A Novel Trap Jamming Technique to Defeat Cognitive Radar

Heath Couture
Mechanical Engineering
University of Waterloo
Waterloo, Canada
e-mail: hcouture@uwaterloo.ca

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

***Abstract*—Although the cognitive era is still in its infancy, there has been a growing research interest in the development of cognitive capabilities in various electronic systems, such as, cognitive radio and cognitive radar. Historically, there has been a back-and-forth competition between radar and electronic warfare. Thus, with the advances in radar technology, especially the new cognitive radar systems, electronic countermeasures need to be developed to catch up in the race. To defend against cognitive radar systems, a trap jamming technique is proposed to periodically disrupt cognitive radar's measurement capabilities. The algorithm has been developed in a MATLAB environment. The experimental results have shown that the cognitive radar will be rendered ineffective.**

Keywords-jamming; cognitive radar; MATLAB environment.

I. INTRODUCTION

In recent years, there has been a growing research interest in the development of cognitive capabilities in various electronic systems, specifically in the fields of cognitive radio and cognitive radar [1]. The idea of cognitive radio was proposed by Joseph Mitola III in a seminar held at the Stockhom-based KTH Royal Institute of Technology in 1998 [2]. The objective is to enhance the spectrum utilization efficiency by intelligently detecting spectrum holes and rapidly jumping to broadcast on them [3][4]. The concept of cognitive radar was proposed by Haykin in 2006, which presented a dynamic system to adapt and optimize transmitted waveforms based on the operational environment [5]. It was indicated that "Cognitive radar is the radar counterpart to cognitive radio" [6]. With the advances of radar technology, electronic warfare (EW) technology has also improved to disrupt the functionality of radar systems. Radar and EW are always in competition with each other. Therefore, it is necessary to develop a countermeasure technique to defend against cognitive radar systems.

Electronic Attack (EA) or jamming is a key component of EW, and an effective Radio Frequency (RF) technology used to defeat radar systems. Although there are various jamming techniques, they have a common objective — to prevent the proper operation of adversary radars. Since cognitive radars have strong anti-jamming and target detection capabilities, the conventional jamming techniques are unable to interfere effectively with the operation of cognitive radar systems. Based on the principles that "cognitive radar uses the under-utilized spectrum using dynamic spectrum allocation techniques" [7], and "the radar environment is modelled as a Markov decision process to predict the frequency band with the lowest jamming energy [8]", a trap jamming technique is proposed, which will periodically disrupt cognitive radar's measurement capabilities. The algorithms are developed using MATLAB (Version 2023b). The experimental results showed that the proposed technique could disrupt cognitive radar and render it ineffective. The rest of this paper is organized as follows. Section II discusses the different EA techniques. Section III presents a trap jamming approach against cognitive radar. Section IV addresses the development of MATLAB application, while the simulation results are presented in Section V. Finally, Section VI concludes the paper.

II. ELECTRONIC ATTACK TECHNIQUES

Radar is a system that uses electromagnetic waves to identify the range, altitude, direction or speed of objects. It is one of the most powerful and commonly used sensors in the battlefield to detect and track targets such as, aircraft, ships, and vehicles. In contrast, EA, colloquially referred to as jamming, is the electronic countermeasure used to create interference signals to saturate or deceive adversary radars. Different jamming techniques can be employed against radars with a common objective of preventing the proper operation of the radar systems. For example, when detected by a radar, a targeted platform will conduct EA activities to deny range and position information to make the radar lose the tracking information.

A. Passive EA

Passive EA takes place by means of reflection or re-reflecting RF wave energy back to the source to produce false target returns to the radar. Devices used in passive EA include chaff, decoys and other reflectors that require no prime power [9][10].

1) Chaff

Chaff is made of aluminum strip or aluminum-coated nylon or fiber glass, which is developed to create a cloud of false returns on adversary radar systems. It consists of a large number of dipole reflectors that are designed to match the half wavelength of the frequency used by the victim's radar. Chaff with different lengths can be packed in the same package to be effective against radars of widely different frequencies.

2) Passive decoy

Radar corner reflectors are an effective passive decoy against radar detection, which are used to re-radiate relatively

 ISBN: 978-1-68558-375-0

high radar energy mostly back toward the source. Floating corner reflector and corner-reflector decoy were introduced in [11]. With rapid deployment and inflation time, full radar cross-section can be achieved within seconds of reflector launch.

B. Active EA

Electronic jamming is a conventional method of EW, which transmits interfering signals, such as, noise signals or false information, to saturate or deceive the receiver of any electronic device within the range of interference. There are two main techniques of electric jamming: noise techniques and deception techniques [12], while noise jamming can be further categorized as barrage jamming, spot jamming, and sweep jamming.

1) Noise jamming

The objective of noise jamming is to mask the actual signal by introducing an interference signal into the adversary's electronic system. Gaussian noise is the most common noise-jamming waveform. In general, there are three types of techniques for generating the noise signal: wideband jamming, narrow-band jamming, and shifted narrow-band jamming.

a) Barrage jamming

Barrage jamming refers to the use of a single jammer to cover several frequencies with a wide noise bandwidth. In this type of jamming, the power output of the jammer is spread over a bandwidth that is wider than that of several radar signals (Figure 1 (a)). The advantage is that multiple radars can be jammed continuously and simultaneously. The disadvantage lies in that the jammer needs to spread its power over a very wide band, which reduces the jamming power in any one particular band. The wider the frequency band covered, the less effectively each band is jammed.

b) Spot jamming

Spot jamming is simply narrowing the bandwidth of the noise jammer, ideally identical to that of threat emitter frequency, to concentrate the maximum amount of jamming power (Figure 1 (b)). The advantage of spot jamming lies in the jamming efficiency by focusing jammer power on a particular frequency. The disadvantage is its inability to be effective against modern frequency agile radar because the jammer can only jam one frequency. Spot jamming is usually directed against a specific radar. Multiple jammers are required to overcome uncertain frequency parameters.

c) Sweep jamming

To jam a broad band with less output power, sweep jamming repeatedly shifts its full power from one frequency to another (Figure 1 (c)). A group of jamming platforms operating in cooperation may present this scenario [13]. The advantage is that it is able to jam multiple frequencies while maintaining adequate power in quick succession. The disadvantage of sweep jamming is that the jammer cannot affect all the frequencies at the same time.

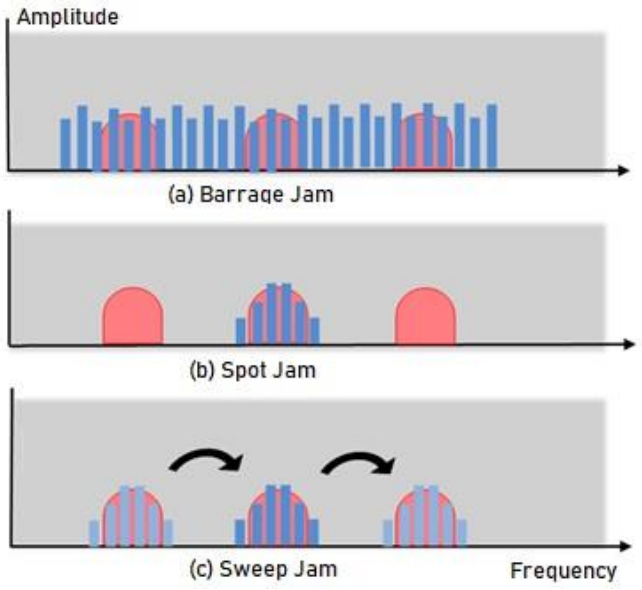


Figure 1. Visual representations of jamming techniques.

2) Deception jamming

Deception jamming consists of manipulating the return signal that the radar receives to generate incorrect data. This can either be through creating false targets or creating misleading range gate information by exploiting Doppler returns. Deception jamming is generally more effective than the noise jamming techniques against modern radars equipped with Electronic Counter-Countermeasures (ECCMs) such as, constant false alarm rate or home-on-jam.

III. TRAP JAMMING TECHNIQUE

As mentioned above, cognitive radar stems from cognitive radio that tries to predict the frequency band with the lowest jamming energy. Therefore, a trap jamming technique is proposed that sets up spectrum holes, lures the cognitive radar jump into one of the spectrum holes, and then generates a jamming signal to cover the spectrum holes. In such a way, the radar cannot lock onto the intended target. The algorithm is explained in detail as follows.

When a radar signal at frequency f_0 is detected using Electronic Support (ES) measures, a low-power noise jamming signal is emitted centred around f_0. Depending on the capacity for the total power output of the EA system, the jam will attempt to create noise coverage of the entire frequency band on which the radar or RF seeker is operating. It can be noted that on larger NATO-designated frequency bands such as, the *J* band (10 to 20 GHz), an RF seeker will only operate on a specific range of the band and not the entire 10 GHz bandwidth. If full band coverage is not possible due to a constraint on the power output of the jammer, noise will be created across a bandwidth from f_1 to f_2 centered around f_0. In this case, the bandwidth will be determined by the emitted power for each Δf that will be high enough to impact the performance of the radar. It is possible that multiple jammers could be used synchronously to cover sufficient bandwidth and meet the power threshold.

 ISBN: 978-1-68558-375-0

As shown in Figure 2, the initial jamming signal transmitted at time t will be similar to a barrage noise jam, with the only difference being that there are two or three spectrum holes of bandwidth b that are not jammed. Using Electronic Intelligence (ELINT) gathered from ES, b should correspond or be close in value to the bandwidth that the radar signal is transmitting. In this case, the Δf of the jamming signal is 10 MHz.

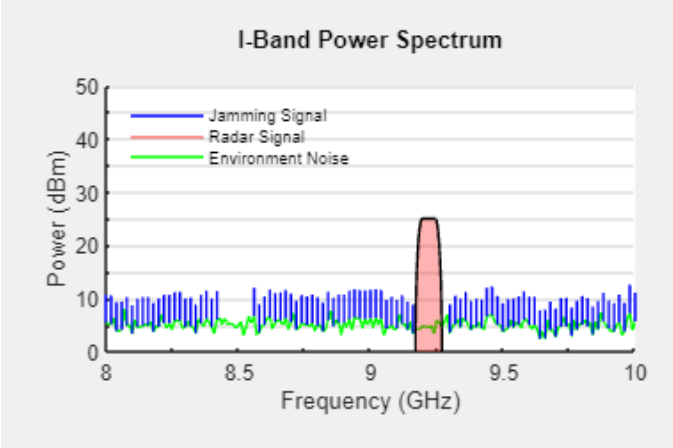


Figure 2. Frequency-power plot at time t, with trap jam signal.

At time t plus an interval of Δt, Figure 3 depicts that the jamming signal will switch to spot jamming with power, P_J, and bandwidth, b, on the "trapped" sections of the frequency domain that were initially left without transmitted noise signals. The Δt intervals will be designated so that the cognitive radar will have ample time to find the trapped locations and start transmitting from them, as shown in Figure 2. The cognitive radar will do this because it will have an optimized Signal-to-Noise ratio (S/N) at the point where there is no interfering noise from the jammer.

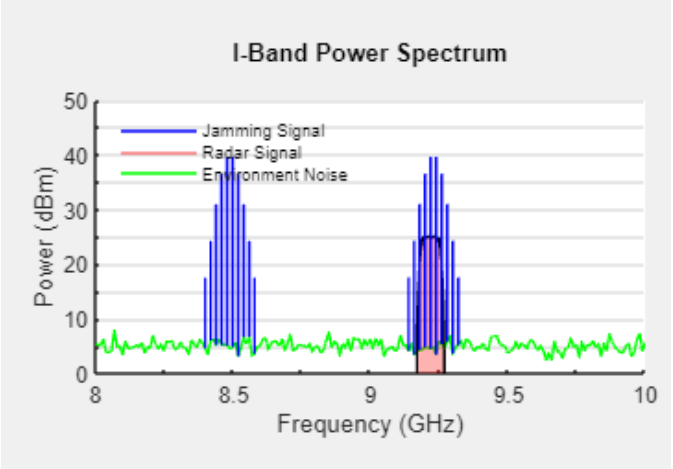


Figure 3. Frequency-power plot at time $t + \Delta t$ with the spot jam signal.

The objective of this Electronic Countermeasure (ECM) is achieved by minimizing the amount of time that the adversary radar is illuminating and locked onto the target. The repetitive nature of this technique will continuously reset adversary radar into its search mode. This also enables the effective use of supplementary ECM. For example, when an RF seeker is in the search mode, launching chaff or deploying a decoy would have a heightened chance of successfully causing the seeker to lock onto those false targets, as opposed to deploying those measures when the seeker is already locked on.

Advantages of this method include no longer needing sophisticated ES measures to gain the exact parameters of the cognitive radar, which could then quickly change regardless. It would be an inefficient use of resources, computational power and time, if every instance the Radar Warning Receiver (RWR) keeps on the illuminated target, and the ESM is employed to identify the radar parameters to generate a spot jam. Therefore, the proposed technique is ideal because ES is only needed for the initial f_0 reading and bandwidth values. After that, the cycles will continue without the delay of an ELINT system to collect and disseminate the parameter values.

IV. MATLAB SIMULATION

The MATLAB simulation of the trap jamming technique was designed with flexibility as the foremost priority, as this is not a comprehensive system design but rather a proof of concept. The development of ECM strategies has additional challenges when only the peacetime operational parameters of radar systems are known in databases with predefined threats. War Reserve Mode (WARM) refers to the use of non-traditional behaviors or modes that are not observed outside of conflicts [14]. This simulation can be used as a guiding tool if those specifications become available.

As previously explored, the cognitive radar allows for the waveform parameters to be flexible, and the simulation incorporates this by making these variables. This MATLAB simulation takes user inputs from the different radar and jammer parameters console, storing them as variables. It then evaluates the signals from both the friendly and adversary sides by using the radar and jammer equations in decibel (dB) form. A Graphical User Interface (GUI) is developed in MATLAB where the user can easily set parameters of the ship, jammer, missile, and radar (Figure 4).

The two-way link radar equation (1) has been standardized in technical literature, and the simulation uses the decibel version (2), which converts the linear parameters to decibel values and includes numerical conversion constants [15]. Using this logarithmic scale allows for comparing high transmitted power values with very low return signal power. This is a standard convention and is used for simplicity and ease of evaluating the simulation results. Signal return power, S, can be written as a function of the range between radar and target. Target detection is also dependent on the S/N ratio, usually in decibels.

 ISBN: 978-1-68558-375-0

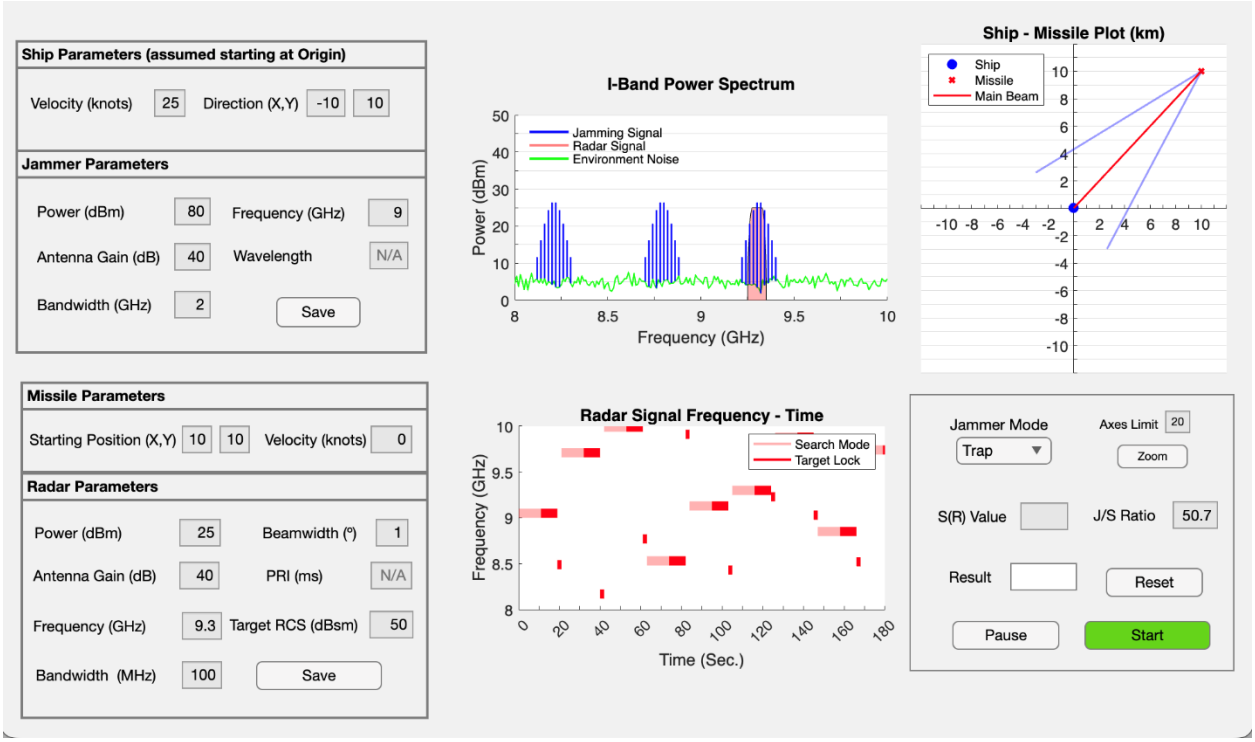


Figure 4. MATLAB GUI.

$$P_r = \frac{P_t G_t G_r \lambda^2 \sigma}{(4\pi)^3 R^4} \quad (1)$$

$$S = P_T + G_T + G_R - 20\log(f) - 40log(R) - 103.4 + \sigma \quad (2)$$

P_r is the return power received by the radar in decibel milliwatts (dBm), P_t is the transmitted power in dBm, G_t is the antenna gain for the transmitter in dB, G_r is the antenna gain for the receiver in dB, λ is the wavelength in meters, σ is the RCS signature of the target in decibel square meters (dBsm), R is the range between the target and radar in km, and f is frequency in MHz.

It is to be expected, and is observed in the simulation with demonstration parameters, that the return power will be a negative number in decibels because this signal power is less than the transmitted power. For simplicity and technical accuracy, it is fair to assume that the same antenna is used for both the transmission and receiving. This is known as a monostatic radar, which uses a transceiver. A missile head will not have the space for multiple antennas. This aspect of the two-way link equation is used more for communications where the transmitter and receiver are not collocated. This restricts the simulation scenarios to the use of Active-Radar Homing (ARH) instead of Semi-Active Radar Homing (SARH), where the missile would only contain a receiver and the transmitted signal would come from an offboard source.

The jamming equation (3) is similar to the radar equation (1), except it is a one-way link. This is because the signal travels directly from the EW device to the receiver of the radar with no return. The jamming signal is a one-way transmission, so it has the advantage of R^{-2} propagation, instead of R^{-4} in (1) [16]. The Jam-to-Signal ratio (J/S) is derived from the decibel form of the radar equation in (2) divided by the decibel version of the one-way link in (4).

$$P_r = \frac{P_j G_j G_r \lambda^2}{4\pi R^2} \quad (3)$$

$$J = P_J + G_J + G_{RJ} - 20\log(f) - 20log(R) - 32.4 \quad (4)$$

$$J/S = P_J + G_J + G_{RJ} - P_T - G_T - G_R + 20log(R) + 71 - \sigma \quad (5)$$

Equation (5) is used as a ratio, and when J/S is less than zero, the radar is effective, but if J/S is greater than zero, the jammer has an advantage and the radar will not operate as effectively [15][17]. It is unknown what the exact threshold of jamming noise is in relation to the signal power that is required to force a cognitive radar to initiate a frequency hop or other parameters modifications. This depends on the specific radar, but for this purpose of proof of concept, the threshold is met when J/S switches signs from positive to negative.

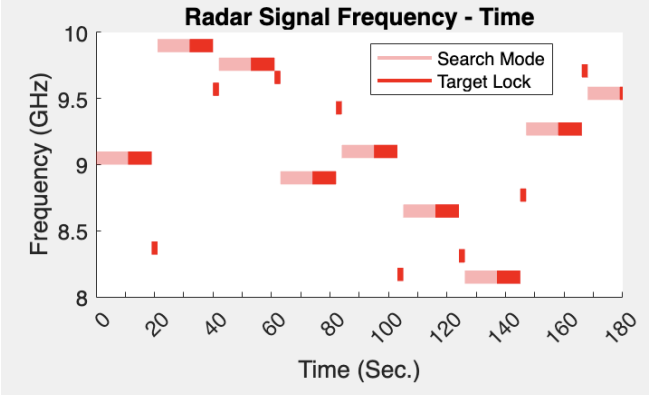
V. SIMULATION EXPERIMENTS

The primary method for evaluation is the radar (2) and jamming (5) equations with test parameters from the simulation. This is then displayed in the numeric edit fields labelled on the GUI. This will give the user confirmation of the mathematically predicted success of the ECM on the cognitive radar. Figure 3 shows that the return pulse is completely hidden. Results with the demonstration parameters

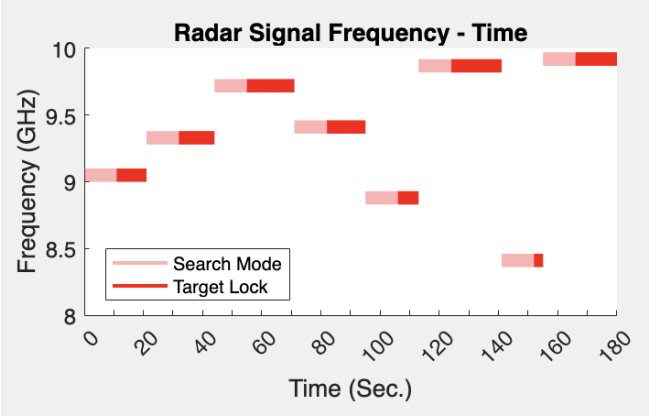
 ISBN: 978-1-68558-375-0

have a J/S ratio of 51.3 when the spot jamming occurs, which confirms this principle.

As aforementioned, the other live-updating figure is displayed in Figure 5. It is a plot of the radar signal frequency as it changes over time, measured in Pulse Repetition Interval (PRI) repetitions. This visualizes how often the cognitive radar is being allured to change its carrier frequency. For target tracking purposes, the jamming method can be considered successful by limiting the amount of time that the radar is locked on or illuminating the intended target.



(a) The radar carrier frequency when the trap jamming method is used



(b) Same plot with the sweep jamming method simulated

Figure 5. Frequency-time plot representing jamming scenario.

There is a drop-down menu that allows the user to select other jamming methods. While no formal comparison exists, although it could and this is a recommendation for improvement, a visual comparison between the time locked on the target for the radar is given if the user runs the simulation multiple times using the trap method, sweep jam, or barrage jam options. Using the Frequency-Time graph shown in Figure 5 (a) to substantiate this, the adversary radar is allured to change transmitting frequency more often when the trap method is used as opposed to sweep jamming, shown in Figure 5 (b), and barrage jamming.

VI. Conclusions and Future Work

A MATLAB interactive simulation of the trap-jamming concept was successfully created to work in all spatial situations and proves the viability of this technique. The desired jamming sequence was achieved through the live updating GUI to replicate the novel trap electronic countermeasure concept (Figure 4). Radar and jamming equation results mathematically prove that the cognitive radar will be rendered ineffective due to the noise transmitted on the radar's operating frequency after it is changed to transmit on the desired, initially unjammed spectrum holes within the operating band. The spot jam will break the lock the radar has which is illuminating the target and reset it back into search mode. While a cognitive radar will learn using reinforcement learning, this concept shows that this cycle will at least be successful once, which is all it might need to be in a real-world EW scenario.

Possible future works include simulation supplemented with improvements such as, implementing Artificial Intelligence (AI) on the radar to have it learn ECCMs, and the addition of other supporting ECM such as, chaff or decoys. The user experience can be enhanced by adding a way to speed up time, from seeing each pulse in microseconds to real-time to see the missile and target moving. These are top areas of future research.

References

[1] W. Hilal, S. A. Gadsden, and J. Yawney, "Cognitive Dynamic Systems: A Review of Theory, Applications, and Recent Advances," in Proceedings of the IEEE, vol. 111, no. 6, pp. 575-622, 2023.

[2] A. Sarode and P. Ojha, "Cognitive Radio," International Research Journal of Innovations in Engineering and Technology (IRJIET), vol. 5, no. 8, pp 71-74, 2021.

[3] S. Pavithra, S. Karthikeyan, V. J. K. Sonti, and S. Jayashri, "Competent Realisation of Cooperative Spectrum Sensing in Cognitive Radio Systems," International Journal of Engineering Systems Modelling and Simulation, vol. 7, no. 2, pp. 103-110, 2015.

[4] K. B. Letaief and W. Zhang, "Cooperative Communications for Cognitive Radio Networks," in Proceedings of the IEEE, vol. 97, no. 5, pp. 878-893, 2009.

[5] S. Haykin. "Cognitive Radar: A Way of The Future," IEEE Signal Processing Magazine, vol. 23, pp. 30-40, 2006.

[6] C. Baylis, J. Martin, M. Moldovan, O. Akinbule, and R. J. Marks, "A Test Platform for Real-Time Waveform and Impedance Optimization in Microwave Radar Systems," 2012 International Waveform Diversity & Design Conference (WDD), Kauai, HI, USA, 2012, pp. 019-022, doi: 10.1109/WDD.2012.7311307.

[7] D. Brahma, S. Swayamsiddha, and G. Panda, "Dynamic Spectrum Allocation in Cognitive Radar: A Brief Overview," 2023 3rd International Conference on Range Technology (ICORT), Chandipur, Balasore, India, pp. 1-4, 2023.

[8] Z. Zheng, W. Li, and K. Zou, "Airborne Radar Anti-Jamming Waveform Design Based on Deep Reinforcement Learning," Sensors 2022, 22 (22): 8689.

[9] A. De Martino, Introduction to Modern EW Systems, Norwood: Artech House, 2012.

 ISBN: 978-1-68558-375-0

[10] M. I. Skolnik, Radar Handbook, 3rd Edition, New York: McGraw-Hill, 2008.

[11] N. Friedman, "Soft Kill Versus Anti-Ship Missiles," Naval Forces, vol. 30, no. 1, pp. 85-89, 2009.

[12] Electronic Warfare And Radar Systems Engineering Handbook, *NAVAIR Electronic Warfare/Combat Systems*, June 2012, [Online]. Available from: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA566236.

[13] F. Schmied and J. Schobel, "Algorithmic Optimization of Sweep-based Signals for Jamming RF Modules and UAVs," STO-MP-IST-205-37, pp. 1-8, 19, 2024.

[14] P. M. Gale, "Counter ESM/ELINT - A Review," Maple Leaf Chapter Newsletter - Association of Old Crows, vol. 1, no. 7, pp. 3–6, 2023.

[15] D. Adamy, "EW Against Modern Radars - Part 1 Radar Jamming Equations," Journal of Electronic Defense, pp. 56–57, 2009.

[16] M. Davis, "Key Differences between Radar and Communications Systems," in Proceedings of the 12th Annual International Symposium on Advanced Radio Technologies, pp.1-11, 2011.

[17] D. Adamy, EW 101: A First Course in Electronic Warfare. Boston: Artech House, 2001.

 ISBN: 978-1-68558-375-0