Development of a Mobile Electronic Warfare System

Dr Abdullah Alshammary
King Abdulaziz City for Science and Technology (KACST), Saudi Arabia
ashammary@kacst.edu.sa

***Abstract*— Military communications utilize sophisticated modulations and tactics that are challenging to intercept and track. Communications intelligence (COMINT) is the act of gathering intelligence about the enemy communications channels and its contents in order to enable interception of messages or interruption of the command and control flow. King Abdulaziz City for Science and Technology (KACST) and Grintek Ewation (GEW) have collaborated on a series of joint development projects to develop an integrated communications intelligence, electronic support and electronic attack system. The last stage of this cooperation was to integrate all of these capabilities into a mobile system. This final product has been tested and demonstrated in various military trials. This approach supports the creation of a local industry to supply the Royal Saudi Land Force (RSLF) and other military users with a COMINT and Electronic Warfare (EW) capability and contribute to the national 2030 vision by localizing the supply of military products and services.**

Keywords—component; formatting; style; styling; insert (key words)

I. INTRODUCTION

Electronic Warfare is defined as a military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent the hostile use of the electromagnetic spectrum but which retains friendly usage of the electromagnetic spectrum. EW is divided into four categories [1]:

1. Electronic Support (ES), formally Electronic Support Measures (ESM), is the utilization of electromagnetic energy to search for, intercept, identify, and locate sources of electromagnetic radiation for the purpose of immediate threat recognition. For example, the Radar Warning Receiver (RWR) is an ES system installed in almost all military aircrafts to identify Radar threats.
2. Electronic Attack (EA), or Electronic Counter Measures (ECM), prevents the enemy from utilizing ES by denying them the use of electromagnetic energy. For example, EA-6B Prowler aircraft act as a stand-off jammer in the US military fleet.
3. Electronic Protection (AP), formally Electronic Counter Counter Measures (ECCM), is the protecting of electronic support measures from electronic attack. For example, sidelobe antennas installed in many Radar protects the Radar from sidelobe jamming.
4. Electronic Reconnaissance (ER) is the gathering and collecting of Electromagnetic emissions that are radiated by potentially hostile sources for intelligence purposes. ER is an area that is related to ES and overlaps with it in many of its functions however, ER is mainly strategic while ES is tactical. For example, E-3 AWACS collects electromagnetic signals for the purpose of analysis and assessment of the Electronic Order of Battle (EOB). ER can be divided into three subcategories [2]:
    a. Communications Intelligence (COMINT) is the non-immediate collection of communication channels.
    b. Electronic Intelligence (ELINT) is the non-immediate collection of Radar.
    c. Radiation Intelligence (RINT) is a new technique to capture electromagnetic energy from non-information or sensory emitters within target platforms, such as engines, power systems etc.

II. THE NEED FOR A NATIONAL CAPABILITY

Electronic Warfare and signal intelligence is different from many other military systems and tools in that they have to be built and operated locally. EW and intelligence information is highly sensitive and holds the highest security classification in many countries. Although EW and signal intelligence systems are offered in the international market, most of these systems are configured for a basic capability and the end user then relies on local industry to supply and support the EW and intelligence tools. The reason that the industry limits or withholds EW and intelligence capability is that most of the Intellectual Properties (IP), documents and databases related to intelligence are state-owned and require government-to-government agreement before they can be used. The national vision 2030 [3] states that military spending on local industry should reach 50% instead of the current 3% share. The EW and intelligence sector relies heavily on the threat database, programming and data analysis tools.

III. KACST HISTORY IN EW AND SIGNAL INTELLEGENCE

KACST has been developing electronic warfare and signals intelligence systems since 2004. The initial objective, during the first three years, was the transfer of technology and the expertise but with little attention being paid to system performance and operational maturity. This enables KACST to absorb and adopt the partner company's engineering processes and workflow. Figure 1 shows the history of EW and signal intelligence capability since 2004.

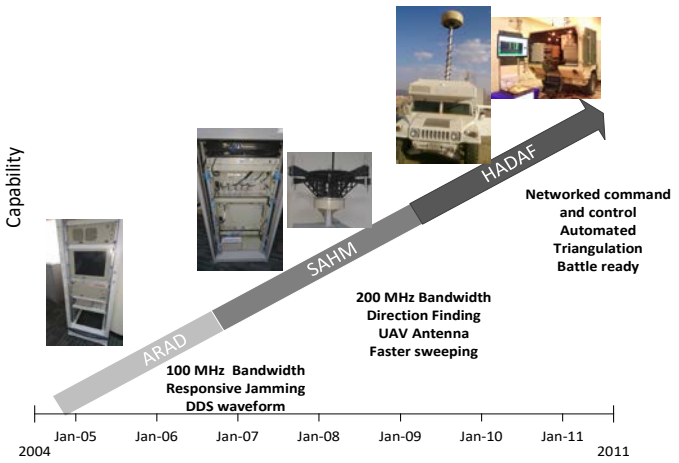

Fig. 1. : History of the joint development between KACST and GEW in communications intelligence and electronic warfare.

A. ARAD Project: Tracking and Waveform Synthesis

The ARAD project started in 2004, in partnership with GEW Technologies, to transfer the technology of wideband receivers and tracking jammers to the Kingdom of Saudi Arabia. The ARAD system is a Wide Band Receiver and Target Tracker (WBRTT). WBRTT is suitable for tactical signal monitoring, reconnaissance and jamming. KACST was responsible for two features in the system: frequency hopping tracker algorithms and signal synthesis.

Frequency Hopping

Frequency hopping (FH) signals are widely used in military systems. FH is immune to conventional detection, interception, location, and jamming techniques.

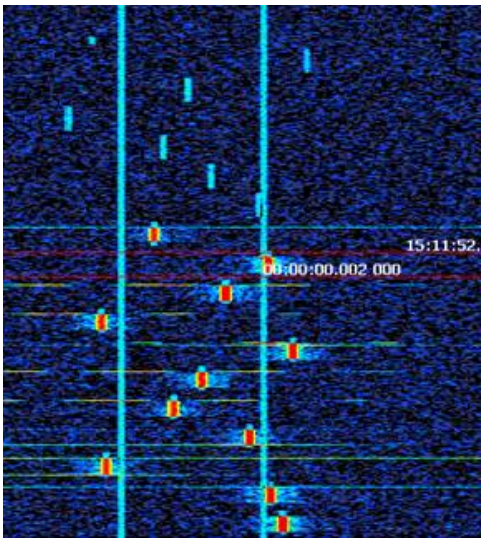

Fig. 2. : Histogram graph showing frequency hopping signal shown in cyan, and the jamming signal in red. The horizontal axis is frequency domain and the y-axis is time.

The waveform instantly changes its carrier frequency and "hops" to a random frequency within the operating bandwidth [4]. This bandwidth is normally limited by the waveform generator and the receiver. The hop rate is the number of hops per second. A waveform is considered to be a fast hopper if it exceeds its symbol rate.

Tracking Hopper Signal

Advances in Digital Signal Processing (DSP) have led to improvements in COMINT receivers. These same advances enable the synthesis of ever more complex waveforms which, in turn, drives challenges to the detection and processing of communication signals. Hopping signals are commonly tracked by predicting the frequency sequence [4], then tuning the narrowband receiver to the predicted frequency in order to confirm the prediction. The hopping frequency is not completely random but, rather, quasi-random because it is generated using a digital processor. Hence, it is possible to observe convergence or predict sequence size. However, there are two challenges that faced the development of the ARAD receiver. Firstly, many military communication systems use advanced, quasi-random generation algorithms with extremely large sequences, sharing complex seed states. Secondly, when jamming the signal, the ARAD system should intercept the target signal and propagate the jamming waveform in real time.

There are two common approaches to track frequency hoppers. Some COMINT systems predict the frequency sequence using adaptive processing like Kalman filter [5], then transmit the jamming waveform with sufficient time to suppress the current hop burst. Another approach is to monitor the spectrum for a predetermined time period during jamming sessions. The most common tracking approach, which is the one used in ARAD, is combining both methods to improve the probability of interception and jamming effectiveness. Such COMINT systems can calculate a reliable prediction model for slow and predictable hoppers. Reducing the 'look-through' periods reduces the jamming effectiveness.

The ARAD system was tested against the frequency hopping communication systems used by a government organization and it successfully intercepted and jammed the hopper signal. However, when it was tested against the slower-frequency hopper communication system with a variable duration, the system failed to track the hopper. In such a case, the system resorts to a fixed look-through duration. Look-through is the state where the system stops transmission and monitors the spectrum to detect any changes in emitters' activity. This setting reduces jamming effectiveness by missing hopper session transitions.

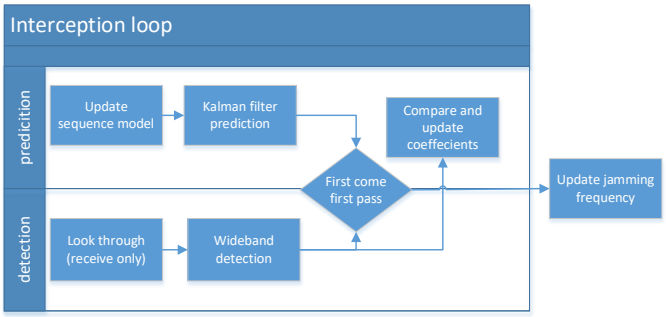

Fig. 3. : Combined prediction and detection process to track frequency hoppers.

The response time varies between prediction and detection. Prediction only requires a one-way propagation time between the COMINT station and target receiver and a prediction processing time. Detection requires a one-way propagation time between the target source and COMINT station, a one-way propagation time between the COMINT station and target receiver and a responsive processing time. When relying on detection, the look-through period is calculated based on the observed hopper session.

Jamming Waveform Synthesis

The ARAD system utilized a new technology, relative to the time of development, called Direct Digital Synthesis (DDS). In its primitive form, DDS is a fast, high-resolution Digital to Analog (DAC) system optimized for waveform generation [6]. The ARAD system uses DDS to generate baseband waveforms within half a Gigahertz, then dynamically up-converts the waveform to cover the system's operational bandwidth.

B. SAHM project: Direction Finding

Direction finding (DF) systems are generally considered an intelligence-gathering measure for locating radio or radar. However, reliable and real-time DF capabilities are critical to systems including self-protection suites, homing weapons, and real-time situational awareness tools.

The SAHM project integrated correlative interferometry [7] using five channels. Each channel has a dedicated antenna and a digital receiver. Two SAHM DF receivers at different locations can automatically calculate the approximate position of the emitter, provided that the emitter is not along the same line joining the two DF stations. The geolocation processor can obtain the emitter location in real-time even with only a short-time emission or signal. When using only one DF mobile receiver, the emitter location can be calculated automatically, with sufficient accuracy, using the intersection of the lines of their bearings. However, single receiver geolocation only applies to stationary emitters.

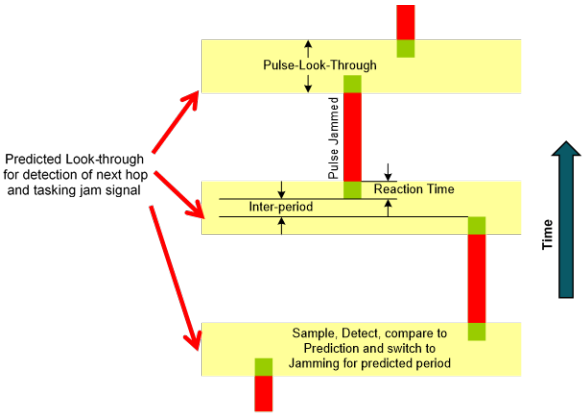

Fig. 4. : Combined prediction and detection process to track frequency hoppers.

C. HADAF project: Integration

The purpose of the HADAF System is to provide a comprehensive facility to validate and demonstrate the technologies improved on in the ARAD and SAHM projects. The HADAF system can effectively counter emissions in the VHF frequency range by the monitoring and direction finding of communications in the HF, VHF, and UHF frequency ranges. The system consists of three subsystems as follows:

1. Command and Control Center, Communications Electronic Support (CCC CES). This vehicle comprises a DF receiver and the workstation of the mission supervisor.

2. Communications Electronic Support (CES). This vehicle only contains a DF receiver.

3. Communications Electronic Attack (CEA). This is a semi-mobile truck, meaning it does not operate whilst in motion. The CEA station contains the WBRTT and the jamming equipment but it has no DF capability.

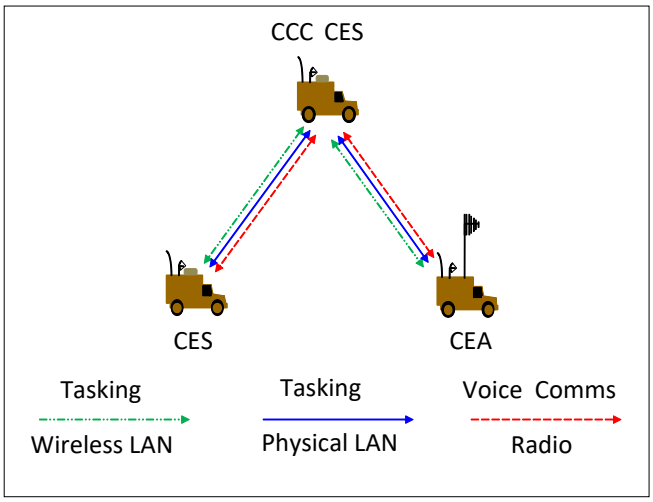

Fig. 5. : Configuration of HADAF system. CCC CES is the command and control center. CES is a communications electronic support unit (both units intercept and locate enemy communications). CEA is the communications attack unit, which receives jamming tasks from tasks from the CCC.

HADAF Deployment Process

The mission objectives are defined at the mission planning meeting and given to the Supervisor to execute using the HADAF System. The Supervisor then interprets the mission objectives and plans the mission in the Command and Control Center (CCC CES). Using the system tools available, the Supervisor selects the best locations for the vehicles under his command and defines a list of tasks for each sub-system. These tasks are then distributed to the various sub-systems and the mission is ready to be executed.

The vehicles then deploy to their planned locations and set up their equipment for the mission. Communication links are established with the CCC CES and, once complete, the mission commences. During the mission execution, each operator will carry out the tasks defined in their task lists whilst the Supervisor monitors overall progress. The Supervisor will coordinate the DF sub-systems from a DF Commander perspective, as well as the ECM sub-system (from an ECM Commander perspective). The Supervisor may initiate further tasks should the need arise during execution of the mission.

Upon completion of the mission, the vehicles will pack up and return to home base, normally KACST solar village. The Supervisor will then consolidate the results of the mission and compile a mission report. A mission-debrief session will then be held with the various HADAF System crews. The mission report will be returned for analysis at KACST as well as any other data that is required.

IV. DF, COMINT AND EA BENCHMARKING

The electronic attack (EA) capability is compared with similar systems currently available in the international market in Figure 6. Note that the EA is heavier, larger and requires more power and, therefore, this drives the choice of platform.

DF and COMINT are normally integrated into EA systems due to the jamming systems' reliance on careful threat identification and the need to plan to ensure effective suppression. Even if a suitable countermeasures waveform and timing plan is created, DF and COMINT are still required to track emitter movements and mode of operation before jamming or deception operations can be carried out. The following diagram compares HADAF with similar DF\COMINT systems available in the international market.

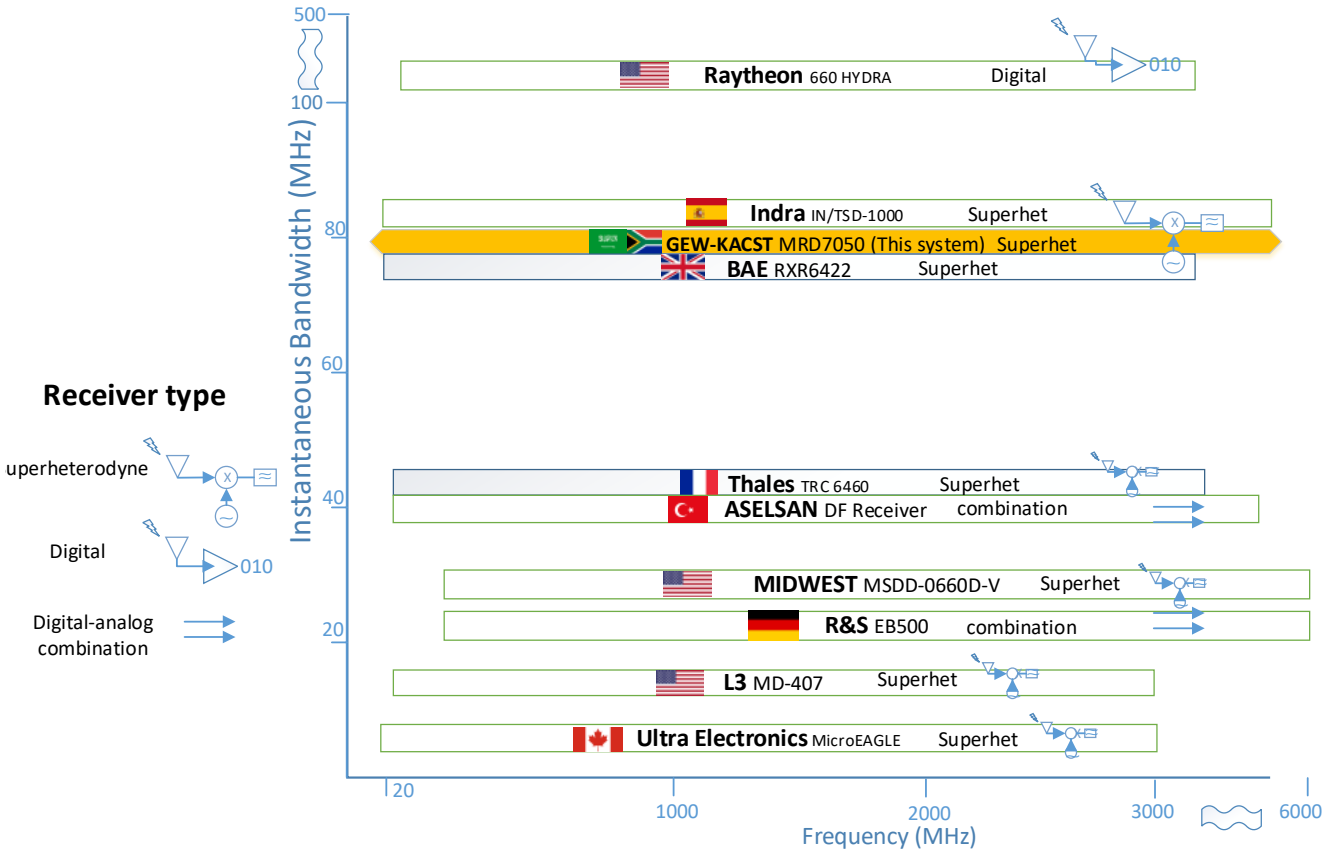

Fig. 6. : Comparison between DF\COMINT products available in the international defense market in terms of operating frequency, instantaneous bandwidth, and receiver type.

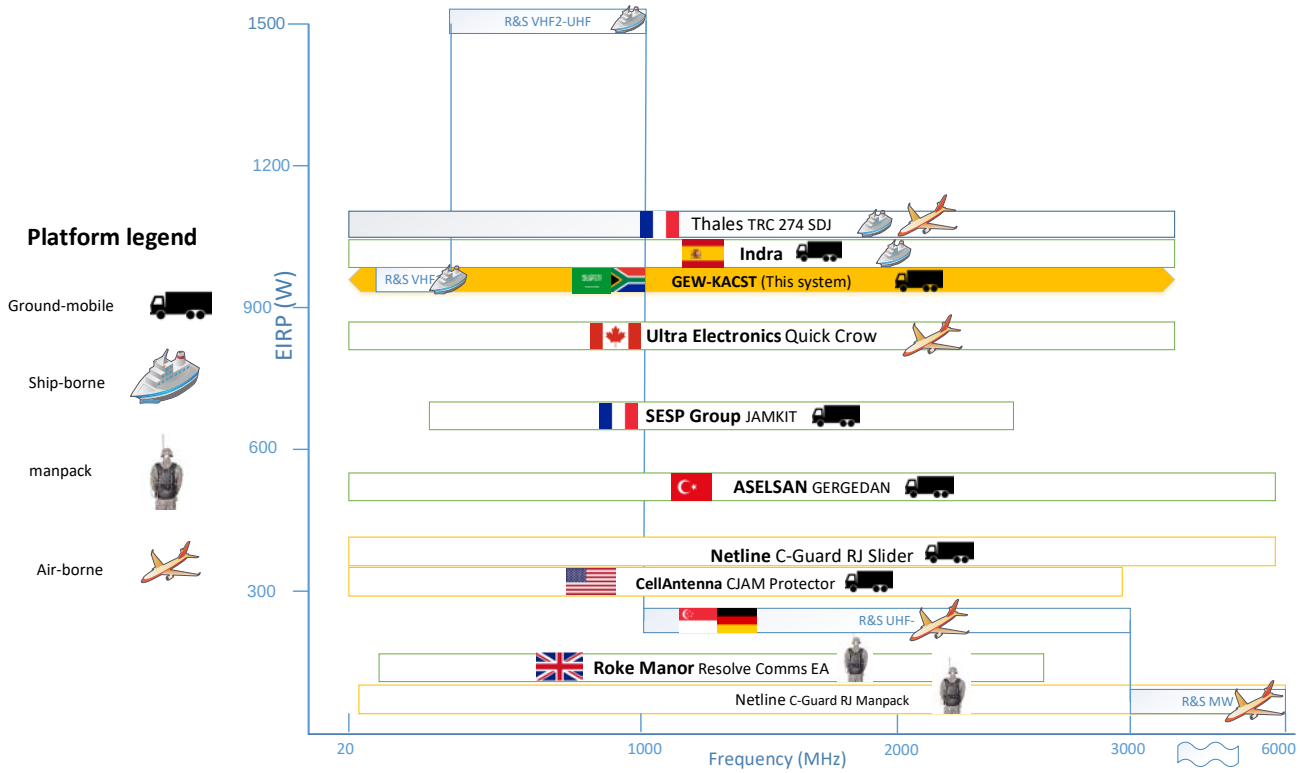

Fig. 7. Comparison between electronic attack products available in the international defense market [8].

REFERENCES

[1] P. H. J. Davies, "Intelligence, information technology, and information warfare," *Annual Review of Information Science and Technology*, vol. 36, no. 1, pp. 312-352, 2002.

[2] Martti Lehto, Cyber Security: Analytics, Technology and Automation. Intelligent Systems, Control and Automation: Science and Engineering, vol. 78, Springer, Cham, 2015.

[3] C. o. M. o. t. K. o. S. Arabia, 25 4 2016. [Online]. Available: www.vision2030.gov.sa.

[4] N. H. Motlagh, Advanced Trends in Wireless Communications, InTech, 2011.

[5] P. S. R. Diniz, Adaptive Filtering: Algorithms and Practical Implementation, Rio de Janeiro: Springer, 2013.

[6] E. M. a. C. Slattery, "All About Direct Digital Synthesis," *Analog Dialogue*, vol. 38, p. August, 2004.

[7] H.-W. &. S. Y.-G. Wei, "Performance analysis and comparison of correlative interferometers for direction finding," 2010.

[8] O. Holt, "Technology Survey: Communications and IED Jammers," *The Journal of Electronic Defense*, pp. 32-41, June 2016.

[9] O. Holt, "Technology Survey: COMINT/DF Receivers," *The Journal of Electronic Defense*, pp. 43-58, September 2015.