A Conceptual Architecture of Cognitive Electronic Warfare System

Qinghan Xiao
Radar Electronic Warfare Section
Defence R&D Canada – Ottawa Research Centre
Ottawa, Canada
e-mail: Qinghan.Xiao@drdc-rddc.gc.ca

***Abstract*—The major motivation behind research on cognitive Electronic Warfare (EW) is the requirement to defeat modern radar systems using emerging technologies, especially cognitive algorithms. Using cognition-based techniques, a radar system would be able to perceive its operational environment, fine-tune and accordingly adjust its emission parameters, such as the pulse width, pulse repetition interval, and transmitter power, to perform its assigned task optimally. It is certain that traditional EW methods, which rely on pre-programmed attack strategies, will not be able to efficiently engage with modern radar threats. Therefore, the next generation of EW systems needs to be enhanced with cognitive abilities so that they can make autonomous decisions in response to changing situations, and cope with new, unknown radar signals. In this paper, a conceptual architecture of a cognitive EW system is presented. The system consists of five major functional components, namely: environmental perception to observe the operational environment; intelligent signal analysis to assess and characterize electromagnetic spectrum signals emitted by enemy radars; a cognitive thinking module to produce close-to-optimal jamming solutions; a dynamic knowledge base that continues to grow during the operation; and a feedback loop as a facilitator of intelligence to improve the jamming performance. The system architecture and functional modules are described in detail.**

Keywords-adaprive electronic warfare; cognitive electronic warfare; machine leaning; cognitive thinking.

I. INTRODUCTION

In recent years, there are growing research interests in the development of cognitive capabilities in various electronic systems. Mitola and Maguire first introduced the concept of cognitive radio in 1999 [1]. In 2006, Haykin proposed the idea of cognitive radar, which is a dynamic system that adapts and optimizes transmitted waveforms based on the operational environment [2]. The proposed cognitive radar system is characterized by the following three key features: (1) the receiver learns, iteratively, from experience gained through interaction with the environment; (2) the transmitter adapts its illumination of the environment in an optimal manner in accordance with information about the environment passed on to it by the receiver; and (3) the feedback link coordinates and optimizes the operations of the transmitter and receiver in a synchronous manner [3]. Different from traditional radar systems, cognitive abilities could allow a radar to fine-tune and adjust its emission parameters, such as the pulse width, pulse repetition interval, power, and pulse compression technique, to perform its assigned task optimally. Therefore, to defend against cognitive radar systems, cognition is the key to the next generation Electronic Warfare (EW) system. The US Air Force Science Advisory Board carried out a study entitled, “Responding to Uncertain or Adaptive Threats in Electronic Warfare” in 2016. It pointed out that, “increasing signal density and highly variable or real-time adaptive waveforms and modalities will challenge the ability of Air Force systems to identify source and intent of signals in the Radio Frequency (RF) spectrum” [4]. Legacy EW systems that rely on databases of known threats and predefined countermeasures lack the ability to identify and respond to parameter agile radars in real time. Therefore, the front-end of EW system, Electronic Support (ES), and the back-end of the system, Electronic Attack (EA), need to be enhanced with intelligence to provide accurate situational awareness information through ES, and decide where and how to apply jamming through EA.

As shown in Figure 1, a basic cognitive EW system should include five modules: signal analysis and characterization, countermeasure preparedness and response, countermeasure effectiveness assessment, a database to hold a priori and dynamic knowledge of the operational environment and threats, and a feedback loop encompassing the environment, receiver and transmitter [5][6]. In the system, Environmental Perception focuses on sensing of the operational environment to optimize further processing procedures based on the surrounding environment. Intelligent Signal Characterization block performs pattern recognition and uses machine learning algorithms to assess and characterize electromagnetic spectrum signals emitting from enemy radars as either known or unknown threats. The objective of the Cognitive Thinking module is to synthesize close-to-optimal countermeasures subject to transceiver limitations, user-input restrictions and performance goals. The Dynamic Knowledge Base contains not only environmental, target, and other a priori information, but also information on recently learned threats. The Feedback loop plays a key role in causing the transmission parameters to be adjusted in order to improve the jamming performance in real time.

The rest of the paper is organized as follows. Section II discusses the major differences between adaptive EW and cognitive EW. Section III presents a cognitive EW system architecture, and finally, Section IV concludes the paper.

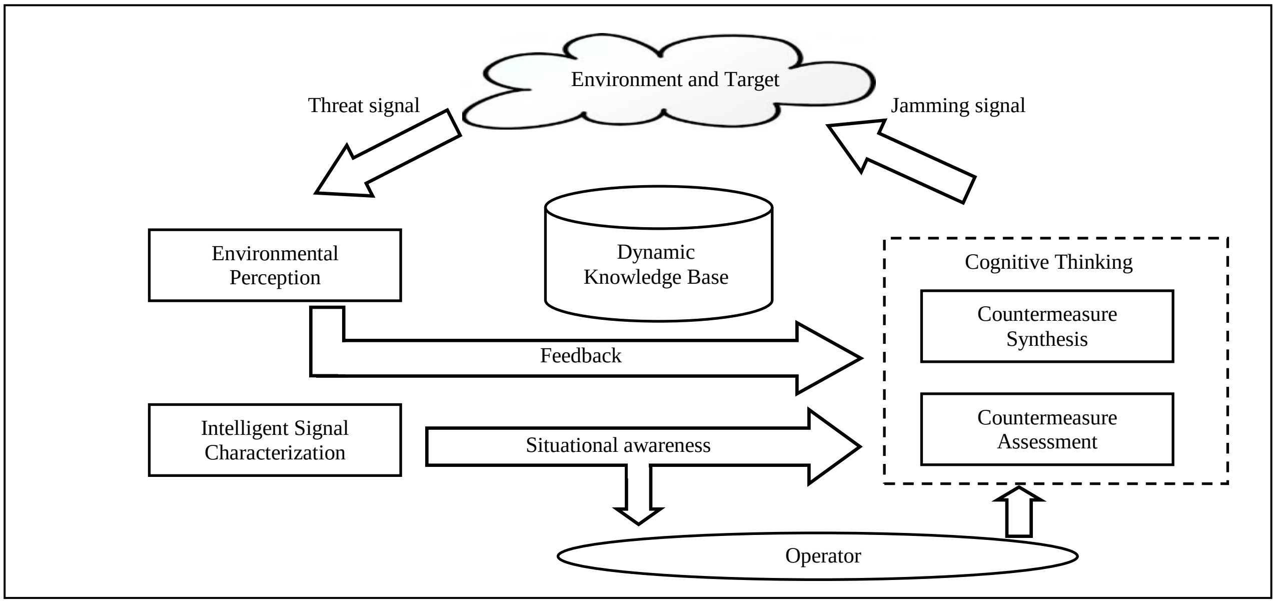

Figure 1. Basic cognitive EW system.

II. ADAPTIVE EW AND COGNITIVE EW

Over the past few years, the terms adaptive EW and cognitive EW have been used interchangeably by many people. In [7], the author raised the following questions: What is the difference between adaptive and cognitive electronic warfare? Does it even matter? This section is intended to address these questions.

A. Adaptive EW

The advances of digital radar technology have led to a shift in the way legacy EW is executed and raised the need for more advanced EW solutions. Adaptive EW is proposed in the literature as being capable of recognizing a change in the operating environment, and then selecting from a series of predetermined EA actions that have been deemed to be optimized in an off-line environment [7][8]. For example, when the receiver detects a target radar changing its transmit frequency, the EW system adapts the transmitter to the corresponding frequency band. The main properties are summarized as follows:

- Adaptive EW is reactive;
- ES identification relies on a pre-programmed library;
- EA responses are pre-programmed solutions; and
- The system operates with a feedback mechanism between transmitter and receiver, which is independent of the environment.

B. Cognitive EW

The concept of cognitive EW is based on a perception-learning-action framework, which is one step beyond that of adaptive EW (Figure 2). Not only would a cognitive EW system adapt based on what it observes, but also it should use machine learning and pattern recognition algorithms to mimic human mental processes of perception, memory, judgment, and reasoning. Cognitive EW needs to be a dynamic closed-loop feedback system that would enable an intelligent response to defeat threat radars.

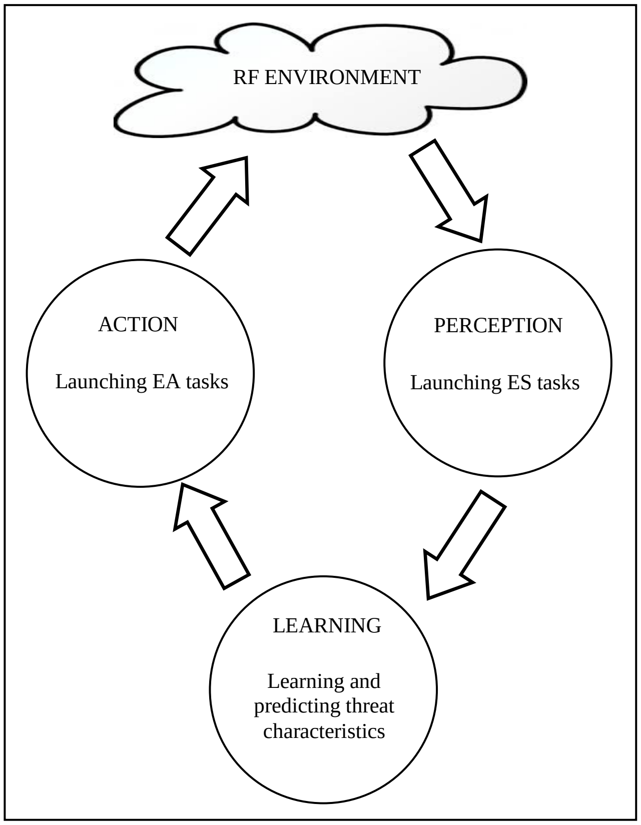

Figure 2. Perception-learning-action loop.

Artificial Intelligence (AI) and machine learning could make it possible for a cognitive EW system to exploit unknown radar waveforms that the system has never seen before. A feedback mechanism could possibly coordinate the operations of the transmitter and receiver to achieve optimal jamming performance. The following are the key features of cognitive EW with which cognitive EW needs to be proactive, i.e., it would:

- Adaptive EW is reactive;
- ES identification relies on a pre-programmed library;
- Attempt to learn the target's dynamic states and account for time-varying environmental conditions;
- Operate as a dynamic closed-loop feedback system encompassing the transmitter, environment and receiver; and
- Produce effective countermeasures against a threat radar even for a new or unknown threat.

C. *Major Differences*

As discussed in the previous sections, there are several fundamental differences between cognitive EW and adaptive EW. Mark Pomerleau stated in his article [7], “differentiating between different levels of adaptability and true cognitive EW is important”, although a few experts viewed it differently [8]. An adaptive EW system adapts and responds to a threat in a pre-programmed manner, either based on rules or pre-processed knowledge obtained off-line. A cognitive EW system would overcome the limitations of the rule-based or knowledge-based adaptive EW system through machine learning to make the system better aware of the environment in which it is being used, and then characterize the threat and determine appropriate countermeasures. Let us conclude this section with three remarks:

- A cognitive EW system should continuously learn about the environment through experience gained from its interactions with the environment, and should continuously update itself with relevant information.
- The transmitter could deploy jamming signals in an intelligent manner which would:
  - take into account factors such as threat function, the relative positions and motions of targets, and construct optimal countermeasures techniques;
  - assess countermeasure effectiveness; and
  - adjust the countermeasure appropriately in order to maintain optimal effectiveness.
- The whole EW system would constitute a closed-loop dynamic system, which should encompass the transmitter, environmental, receiver, and feedback channel.

III. SYSTEM ARCHITECTURE

Based on above analysis, a conceptual architecture of a cognitive EW system is developed. Figure 3 shows a functional block diagram of the proposed system. The following important aspects distinguish a cognitive EW system from a legacy EW system.

A. *Closed-Loop*

A legacy EW system has an open-loop structure that does not assess the jamming effectiveness in real-time. A cognitive EW system needs to be a closed-loop system that performs environmental analysis, signal characterization, countermeasure synthesis, and countermeasure effectiveness assessment in real-time. It would continually adjust its jamming strategy based on feedback concerning threat behavior.

B. *Completely Automated*

In order to devise countermeasures in real-time, a cognitive EW system needs to continuously learn about the dynamically changing environment, automatically generate an optimized jamming technique and evaluate its effectiveness. Therefore, it is necessary to perform autonomous decision-making in real time.

C. *Machine Learning*

In contrast to static and adaptive EW systems that rely on pre-programmed threat libraries, a cognitive EW system needs to be able to analyze signals that have not previously been encountered, devise effective countermeasures, assess their effectiveness, and predict future threat emissions, all in real time. Therefore, machine learning is a basic ingredient of a cognitive EW system with which to learn and predict threat characteristics, and to automatically generate effective countermeasures by reasoning about past experiences.

D. *Fuzzy Reasoning*

Fuzzy Logic is an AI technique that can handle ill-defined, imprecise systems, and therefore enables a system using imprecise concepts and dependencies to reason about target systems [9]. Due to dynamic changes in the electromagnetic spectrum environment, fuzzy reasoning is a good tool to address uncertainty and deal with unexpected inputs by modeling human behavior to provide approximate reasoning when precise information is not available.

IV. CASE STUDIES

In order to gain a better understanding of the differences between cognitive EW and adaptive EW, two case studies are described and discussed in this section. The first one is about dealing with a previously unknown radar signal. As mentioned above, an adaptive EW system relies on libraries of known emitter (radar, communications, electro-optical, etc.) waveforms to identify the threat and determine the appropriate countermeasures response. To detect, deceive, and defeat enemy radar threats using new waveforms and unknown techniques, the adaptive solution involves collecting evidence and analyzing it in a laboratory for countermeasure development. There are two challenges: (1) it may take months to develop and deploy new profiles and countermeasures; and (2) when the received signal is slightly out of tolerance compared to what was recorded in

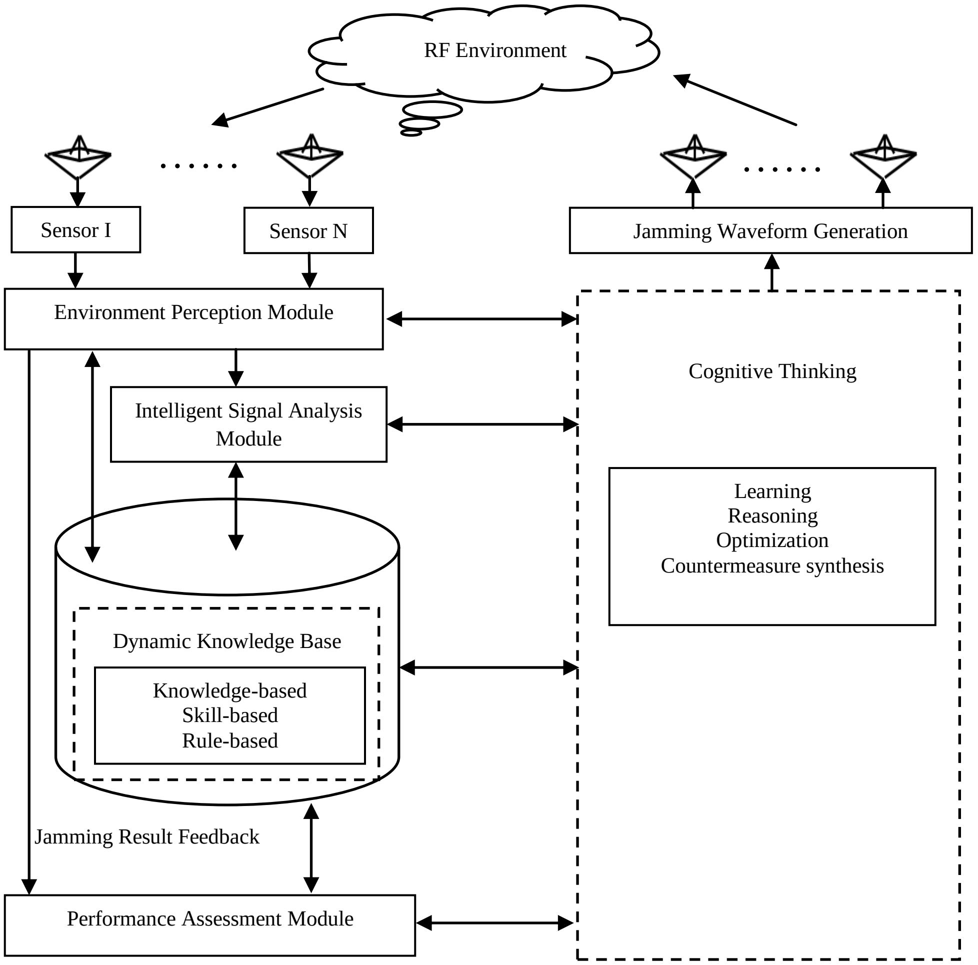

Figure 3. Functional block diagram of a cognitive EW system.

the library, the threat emitter cannot be identified and defeated. On the contrary, a cognitive EW system would use AI and machine learning to detect, characterize, and counter both known and unknown threat transmissions in real time. It would start by analyzing the electromagnetic spectrum environment. If changes are detected, then it is reasonable to conclude that new or unknown radar emitters are present. The environmental change would then be extracted for spectrum analysis. Machine learning algorithms would be used to characterize and predict the threat's properties and capabilities. The second example concerns the appropriate countermeasures response. As mentioned above, an adaptive EW system is only reactive' to the received data stream, which relies on a pre-programmed library to provide a specific, pre-determined countermeasure. With a dynamic knowledge base, a cognitive EW system would generate a dynamic action library consisting of several countermeasures options, and perform perception-learning-action feedback cycles to determine the optimal one.

V. CONCLUSIONS AND FUTURE WORKS

With the evolution of radar systems from fixed analogue systems to programmable digital variants, it is possible to endow radars with the ability to produce an almost infinite variety of signals. These developments have made legacy EW systems less and less effective against modern radar systems, especially those that are highly adaptive or cognitive [10]. The introduction of cognition into engineering systems is therefore key to the development of next generation EW systems. In this paper, a conceptual architecture of a cognitive EW system is presented, based on a perception-learning-action framework. Its major components include: an environmental perception module, an intelligent signal analysis module, a cognitive thinking module, a dynamic knowledge base, and a performance feedback module. The important aspects that distinguish a cognitive EW system from a legacy EW system are discussed in detail. This is the first step in the development of novel cognitive EW techniques. Further research will address the following issues: (1) development of analytic abilities to perceive the surrounding environment; (2)

application of machine learning techniques to characterize previously unknown radar signals; and (3) implementation of fuzzy logic techniques to deal with environmental uncertainty.

REFERENCES

[1] J. Mitola III and G. Q. Maguire, Jr., “Cognitive radio: Making software radios more personal,” IEEE Personal Commun., vol. 6, no. 4, pp. 13–18, August 1999.

[2] S. Haykin, “Cognitive radar: A way of the future,” IEEE Signal Processing Magazine, vol. 23, no. 1, pp. 30-40, Jauary 2006.

[3] S. Haykin, “Cognition is the key to the next generation of radar systems,” Proc. of the 13th IEEE Digital Signal Processing Workshop and 5th IEEE Signal Processing Education Workshop (DSP/SPE ’09), January 2009, pp. 463–467.

[4] USAF Scientific Advisory Board. *Responding to Uncertain or Adaptive Threats in Electronic Warfare*. [Online]. Available from: http://www.scientificadvisoryboard.af.mil/About-Us/Fact-Sheets/Display/Article/878167/fy16-study-tors/, (Access date: 13 September 2017).

[5] S. Cole, “Cognitive electronic warfare: Countering threats posed by adaptive radars,” Military Embedded Systems, pp. 16-19, January/February 2017.

[6] B. H. Kirk, R. M. Narayanan, A. F. Martone, and K. D. Sherbondy, “Waveform design for cognitive radar: Target detection in heavy clutter,” Proc. of SPIE Radar Sensor Technology XX, vol. 9829, 13 pages, 30 June 2016.

[7] M. Pomerleau, “What is the difference between adaptive and cognitive electronic warfare?” C4ISRNET. [Online]. http://www.c4isrnet.com/c2-comms/2016/12/16/what-is-the-difference-between-adaptive-and-cognitive-electronic-warfare/, (Access date: 14 September 2017).

[8] J. Knowles, “Regaining the advantage – Cognitive electronic warfare,” The Journal of Electronic Defense, vol. 39, no. 12, pp. 56-62, December 2016.

[9] S. Lee-Urban, et al. “CORA: A flexible hybrid approach to building cognitive systems,” Proc. of the Third Annual Conference on Advances in Cognitive Systems, Poster Collection, 2015, pp. 1-16.

[10] M. Arik and O. B. Akan, “Enabling cognition on electronic countermeasure systems against next-generation radars,” Proc. IEEE Military Communications Conference 2015 (MILCOM 2015), October 2015, pp. 1103-1108.