Defense Systems Information Analysis Center

DSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

An Overview of Decoys Used in the U.S. Military

Report Number:

DSIAC-BCO-2024-592

Completed September 2024

DSIAC is a U.S. Department of Defense Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443-360-4600

REPORT PREPARED BY:
Taylor H. Knight
Office: DSIAC

DSIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. DSIAC is operated by the SURVICE Engineering Company.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
18-09-2024	Technical Research Report	

4. TITLE AND SUBTITLE

An Overview of Decoys Used in the U.S. Military

5a. CONTRACT NUMBER
FA8075-21-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Taylor H. Knight

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Defense Systems Information Analysis Center (DSIAC)
SURVICE Engineering Company
4695 Millennium Drive
Belcamp, MD 21017-1505

8. PERFORMING ORGANIZATION REPORT NUMBER

DSIAC-BCO-2024-592

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center (DTIC)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION A. Approved for public release: distribution is unlimited.

13. SUPPLEMENTARY NOTES
Energetics, Survivability and Vulnerability

14. ABSTRACT
The Defense Systems Information Analysis Center was asked to identify what decoys are being developed and fielded across the U.S. Department of Defense (DoD). Decoys have evolved over the past several decades, from inflatables to electromagnetic (EM) spectrum decoys, with options in between. Decoys improve the Warfighter's capability to conduct electronic warfare, produce alternate targets for the protection of military assets, and help increase survivability by deflecting enemy threats. Decoys are designed to deceive adversaries through a variety of methods, such as manipulative, simulative, and imitative. Recent developments in decoys have allowed them to mimic EM spectrum signatures, counter radar-guided threats (including anti-ship missiles), and protect combat platforms. This report identifies decoys currently in use, or in development, by DoD organizations and branches of the military and summarizes their capabilities.

15. SUBJECT TERMS
decoys, electromagnetic spectrum operations

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Ted Welsh, DSIAC Director
U	U	U	UU	13	**19b. TELEPHONE NUMBER** *(include area code)* 443-360-4600

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

DISTRIBUTION A. Approved for public release: distribution is unlimited.

About

DTIC and DSIAC

The Defense Technical Information Center (DTIC) preserves, curates, and shares knowledge from the U.S. Department of Defense's (DoD's) annual multibillion-dollar investment in science and technology, multiplying the value and accelerating capability to the Warfighter. DTIC amplifies this investment by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision-makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Centers (DoDIAC), which provide critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Defense Systems Information Analysis Center (DSIAC) is a DoDIAC sponsored by DTIC to provide expertise in 10 technical focus areas: weapons systems; survivability and vulnerability; reliability, maintainability, quality, supportability, and interoperability (RMQSI); advanced materials; military sensing; autonomous systems; energetics; directed energy; non-lethal weapons; and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). DSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

TI Research

A chief service of the U.S. Department of Defense's Information Analysis Centers is free technical inquiry (TI) research limited to four research hours per inquiry. This TI response report summarizes the research findings of one such inquiry. Given the limited duration of the research effort, this report is not intended to be a deep, comprehensive analysis but rather a curated compilation of relevant information to give the reader/inquirer a "head start" or direction for continued research.

Abstract

The Defense Systems Information Analysis Center was asked to identify what decoys are being developed and fielded across the U.S. Department of Defense (DoD). Decoys have evolved over the past several decades, from inflatables to electromagnetic (EM) spectrum decoys, with options in between. Decoys improve the Warfighter's capability to conduct electronic warfare, produce alternate targets for the protection of military assets, and help increase survivability by deflecting enemy threats. Decoys are designed to deceive adversaries through a variety of methods, such as manipulative, simulative, and imitative. Recent developments in decoys have allowed them to mimic EM spectrum signatures, counter radar-guided threats (including anti-ship missiles), and protect combat platforms. This report identifies decoys currently in use, or in development, by DoD organizations and branches of the military and summarizes their capabilities.

Contents

1.0 TI Request

1.1 Inquiry

What decoys are being developed and fielded by the U.S. Department of Defense (DoD)?

1.2 Description

The inquirer has requested information regarding the U.S. services developing and fielding any type of decoy, such as radar, missile systems, and vehicles.

2. TI Response

The Defense Systems Information Analysis Center (DSIAC) was asked to identify what decoys are being developed and/or fielded for use in the DoD. DSIAC staff searched open-source literature and the Defense Technical Information Center's Research and Engineering Gateway for related information. Programs currently developing or fielding decoys for use in the DoD are included in this report, along with a summary of their capabilities.

2.1 Introduction

Decoys are used throughout the DoD for a variety of reasons, and different varieties accomplish different missions. They mislead an "adversary by manipulation, distortion, or falsification of information" [1]. Decoys improve the Warfighter's capability to conduct electronic warfare (EW), produce alternate targets for the protection of military assets, and help increase survivability by deflecting enemy threats. Decoys have evolved over the past several decades from inflatables to electromagnetic (EM) spectrum decoys, with options in between. Recent developments in decoys have allowed them to mimic EM spectrum signatures; counter radar-guided threats (including anti-ship missiles); and protect combat aircrafts, warships, ground vehicles, and other military assets. They do not allow the enemy to pinpoint U.S. targets or capabilities through the EM spectrum and also hide in plain sight by reducing a unit's overall signature in the EM spectrum.

Decoys are designed to deceive adversaries in EM spectrum operations through a variety of methods, such as manipulative, simulative, and imitative. Manipulative deception "involves an action to eliminate revealing or convey misleading EM indicators" used by an adversary. It can lead an adversary to "misdirect actions." Simulative deception is "the action of simulating friendly, notional, or actual capabilities to mislead enemy forces." This could mean using expendables simulated as false targets or "transmitting deceptive EM attack techniques to mask

true friendly forces." Finally, imitative decoys introduce "EM energy in enemy systems that imitate enemy emissions." Decoys used in EM spectrum operations are being researched and developed more frequently than older versions of decoys, such as inflatables [1].

The variety of decoys being used in the DoD allows for increased survivability across multiple mission areas. These include towed decoys, those attached to aircraft-launched missiles for threat deflection, offboard electronic countermeasure decoys, submarine- or air-launched decoys, and radar decoys. Many of these are summarized in the following sections and include how they benefit the DoD.

2.2 U.S. Air Force

There are two prominently used decoys within the U.S. Air Force: (1) the BriteCloud AN/ALQ260(V1) and (2) the miniature air-launched decoy (MALD).

2.2.1 BriteCloud AN/ALQ260(V1)

The UK-based company Leonardo developed the BriteCloud AN/ALQ260(V1) Expendable Active Decoy. The U.S. Air National Guard (USANG) "issued a fielding recommendation for the BriteCloud 218," then designated it as the AN/ALQ260(V1). This recommendation identifies "it as an airborne EW countermeasure" [2]. It counters radar-guided threats, has a low integration cost, and can be adapted for use as an expendable decoy. The decoy can be launched from a conventional dispenser and has been tested by the United Kingdom on platforms including the F16, Tornado, and Gripen. Following this, the USANG recommended the decoy system for fielding on F-16s [3]. When fired like a flare, the AN/ALQ260(V1) uses a miniature jammer to protect combat, transport, and special mission aircraft from radar-guided surface-to-air and air-to-air missiles. Digital radio frequency memory technology allows it to transmit a convincing "electronic ghost signal to lure away incoming missiles, keeping the crew and aircraft safe" [3].

2.2.2 MALD

MALD, jointly created by the Defense Advanced research Projects Agency (DARPA) and Raytheon in the early 2000s, is an airborne decoy with a range of over 500 miles that looks like a U.S. aircraft to enemy-integrated air defense systems [4]. DARPA states that "although [it] did not directly evolve into fielded systems, management of the effort was subsequently picked up by the Air Force and follow-on efforts led to production models of what became known as [the miniature air-launched decoy jammer] MALD-J" [5].

The MALD-J decoy is a jammer version of the basic MALD. It is an unmanned system that can operate solo or in pairs and "moves much closer to the victim radar than conventional EW when jamming electronics." The ability to loiter near the target increases the likelihood of completing its mission. It is programmable, low-cost, and expendable, allowing it to deceive adversary air defense systems. Operators send multiple MALDs to a designated airspace with a preprogrammed mission "that protects allied aircraft while confusing enemy integrated air defense systems" [6].

2.3 U.S. Army

The Army is using multiple decoy systems to protect the Warfighter and its assets.

2.3.1 Electromagnetic Warfare Decoy Emitter (EWDE)

The winner of the 2023 Army Futures command annual Dragon's Lair competition developed the EWDE, which is "designed to protect soldiers from being detected in the EM spectrum." The EWDE transmits and mimics radio frequency signatures of tactical receivers "with the decoy doubling up as a frequency jammer." The emitter has a control device using software specifically for the EWDE's emitter, which "comprises an analogue synthesizer [that] emits custom frequencies" [7]. Long-range spread spectrum radio communication protocols are used to send instructions from the control device to the emitter. The EWDE is currently at technology readiness level 4, having been validated in laboratory conditions. The next steps are to make the EWDE a program of record, most likely needing an industry partner to eventually mass manufacture the emitter.

2.3.2 Spectrum Situational Awareness System (S2AS)

The S2AS program offers a commercial-off-the-shelf solution that gives "sensing and visualization of what units look like in the spectrum" and provides capabilities for "commanders to be able to sense and report in real-time their command post signature." This is crucial in understanding what a unit's electronic footprint looks like to the enemy. For fiscal year (FY) 2025, the Army requested $9.3M in research and development funds "for integration, testing, and technical and program management support of the [S2AS] program" [8].

2.3.3 Robot Decoys and Cannon-Fired Jamming Pods

The Army is studying cannon-launched jamming pods, air-dropped dummy command posts, and mobile robots pretending to be both tanks and infantry squads [9]. Decoys are being explored in the form of air- and ground-based jammers.

One of these decoys is the multifunction electronic warfare (MFEW) air system, which is a "series of flying jammers initially on drones." Lockheed Martin developed the Silent Crow EW system for a sensing-and-jamming pod to go on the Army's Grey Eagle. The first iteration is the MFEW-Air Large. The MFEW-Air Small and MFEW-Air Rotary are also offered. The MFEW-Air Small is for individualized combat brigades for use on the Shadow drone, while the MFEW-Air Rotary is a self-defense jammer for Army helicopters and future vertical-lift aircraft [9].

A ground-based system, the Terrestrial Layer System (TLS), can "be mounted on trucks and/or armored vehicles" and can also detect and jam enemy transmissions, eavesdrop, and/or relay their location to the artillery for bombardment [9]. The TLS-Extended aims to include decoy robots to extend the reach of the system and its tactical options, particularly for deception.

2.3.4 Portable Bradley Vehicle Decoys

The Army's 3rd Infantry Division partnered with Georgia Technical Research Institute students in January 2023 to develop portable Bradley vehicle decoys. "Three teams focused on developing cost-effective, portable solutions to three common ways hostile forces identify Bradleys and similar vehicles—visual identification, heat-signature detection, and EM frequency signatures such as radio transmissions." The proposed decoy comprises easy-to-find hardware store materials to achieve the goal of creating a decoy that can be carried and easily set up by one infantry squad. Other teams developed ways to "mimic radio transmissions and thermal profiles using off-the-shelf components" [10]. The workshop is just a starting point in getting these decoys developed.

2.3.5 Other

Decoy technologies were tested in early 2024 at Project Convergence, including one called MAGPIE. MAGPIE can replicate assets, including "company- to division-level radio frequency signatures—to confuse and deceive enemy signal collection" [8]. It can collect signals and copy them for rebroadcast as a decoy and has the ability to mimic a command post, ultimately confusing the enemy.

Additionally, the Army is aiming to prototype the Modular Electromagnetic Spectrum System (MEMSS), to begin in FY2026. Little has been said about the MEMSS, other than it "could employ techniques to confuse and deceive adversaries" [8].

Finally, the Army's "multidomain task forces can employ cost-effective physical decoys (like fake missile launchers or vehicles) and electronic and cyberspoofing to stimulate enemy detection mechanisms [11]." The decoys can deceive adversary surveillance and targeting.

2.4 U.S. Navy

Three decoys used in the Navy are mentioned in a 2023 report from the Naval Research Laboratory: (1) the super rapid-blooming offboard countermeasures (Super RBOC) chaff, (2) Nulka offboard countermeasure decoy, and (3) AN/ALE-50 towed decoy [12].

The Navy has used the MK-214 and MK-16 cartridges on all major Navy surface combatants as variants of its original decoy system, developed in 1977. The Super RBOC chaff and decoy launching system, along with its subsequent decoys, was used for years, since it could quickly provide an alternate target for the protection of ships against anti-ship cruise missiles [12]. It was eventually replaced by the active decoy Nulka for all capital ships of the Navy.

The Nulka offboard countermeasure decoy went into production in 1999 and is now deployed on Australian and U.S. warships as a surface ship EW system. Due to the system's fast reaction time, it is very effective against anti-ship missiles and "is effective over a full 360 degrees around the defended ship" [12]. The decoy is also effective in extreme environmental conditions.

Finally, the AN/ALE-50 towed decoy, which looks more like an aircraft than the aircraft itself, "pull[s] the threat to itself instead of pushing it away, as in the case of onboard systems." It was the first towed decoy used as an in-flight countermeasure by the Navy. More than 25,000 of these decoys have been delivered for use on the F-16, F/A-18E/F, and B-1B aircraft. It is so effective, the decoy has earned the nickname "Little Buddy," since it protects combat aircraft so closely and so well [12].

2.5 Conclusions

The DoD is investing in a wide range of decoys to increase mission effectiveness. The current trend is to develop and field EM spectrum decoys to allow units to hide their EM signature in the ever-increasing digital age. Hiding in plain sight appears to be key in deceiving adversaries through use of manipulation, distortion, and falsified information. A continued increase in funding will allow the development of decoys to provide DoD missions with the opportunity to increase the outcome of success and minimize the risk to DoD assets. While this report does not offer an exhaustive list of decoys, it does provide an overview of popular decoys being fielded, developed, or researched by the DoD.

References

[1] U.S. Air Force. "Electromagnetic Spectrum Operations." Air Force Doctrine Publication 385, https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-85/AFDP%203-85%20Electromagnetic%20Spectrum%20Ops.pdf, 14 December 2023.

[2] Leonardo Electronics U.S. Inc. "BriteCloud AN/ALQ260(V1)." Leonardo, https://www.leonardo.us/electronic-warfare-britecloud, accessed on 19 September 2024.

[3] Defense Brief Editorial. "Leonardo's BriteCloud Mini RF Decoy Passes U.S. Air National Guard Trials." Defense Brief, https://defbrief.com/2022/11/24/leonardos-britecloud-mini-rf-decoy-passes-us-air-national-guard-trials/, 22 November 2022.

[4] Mills, W. "A Tool for Deception: The Urgent Need for EM Decoys." *War Room*, https://warroom.armywarcollege.edu/articles/tactical-decoys/, 27 February 2020.

[5] Defense Advanced Research Projects Agency. "Miniature Air-Launched Decoy." DARPA, https://www.darpa.mil/about-us/timeline/miniature-air-launched-decoy, accessed on 19 September 2024.

[6] Raytheon. "MALD Decoy." https://www.rtx.com/raytheon/what-we-do/air/mald-decoy, accessed on 19 September 2024.

[7] Withington, T. "Beware of Imitations." Armada International, https://www.armadainternational.com/2024/01/us-army-electronic-warfare-decoy-emitter/, 3 January 2024.

[8] Pomerleau, M. "Army Expects to Mature Electromagnetic Spectrum Decoy and Obfuscation Systems in FY'25." *DefenseScoop*, https://defensescoop.com/2024/03/22/army-electromagnetic-spectrum-decoy-obfuscation-systems-2025/, 22 March 2024.

[9] Freedberg Jr., S. J. "Army Explores Robot Decoys & Cannon-Fired Jamming Pods." *Breaking Defense*, https://breakingdefense.com/2019/08/army-explores-robot-decoys-cannon-fired-jamming-pods/, 23 August 2019.

[10] Winkie, D. "3rd ID Soldiers and Students Develop Portable Bradley Vehicle Decoys." *Army Times*, https://www.armytimes.com/news/your-army/2023/01/13/3rd-id-soldiers-and-students-develop-portable-bradley-vehicle-decoys/, 13 January 2023.

[11] McEnany, C. "Multi-Domain Task Forces: A Glimpse at the Army of 2035." AUSA, https://www.ausa.org/publications/multi-domain-task-forces-glimpse-army-2035, 2 March 2022.

[12] U.S. Naval Research Laboratory. "The Naval Research Laboratory and Our Mission Over a Century: 100 Science and Engineering Contributions to Sea Power and National Security." https://www.nrl.navy.mil/Portals/38/NRL%20100%20Contributions_508_reduced_1.pdf, June 2023.

Biography

Mrs. Taylor H. Knight is the technical lead of the Defense Systems Information Analysis Center (DSIAC). She provides technical consultation and support for products and services produced by DSIAC associated with 10 defense-related technical focus areas (TFAs). Prior to the position, Mrs. Knight was a research analyst with DSIAC and provided research efforts across DSIAC's TFAs. She has authored dozens of scientific and technical reports on defense-related topics, with a focus on hypersonics and unmanned aerial vehicles. Mrs. Knight holds an M.S. in human resources development, instructional leadership and a B.S. in education, with a minor in biology and Spanish.