COGNITIVE ELECTRONIC WARFARE

Dr. Karen Zita Haigh *and* **Julia Andrusenko** *outline the opportunities to use AI in situation assessment for electronic battle management*

The challenges of modern Electronic Warfare (EW) are beyond the ability of traditional approaches to solve. Incorporating Artificial Intelligence techniques into EW systems is the only way to manage the complexity of this problem domain and its rapid timescales. The recently released *Cognitive EW: An AI Approach* describes how AI techniques can help address the challenges of modern EW. The book expects readers to be familiar with at least one of EW, Cognitive Radio or Cognitive Radar domains, and focuses instead on the AI techniques and their associated challenges and tradeoffs. The AI techniques presented apply to cyber and information warfare, but the book does not directly address these related areas.

In the future, AI will be part of every EW system, recording and analysing system previous performance and then adapting behaviour according to the current situation. AI – not just Machine Learning (ML) – is the heart of future Cognitive EW solutions.

What Makes a Cognitive System? A cognitive system perceives its environment and takes actions to achieve its goals. It reasons and understands at a higher level, dealing with symbolic and conceptual information, to make accurate decisions in complex situations. Cognitive systems are aware of context, handle uncertainty, and make judgements autonomously. They are iterative and interactive, and learn from their experiences.

Situation Assessment (SA) is the understanding of the environment and events. Decision Making (DM) sets goals and determines feasible methods of achieving them. Machine Learning extracts information from prior experience to improve future performance. Machine learning techniques may extract rules about how to interpret observations or behave, or they may build functions that approximate the performance of the data.

Electronic warfare focuses on how to control the spectrum or attack an enemy using the electromagnetic spectrum. Electronic Support (ES) understands the spectrum – who is using it, how, when and where. Electronic Protect (EP) involves actions taken to protect the friendly nodes from any undesirable effects due to changes in the spectrum such as jamming or noise. Electronic Attack (EA) denies the adversary access to their own spectrum. Electronic Battle Management (EBM) oversees all aspects of Electromagnetic Spectrum Operations to increase mission effectiveness, including managing changing mission priorities, coordinating effects and collaborating with humans and other elements of mission command.

In the future, AI will be part of every EW system, recording and analysing system performance and then adapting behaviour according to the situation

Electronic Support determines who is using the spectrum, where and when they are using it and whether there are patterns that can be exploited. It describes the signal environment, including features such as instantaneous energy, frequency, scattering and repetition patterns, and their probabilities. ES can combine traditional SIGINT features to offset limited data, Deep Learning models for latent feature generation and classical machine learning models for in-mission-updates. This characterisation and characterisation step provides the foundation for effective spectrum understanding.

Electronic Support does not have to solely rely on the RF data: the data can be fused with non-RF data such as video and still imagery, free space optics or open-source, tactical or operational intelligence. Distributed data fusion across multiple heterogeneous sources must create a coherent battlespace spectrum common operating picture that is accurate in space, time and frequency. Anomaly detection, Causal reasoning and intent inference complete the picture to understand the impact of events and support decision making.

An Electronic Warfare system must choose actions to accomplish mission objectives, given whatever context it knows about the environment and the tasks: the platform(s) have a set of capabilities and the cognitive decision maker composes these into strategies to achieve the desired performance. It is through these knobs, or degrees of freedom, that the EW system can accomplish its goals. From an AI standpoint, Electronic Protect and Electronic Attack differ only in their objectives: EP defines objectives with respect to oneself, while EA defines objectives with respect to the adversary. Likewise, AI is agnostic to whether the solutions apply to radar or communications (or cybersecurity) problems.

Two key reasons for AI-based decision making are time and complexity. Decision-making time requirements are faster than humans are capable of. Moreover, the domain has too many inputs for a human to understand quickly and too many choices for a human to analyse, particularly when jointly optimising EP/EA and comms/radar.

An automated Electronic Warfare decision-maker is interactive and can respond to events as they occur during the mission. Automated planning activities overlap optimisation and scheduling, and will become fully interactive integrated systems in the future.

Planning synthesises a sequence of actions that result in a desired goal state. Planning is what to do and in what order, as a partially ordered graph. Planning is more strategic, more global. An EBM system plans how many platforms to deploy, which resources each gets and where they will go. Electronic Battle Management describes the Electronic Warfare planning problem, which is at a higher level than scheduling and optimisation.

Optimisation evaluates multiple plans to choose the 'best' one. Optimisation is more tactical, more local. An EW system optimises EP and EA metrics like power usage, probability of detection and Electronic Warfare BDA.

Scheduling maps a partially ordered plan to specific resources and timeslots. Scheduling worries about when and how to do things. Scheduling drives down into the specifics of when to transmit and when to receive.

A variety of techniques exist to handle distributed decision-making, information uncertainty, action uncertainty and trade off decision-quality with time required to make a decision.

Real-world environments are usually too complex to collect data that covers all expected situations. In EW, moreover, systems will encounter novel conditions that cannot be captured in any lab setting. In-mission learning allows the system to learn in situ, where learning is most beneficial and most needed.

Reinforcement Learning (RL) is a goal-directed learning approach wherein individuals interact with the environment to improve their performance over time. In EW, RL means that the system can take an EP or EA action in the environment, collect feedback, and evaluate its own performance. Much of the common research in RL is based on Markov Decision Processes (MDPs) to the extent that RL is almost synonymous with MDP. It's not: RL is not defined by the learning method, but by the learning problem and direct interaction with the environment. In fact, MDP-based Reinforcement Learning is generally inappropriate for in-mission EW due to computational complexity and the number of training samples required.

COGNITIVE SYSTEMS ARE AWARE OF CONTEXT, CAN HANDLE UNCERTAINTY, AND MAKE JUDGEMENTS

IN-MISSION MACHINE LEARNING

Support Vector Machines (SVMs) are an effective method for Reinforcement Learning in Electronic Warfare. SVMs learn from small numbers of training examples (even just a single example), and do not require large compute capability – they can be computed on FPGAs or CPUs in sub-millisecond timeframes. As a concrete example, the BBN Strategy Optimiser (SO) uses Support Vector Machines to perform real-time in-mission learning for communications Electronic Protect (see table overleaf). The Strategy Optimiser learns how different strategies impact networked communications performance in the presence of previously unknown interference and jamming conditions and then optimises performance in real time. The SO comprises a Rapid Response Engine (RRE) that makes strategy decisions, and a Long Term Response Engine (LTRE) that learns the models of how strategies perform. The SO is the first known communications Electronic Protect system to use Machine Learning in mission, at mission-relevant timescales. Results demonstrate that in-mission learning allows the system to perform well, even when provided with no initial training data.

To validate a cognitive decision engine, a closed-loop testing framework is essential. Machine Learning systems commonly use static datasets to learn how to classify objects. In Electronic Warfare, this approach is insufficient because it doesn't show how the system handles novel examples, responds to dynamic situations or operates

against an adversary. The environment responds to every action. Therefore, learning systems should be verified with both empirical and formal methods (or a combination thereof).

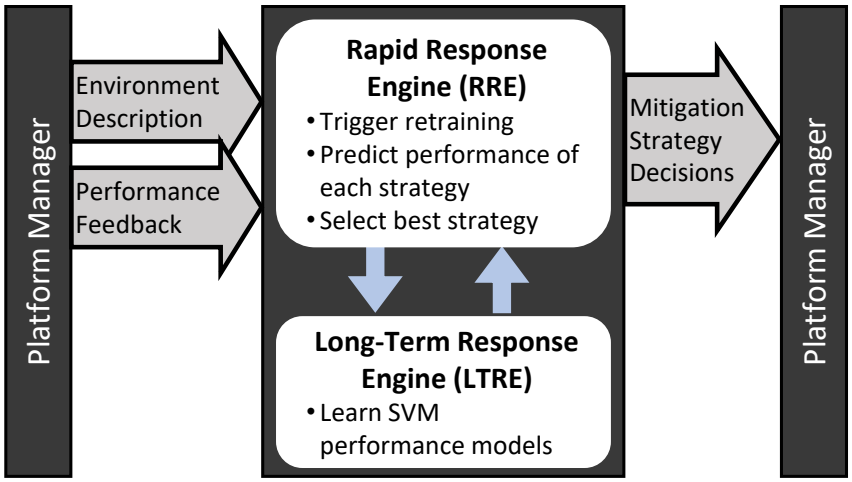
An effective empirical technique that demonstrates that the cognitive system can learn to generalise from its experience to handle novel environments is n-choose-k ablation testing. In ablation tests, we train the system on known cases and test on all n, for all values of k and all subsets . Thus, during the test, environments are novel. Ablation tests are similar to leave-one-out testing, and k-fold cross validation, in that all three methods train on a subset of the data, and test on novel data. The idea is to demonstrate that the system can learn to handle new environments, regardless of what it was initially trained on, and thus build confidence that the system will operate effectively during a real EW mission.

TWO KEY REASONS FOR AI-BASED DECISION MAKING ARE TIME AND COMPLEXITY

Creating a Cognitive Electronic Warfare system is not the hurdle that many believe. It's easy to start small and grow. Starting small develops (human) expertise and awareness of which details will affect the final product. The key steps are to: choose a bite-sized task; choose an AI toolkit and prototype a model; evaluate with representative data in a closed-loop setting; and implement on representative hardware. The book presents tradeoffs for choosing AI/ML tools, techniques for managing data, considerations for both software and hardware architectures, human factors, and methods for evaluating the system.

Building a cognitive Electronic Warfare system requires understanding what and where AI can help: situation assessment for Electronic Support and understanding the RF environment, decision making for choosing Electronic Protect/Electronic Attack/Electronic Battle Management actions and Machine Learning for continuous improvement. This high-tempo complex environment is well-suited to the application of AI ●

Dr. Karen Zita Haigh and **Julia Andrusenko** are the authors of the book *Cognitive Electronic Warfare: An Artificial Intelligence Approach*. Artech House, 2021.



The BBN Strategy Optimiser performs real-time in-mission learning and optimisation for communications EP

Picture credit: FCrown Copyright