MASS
A COHORT PLC COMPANY

Countermeasure Development in the AI Age

By Brian Tottingham

AUGUST 2018

VERSION NO.1

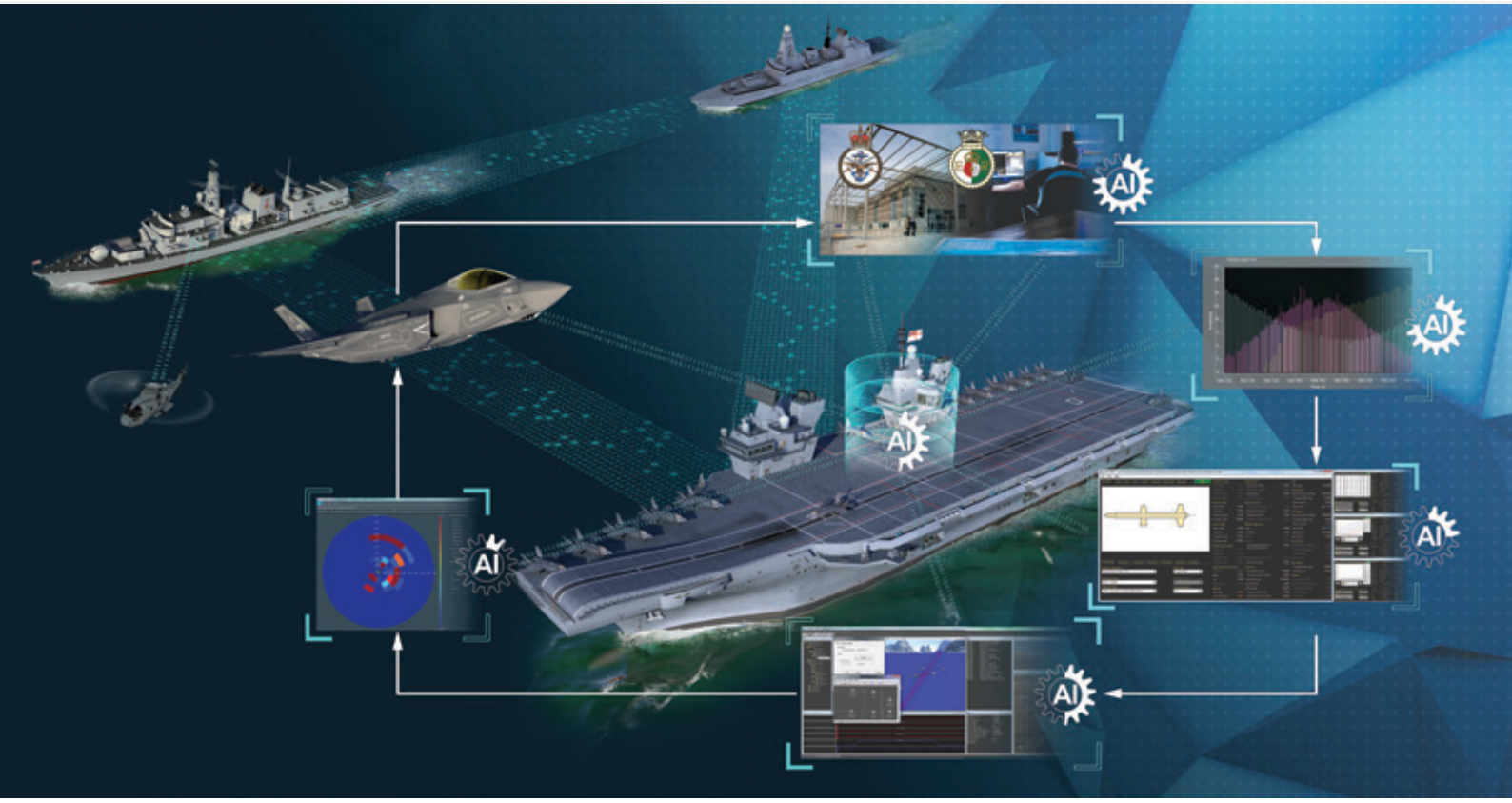
Prepared by:

MASS
Enterprise House | Great North Road
Little Paxton | St Neots
Cambridgeshire
PE19 6BN
United Kingdom

Tel: +44 (01480 222600
www.mass.co.uk
Email: systems@mass.co.uk

COUNTERMEASURE DEVELOPMENT IN THE AI AGE

“ZIPPO 6 inbound bearing 345 possible C802” The shrill excitement interspersed with fear is set within the tone of voice exploding from the Principal Warfare Officer as he shouts the warning, about the imminent threat, across the Ops room. Immediate action ensues, there’s more shouting, Chaff is dispensed, DLH, the Royal Navy’s active off-board decoy is fired and hard ship manoeuvres are performed. Equipment ‘black boxes’ kick into action performing counter-threat activities. Inbound threat signals are rapidly parameterised and compared to the data stored within the equipment’s memory. C-802 is found and the library allocates the ideal dispense sequence to the chaff launchers. Simultaneously other ‘black boxes’ use the threat parameters to allocate the countermeasure techniques and manoeuvre cues.



It sounds like a paragraph lifted from a Tom Clancy book, but this could be the fever of activity employed as a missile accelerates toward a ship. To get to this stage however, many activities have happened months or even years prior to the ship even sailing; largely un-noticed, teams of military personnel, scientists, mathematicians and engineers have undergone a regime of finding, acquiring, analysing data, developing countermeasures, programming each ‘black box’, testing, trialling and repeating this sequence of events to ensure that the ship and its crew will survive such an engagement. This is called the countermeasure development process and hundreds of people have been involved in one-way or another.

Artificial Intelligence (AI) can help

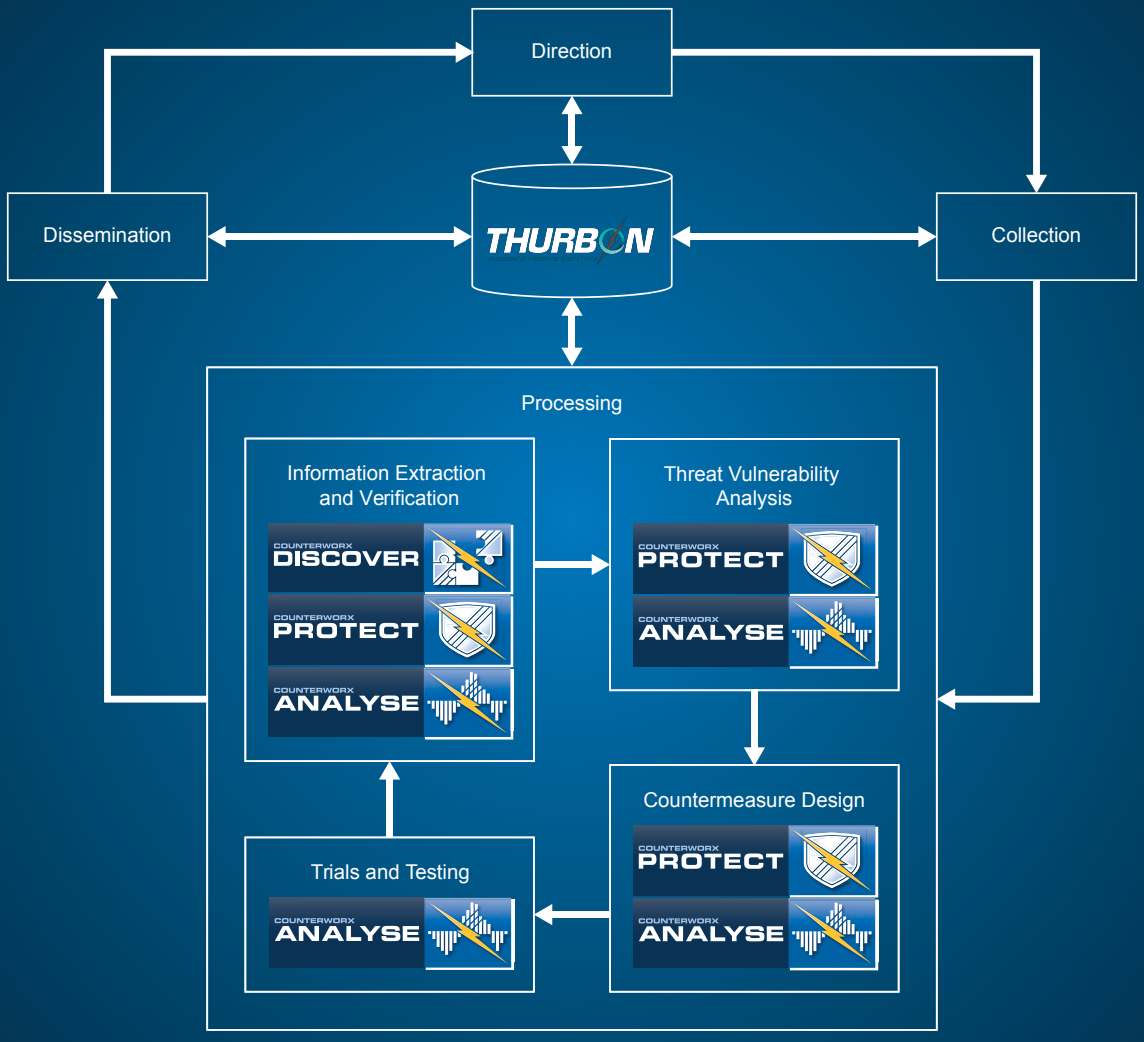
Fast forwarding and perhaps in some years to come, these activities will disappear into the background even more. As Artificial Intelligence (AI) forges its place in our modern world, Electronic Warfare (EW) will undoubtedly start adopting elements of AI and with it, will come some unforeseen benefits. The obvious ones, improved protection, faster, cheaper, fewer people, less operator involvement etc. are of course on the list but perhaps a few surprises will emerge too.

So what are the corner-stones that need to be considered to allow AI foundations to be built?

For the past couple of decades, the development of countermeasures has changed very little. Analysts individually develop their own tools to support their activities and the brains behind the process are seemingly housed in a relatively small number of people around the world. And it is for this reason that countermeasures development differs from one person to the next and is often referred to as “magic”. But does this need to be the case? What could be done to illicit this knowledge from these people and how can we ensure that they are all using the same, correct data?

The answers are actually relatively simple and un-exciting which has generally resulted in their half-hearted adoption or total disregard. Process and data management! The two are intrinsically entangled and it doesn’t take much to realise that a well-documented countermeasures development process enables all stakeholders to ensure they support all other stakeholders with the correct information and data.

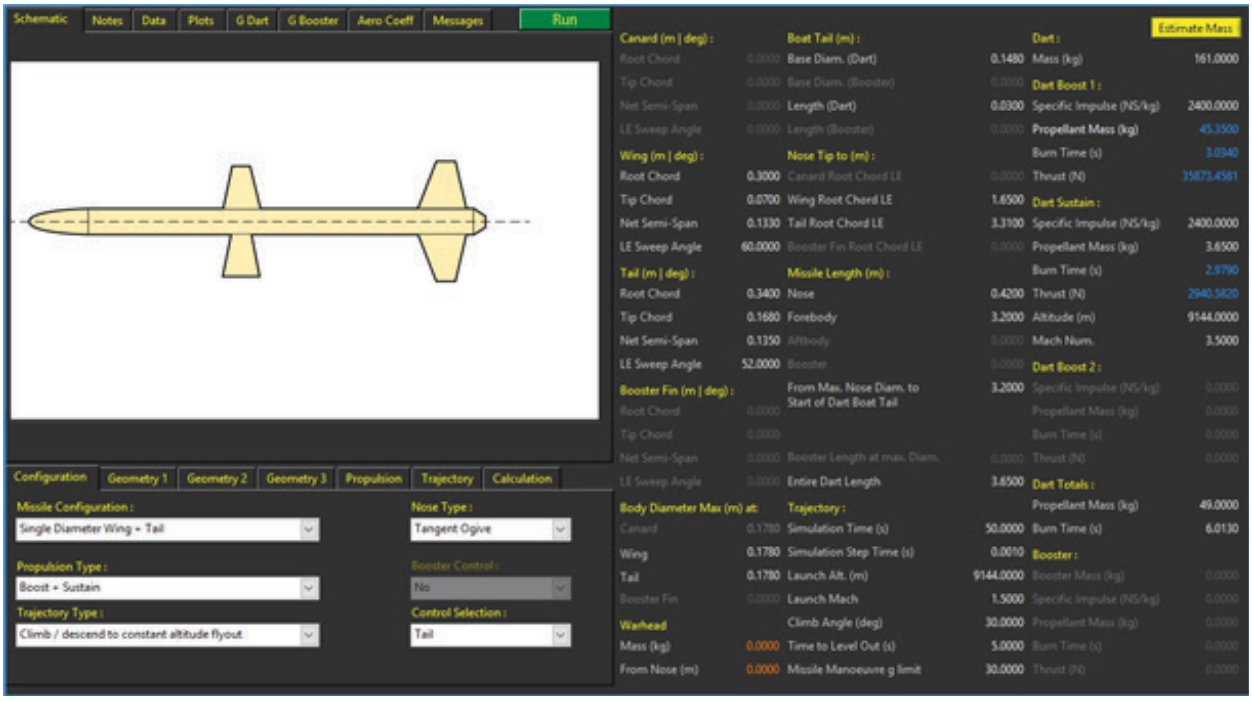
Furthermore, trying to define the countermeasures process highlights areas that are complex and could be supported with tailored tools that are better regulated and shared both locally and to wider stakeholders



The intelligence cycle, including the countermeasure (CM) cycle, stores all data within the THURBON data management system. A single toolset supports all stages of the CM cycle.

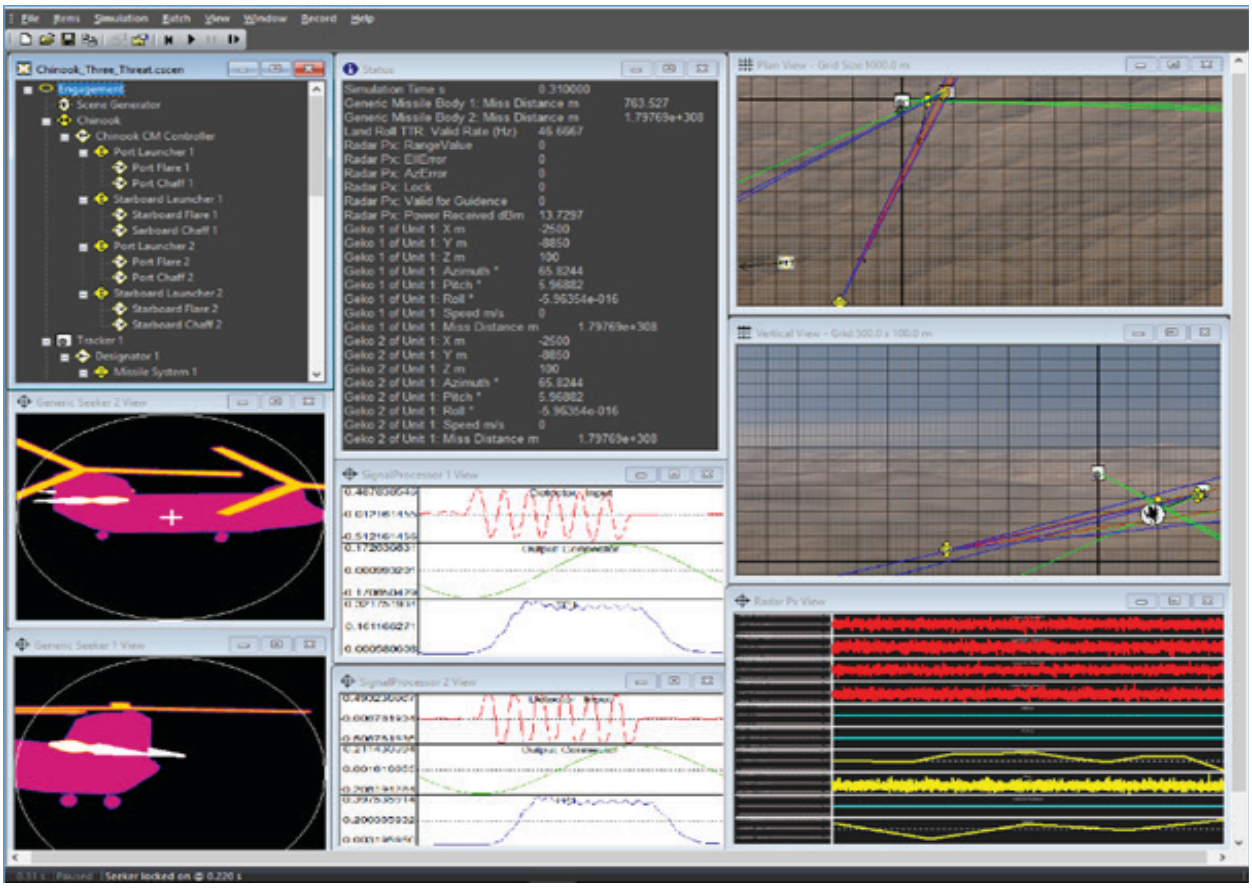
So how do these tools enable AI?

These newly “regulated” tools, could save time and money by reducing analyst time spent developing their own un-verified and un-validated tools, but also by enabling AI to supplement Intelligence Mission Data (IMD) ‘holes’ with data derived from physics ‘first principles’. The use of AI to filter threat data such that only realistic data is employed within the Data Management System (DMS) helps to reduce the analytical burden further and being able to automatically obtain and store EW data from open source intelligence helps to reduce the task of the Intelligence agencies.



Tools such as CounterWorX DISCOVER help to save time and money by enabling threat intelligence to be discovered, assessed and automatically ingested into the DMS.

The tools could expedite the generation of countermeasure tactics by enabling multi-domain (RF and/or IR), multi-environment (Air, Land and/or Sea), multi-platform and multi-threat engagements to be simulated. The risk of man-made data transfer errors and hence wasted development time, or worse still, ineffective countermeasures are significantly reduced and as previously suggested, the months or even years of countermeasure development are further reduced by being able to batch-run many scenarios, some of which, such as unavailable threat systems, may be impossible to replicate in trials. Once again machine learning algorithms may provide the answer to this lack of threat information by enabling manufacturing patterns to inform the modelling. For example, Kalman filters were first employed in the 1960s and hence modelling of 1950s weapon systems should not include Kalman filters. Having such tools also informs the required data being employed and so it becomes an easier task to reduce the amount of missing data, ‘data holes’, by using data mining techniques to source all data pertinent to the engagement.



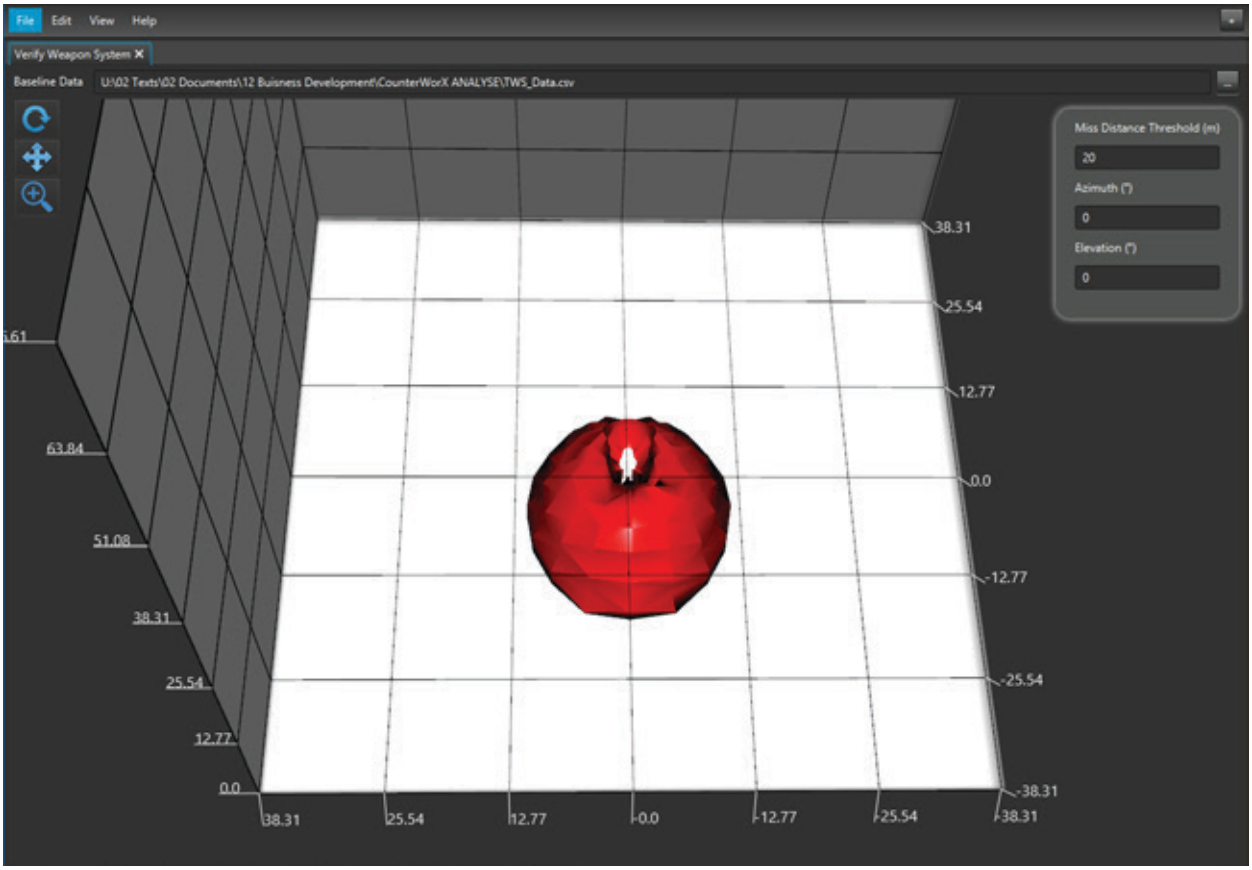
Experienced countermeasure developers save time and money by using multi-domain, multi-environment, multi-platform and multi-threat engagement modelling tools such as CounterWorX PROTECT to ensure effective countermeasures are assessed.

Machine learning within analysis tools improves countermeasure effectiveness

Similarly, tools designed to specifically support EW analysis, used in conjunction with the simulation software, will ensure expensive, time consuming sea, field or flight trials are either performed more quickly or targeted more effectively. Instinctively analysts run trials by changing one factor at a time and yet smart analysis tools incorporating machine learning algorithms, could reduce this burden on the analyst and trials teams by enabling multiple factors to be modified simultaneously within a single engagement. The result being that single factors as well as combinations of factors can be assessed more effectively. To use a basic analogy, it is well known that chaff has limited effectiveness on its own, as does manoeuvre, but combining the two can produce a very effective countermeasure. Being able to analyse combined factors is likely to provide improved capability for counters such as chaff where bundle deployment time, spacing, number of bundles, platform orientation, platform speed etc. are all factors. And if electronic countermeasures are considered, the number of factors and potential survivability increases exponentially.

Allowing for a new breed of tools which could be used by peers nationwide in multiple countermeasure and threat based organisations would reduce the need for individual analysts to develop their own un-verified or un-validated

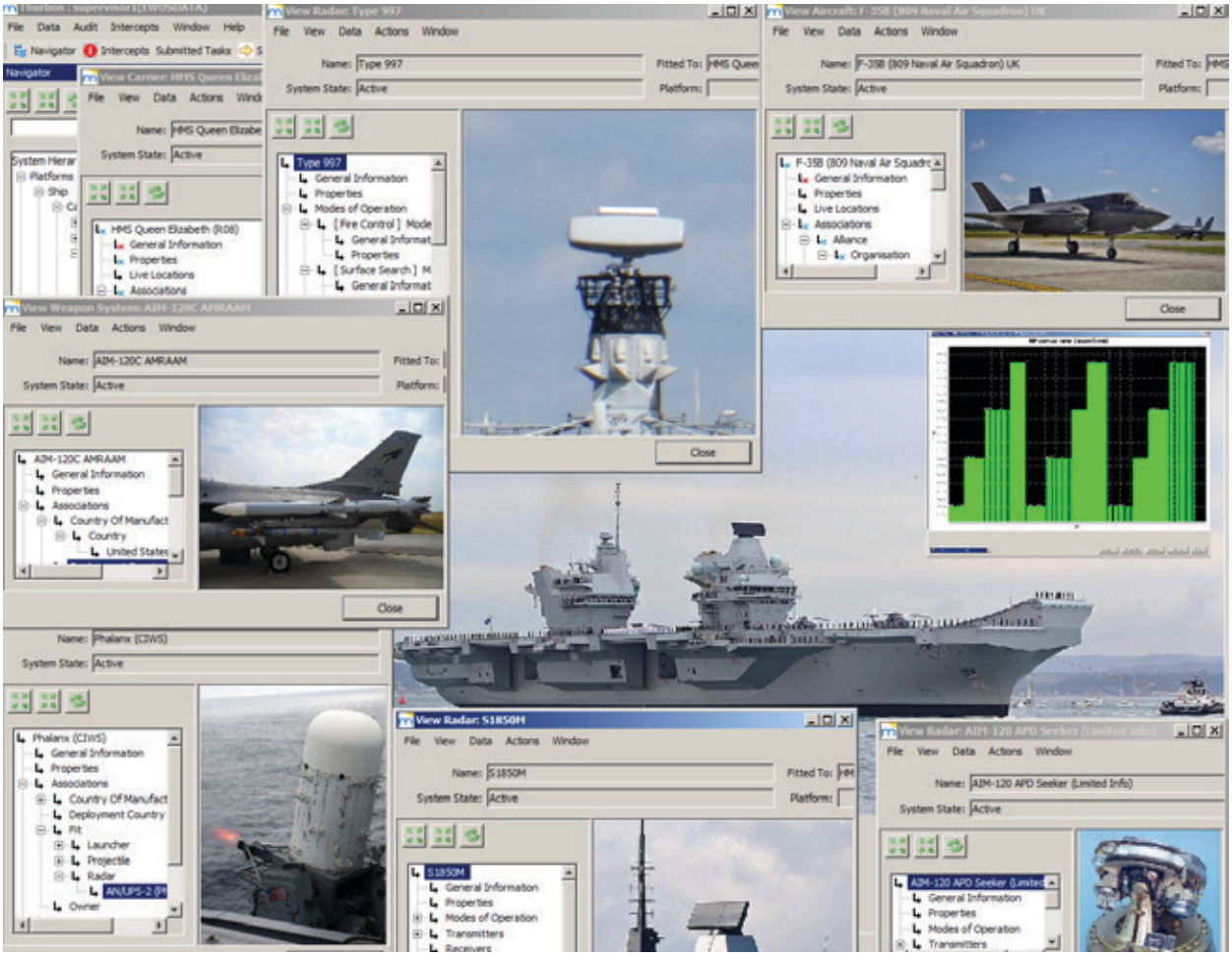
tools just to see how a countermeasure performs. EW analysis tasks, would benefit from the implementation of standard analysis methods developed and underwritten by analysis experts rather than countermeasures or threat systems experts. These could enhance trials design and execution bringing about much more focused trials, ultimately saving time, money and possibly even lives.



Proper statistical Proper statistical analysis is a complex task which can be supported with smart software tools such as CounterWorX ANALYSE to save time and money as trials become more focused.

The employed data is a critical consideration to operations

"Equipment 'black boxes' kick into action…" As this sentence, from our opening paragraph, is considered, it is realised that the equipment really is an unknown. Our military personnel's lives are utterly dependent on what that equipment 'knows' and yet every piece of equipment providing an identification function, relies on its own supporting database. So what happens when the active decoy round has been programmed with data that mismatches the data being used within the chaff launchers? Often the problems are deeper than that, with different parts of the military having separate databases. The result being that the Navy is potentially operating from alternative Intelligence Mission Data (IMD) to that of the Army who in turn have different IMD to that of the Air Force. And if any of that data is incorrect, questions arise for AI: Is the wrong algorithm being learnt? Is one equipment going to negate another? A single national Intelligence Mission Data Management System (DMS) enables all stakeholders and machine learning algorithms, to find, acquire, analyse, develop, program, test, trial and support all EW tasks from a single coherent and managed source of data. Erroneous data input is less likely due to the 'management' component of the DMS, but where it does occur the authority would be able to address the issue at the time of input, thus reducing time and effort spent trying to resolve these issues after the data has been collected.



Development of the countermeasures process and supporting tools has enabled MASS to identify the IMD requirements across EW, ensuring their tailored, system centric, EW Data Management System, THURBON, provides a single data solution for all stakeholders.

Bringing AI into EW has its challenges which are being overcome

Introducing AI and automation into the activities of the countermeasure development process is not without its challenges however. The two main challenges are of course that: stakeholders will have to invest time defining the process, and its relative data taxonomy, before automation is feasible and programming of labour intensive tasks into machine learning algorithms will require an increase in specialists with this skill set.

Perhaps less important, as automation is exploited, is the increased complexity of tools as more stakeholders define their requirements. On the face of it, it would seem that greater training would be required, but perhaps this would reduce as automation takes over and human interaction occurs less frequently. Verification and validation of such tools could be more of an issue that threatens the EW domain as AI becomes a reality.

The challenge confronting the EW domain seems quite daunting. Cohort plc company, MASS, however, has realised the benefit of amalgamating the knowledge of the experts and their individual countermeasure development tools. A single, linked set of verified tailored tools, facilitates the consistent flow of data through MASS' operationally employed countermeasure development process. Yet being able to decipher collected data accurately and more rapidly, operate on parts of the intelligence cycle earlier whilst informing and developing countermeasures within the engagement time, remains a challenge.

The opening paragraph's "…*Equipment 'black boxes' kick into action*…" is better managed and delivered by the MASS toolset. The THURBON DMS provides that single data solution that can 'feed' those 'black boxes' and its multi-level security capability enables more effective coalition interoperability.

MASS has laid the corner-stones to evolve toward an AI solution. Their vision, to use machine learning algorithms to enhance the interpretation of collected data, employ a combined cyber and AI solution that enables earlier 'intelligence cycle' activities and use machine learning to inform countermeasure actions before the threat is viable, is within reach. Ultimately MASS aim to utilise AI to enable countermeasure development as that 'C802', or any unknown threat, is inbound.

For further information, please contact
ewos@mass.co.uk or call +44 (0)1480 222 600