threat. This offsets the need to use expensive and less available hard-kill devices for those threats that can be defeated by soft-kill methods."

However, Hogben contends that the current primacy afforded to hard kill in ASMD has served to erode core skills and confidence in alternative soft-kill methods, and suggests a rebalancing of effort and emphasis. "Good ASMD should address this by integrating hard-kill and soft-kill solutions with a dynamic threat evaluation weapon allocation [TEWA] tool embedded in combat management systems both at the unit and task group level," he said. "This TEWA function should present the operator with an automated solution, able to be vetoed where necessary ['man-on-the loop'] as the man direct 'in-the-loop' will no longer be able to cope when faced with multi-axis, multitype, multithreat scenarios.



Closer integration of hard-kill and soft-kill defences would improve overall ASMD performance, but layering individual systems into a single-defensive strategy requires effective and increasingly automated TEWA. (MIT Lincoln Laboratory) 1704719

He continued, "Intrinsic to integrating hard kill and soft kill is giving the command sufficient confidence to use the latter vice the former, or to integrating soft-kill into a hard-kill response so as to raise the [probability of kill] further, perhaps such that a single missile can be fired (as opposed to a salvo) to defeat the inbound threat missile.

The twin themes of efficiency and sustainability are central to Hogben's argument. "When considering larger-scale operations undertaken at reach from the home base, the sustainment of [missile] capability may be a mission essential element for unit survival and mission success," he said. "Noting that most decoys can be replenished at sea and can be a cost factor of 100 times less than a missile, it may be more viable to launch multiple decoys vice one guided weapon.

[Continued in full version…]

While existing soft kill offers solutions against a large proportion of currently fielded anti-ship missiles, further decoy development beyond, which exists today will be required to evolve solutions against emerging threats. The absence of a catalyst for further innovation in decoy payloads and deployment mechanisms remains a barrier; Hogben observes that the stagnation in maritime soft-kill stands in marked contrast to the airborne realm, where the threat change/threat proliferation encountered during recent conflicts has driven significant investment in the fast-track development of new air platform protection technologies. "The pressing operational need to counter rapidly evolving threats, most notably MANPADS [man-portable air defence system] seekers operating in the EO/IR spectrum, has engendered a more productive community-based approach to countermeasures development across front-line users, the defence scientific community, and industry," he said.

There is a recognition that there are big differences between the air and maritime domains. In the first instance, the imperative to improve air platform survivability in Iraq and Afghanistan was a catalyst to the new enterprise model in EO/IR countermeasures development. Second, the airborne expendables market is characterised by high volumes and high consumption, with annual replenishment buys providing an opportunity for regular payload change and technology refresh to match emergent MANPADS threats in theatre. This is in contrast to the maritime realm, where navies tend to procure 'commoditised' countermeasures rounds off-the-shelf at 10-year intervals, commensurate both with war stock life and budget availability.

Third, MANPADS are smaller and cheaper than ASCMs, and their technology has proliferated widely on the battlefield. This has allowed more ready access to intelligence of detailed threat characteristics, enabling better understanding of seeker function and performance and thus the means to exploit vulnerabilities. ASCMs, by contrast, tend to be a significant magnitude more expensive, and have historically been a more 'state-controlled' weapon, so making intelligence gathering somewhat more difficult.

Even so, Hogben believes there is significant scope in the maritime soft-kill realm to learn lessons from the more 'collegiate' paradigm that characterises airborne countermeasures development. "The potential is there in NATO's MCG 8 [Maritime Capabilities Group 8] but we're not grabbing it," he said. "This is an area where I feel the maritime community lags behind the air domain, with considerable potential still to be realised."

Two Standard Missile-2 anti-air missiles pictured moments after launch from the DDG-51 guided-missile destroyer USS Sampson (DDG 102). Could some threats be more efficiently defeated by soft-kill mechanisms? (US Navy)

1704720

The problem is that while several navies host their own national EW trials, and the NATO Naval Armaments Group Above-Water Warfare Capability Group (AWWCG) hosts its own NEMO trials, the high classification put on threat intelligence limits engagement with industry, and prevents suppliers from accessing the knowledge needed to develop improved soft-kill payloads matched to specific threat types. "[These] can only be developed through close industrial, scientific, and military collaboration, with a sharing of information and requirements to develop solutions akin to what has

been delivered in the air domain in support of Iraq and Afghanistan operations over the last two decades," Hogben said, adding, "The lack of funding from individual nations is equally stifling development, which in turn leads to the 'what is on the shelf' approach to procurement.

"NATO shares common threats, and a jointly managed and funded approach – for example, a 130 mm users group akin to the NATO Sea Gnat programme in the 1980s – would allow new products to be brought to the market. Such an approach would also offer greater interoperability between nations further enhancing sustainability on operations."

[Continued in full version…]

New approaches

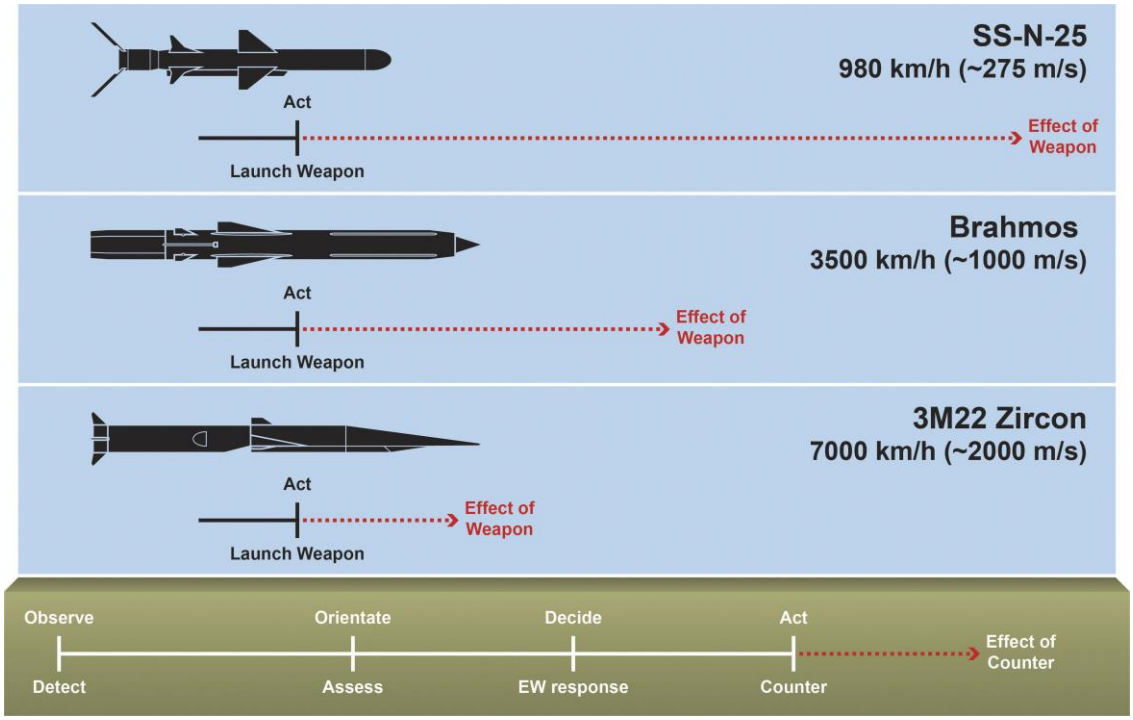
A similarly forensic view of how new technology could be used to improve soft-kill effects was presented to EW Europe 2017 by Paul Bradbeer. A former Royal Air Force air electronics engineer, and now electronic warfare operational support technical sales manager for MASS Consultants, his presentation and accompanying paper explored three themes: a detailed analysis of the kill chain itself; the application of artificial intelligence to automate and compress the decision cycle; and the merging of traditional EW practices with modern cyber techniques.

According to Bradbeer, an understanding of the kill chain at a granular level is essential. "It is important to understand every single element of the chain, and components within an element, how they are linked, and the implications and effects of disrupting any given element or component in the overall weapon system.

"Each part of the system has a crucial role to play in the sequential process of find/fix, recognise, track/engage, prosecute/effect. By understanding the strengths and weaknesses of the individual elements, and the dependencies between them, it is possible to design a countermeasure, which could 'break' a link in the weapon system chain, and degrade the performance or lethality of the threat.

"In order to design such a countermeasure, it is often necessary to go even deeper in to the kill chain. For example, in the case of a threat emitter, characterising and understanding the transitions from one mode to another, maybe even at the mode-line level of radar parameters."

What will be an increasing problem, however, is the increasing velocity of operations. The advent of hypersonic missiles, with speeds in the region of 2,000 m per second, means that platforms will soon face weapon engagement scenarios that will simply outpace traditional man-in-the-loop responses, said Bradbeer. "Just from an approximation, it becomes clear that if we can just about cope with legacy [subsonic] anti-ship missiles such as SS-N-25 'Switchblade' today, it is doubtful that we could counter the current generation of supersonic missiles such as Brahmos.

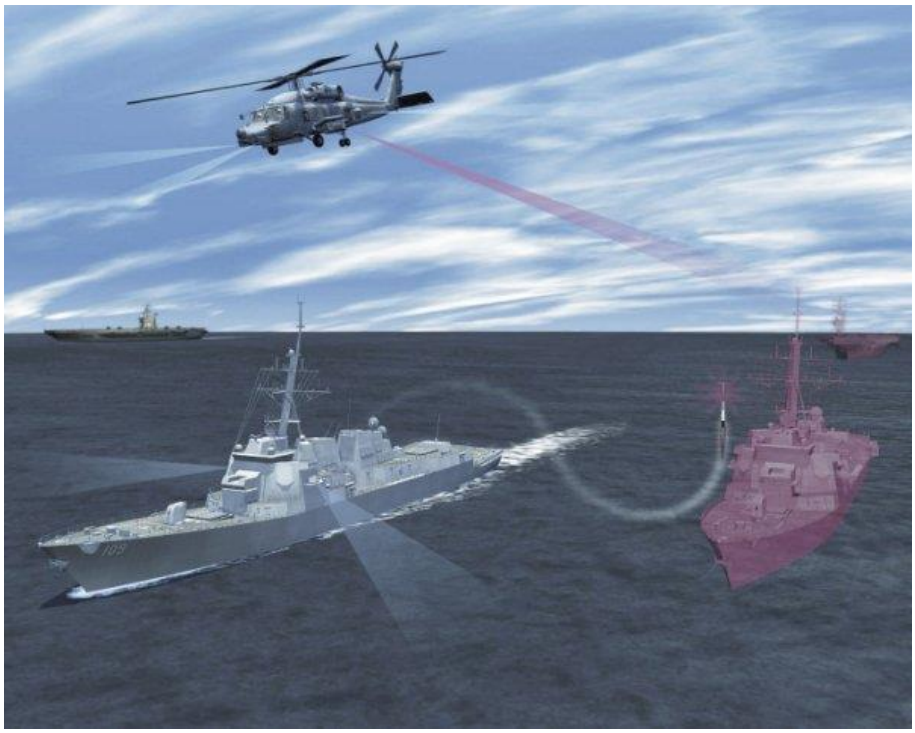


Future hypersonic missiles will massively compress the OODA loop. (MASS Consultants)

1704721

"Moreover, it seems inconceivable that a conventional operations room could even complete its decision-making cycle – let alone initiate any actions – before future hypersonic weapons like Zircon deliver their lethal effect."

According to Bradbeer, the detect-to-engage sequence – today still largely based on manual drills, decisions, and actions executed by the command team – needs to be automated through the exploitation of artificial intelligence methods, specifically machine learning. "[If] a defending platform thoroughly understands the threat kill chains in the local environment, and if that platform can sense and locate exactly where it is on an aggressor's kill chain, the defending platform can make appropriate responses and deploy countermeasures, hopefully long before the end game of trying to hard kill or soft kill a weapon that has already been launched," he said. "In fact, a series of machine learning-based awareness chains takes the general concept of a well-drilled, highly experienced operations room team, but applies it with machine-like rigour and speed, addressing more kill-chain options than is humanly possible, and operates on seemingly unconnected fragments, which may easily be missed by even the most experienced and diligent of human operators."



Lockheed Martin Rotary and Mission Systems is developing the podded AOEW Active Mission Payload (AMP). Designated AN/ALQ-248, the AMP pod will be borne aloft by MH-60R and MH-60S shipborne helicopters to deliver persistent surveillance and countermeasure capabilities against anti-ship missile threats. (Lockheed Martin)

1704722

He continued, "Machine learning has further roles to play in EW. Congestion and confusion are already a problem within our data-dominated world, and we should be honest … in recognising that having lots of data does not necessarily mean we have a clear, coherent picture of our environment. In fact, in some cases, it makes matters worse."

Bradbeer's third theme explored the convergence of EW and cyber, and echoed Hogben's call for a 'left shift' in kill-chain targeting. "If we consider typical 'platform protection' ECM, used by a defending platform against an attacker, the scope and penetration of that technique is actually quite limited… affecting predominantly the attacking platform's sensors and weapons," he said.

"Using a stand-off ECM approach, we could assert that we are reaching further back in to the kill chain [by] targeting sensors and C2 systems of supporting and co-ordinating platforms. However, there are still many parts of the kill chain that are not targeted by traditional [soft kill], and of course, traditional countermeasures tend to address the 'end game'.

Cyber, Bradbeer argued, offers a different mechanism by which to target the kill chain. "There is the potential to disrupt the data, processes, decision making, support infrastructure and C2 systems. For example, corrupting data before it can be made in to effective mission data sets or disrupting the supply chain of critical items. By incorporating cyber

techniques… it will be possible to attack further up the chain [i.e. earlier] and attack elements and components of the kill chain that traditional countermeasures just cannot reach."

[Continued in full version…]

Taking back control of the spectrum

Speaking to the AOC national convention in October 2013, the US Navy's (USN's) then Chief of Naval Operations (CNO) Admiral Jonathan Greenert promulgated a vision of a naval service that would strive to reclaim the electromagnetic spectrum in the years ahead. Using the term electromagnetic manoeuver warfare to characterise this emergent operational concept, he stressed the need for a supremely aware and highly agile approach to the exploitation the electromagnetic and cyber warfare domains.

Adm Greenert's successor as CNO, Admiral John Richardson, has committed himself to the same cause. His January 2016 headmark document, *'A Design for Maintaining Maritime Superiority* ,' outlined the need to further advance and ingrain information warfare, and expands the electromagnetic manoeuver warfare concept to encompass all of information warfare, to include space and cyberspace.

Part of this vision is the recapitalisation of the USN's surface ship EW and soft-kill capability, centred on the navy's shipborne Surface Electronic Warfare Improvement Program (SEWIP) and Advanced Offboard Electronic Warfare (AOEW) acquisition projects. SEWIP and AOEW reflect the desire of senior naval leadership to invest in priority capabilities that will enable the USN to remain ahead of adversary threats in the electromagnetic spectrum.

"Electronic warfare is a key part of the Surface Force Strategy," Rear Admiral Doug Small, Program Executive Officer for Integrated Warfare Systems (PEO IWS) in the Naval Sea Systems Command (NAVSEA), told delegates at the Surface Navy Association annual symposium in January 2017. "In an incremental fashion, we are delivery capabilities that [can] sense everything, and eventually we're going to be able to jam everything from on board ships and now offboard ships with the Advanced Offboard EW [AOEW] project we awarded recently.

"The idea is total theatre-wide tactical electronic warfare dominance," he continued. "We are putting the pieces in place to develop that capability."

SEWIP is an evolutionary acquisition and development programme, which incrementally upgrades the existing out-of-production AN/SLQ-32(V) EW system. SEWIP Block 1, delivered by General Dynamics Mission Systems, has focused on processor enhancement, and improvements in the human-machine interface (Block 1A), a specific emitter identification (SEI) receiver (Blocks 1B1 and 1B2), and high-gain/high-sensitivity (HGHS) receiver (Block 1B3). The SEI and HGHS capabilities provide for improved situational awareness.

The Block 2 instantiation, known as AN/SLQ-32(V)6, introduces an upgraded antenna, receiver, and combat system interface. Lockheed Martin delivered the first Block 2 system to the USN in the first half of 2014; the programme achieved full-rate production in September 2016 and the system is now being rolled out fleetwide to DDG-51 guided-missile destroyers.

SEWIP Block 3 is designed to deliver a common electronic attack (EA) capability to all USN surface combatants currently fitted with active jamming variants of AN/SLQ-32 (these being AN/SLQ-32(V)3 and AN/SLQ-32(V)4), plus selected new-construction platforms. The system, to be designated AN/SLQ-32(V)7, will be designed for installation on all required ship classes concurrently, and will be installed in two different configurations based on the size of the ship.

Northrop Grumman was in February 2015 selected for SEWIP Block 3 design and development ahead of a rival bid from Lockheed Martin (teamed with Raytheon). Building on the AN/SLQ-32(V)6, the AN/SLQ-32(V)7 embodiment introduces an integrated EA capability (encompassing a new transmitter, array, and associated jamming techniques) to protect against RF-guided threats. It also includes a government software development effort for a Soft-Kill Co-ordination System (SKCS) function to manage EA engagements.

The SEWIP Block 3 EA modification will bring specific enhancements in the areas of threat detection and identification, prioritisation, soft-kill co-ordination, and active radar jamming. Northrop Grumman's technical solution, using an active electronically scanned array based on Gallium Nitride transmit/receive modules, capitalises on technology previously matured under the Office of Naval Research's Integrated Topside programme.

Under an engineering and manufacturing development contract award notified in October 2015, Northrop Grumman is continuing to mature the AN/SLQ-32(V)7 system design, finalise integration, modelling and test plans, and produce two production-representative engineering development models (EDMs) for laboratory and field testing.

[Continued in full version…]

For the full version and more content: