INFO FLASH
Finabel
The European Land Force
Commanders Organisation

FINABEL - THE EUROPEAN LAND FORCE COMMANDERS ORGANISATION

JANUARY 2025

WRITTEN BY
BENJAMIN ROBITAILLE

EDITED BY
ANNE-SOPHIE CUBERT

SUPERVISED BY
VICTORIANO VICENTE BOTELLA BERENGUER

Introduction

Western militaries have enjoyed a prolonged period of operational comfort marked by uncontested air superiority, during which the role of deception—particularly the use of decoys—has been increasingly overlooked. However, as we transition into an era of Artificial Intelligence (AI)-enhanced battlefield visibility, where adversaries such as Russia are becoming adept at deploying drones equipped with multi- and hyperspectral sensors, traditional approaches to deception face significant challenges. Consequently, disregarding military deception (MILDEC) techniques is no longer sustainable.

In response to this growing sophistication of detection capabilities, decoys' role becomes increasingly essential and more complex. Despite their proven efficacy in historical conflicts, Western militaries have underinvested in decoy systems, often prioritising offensive capabilities over defensive deception. This paper argues that this oversight has left a critical gap in Western military strategies, as decoy systems are not merely supportive tools but pivotal in countering advanced detection technologies and reshaping adversarial targeting dynamics. By analysing their historical roots, emerging innovations, and operational implications, this paper highlights the necessity of reintegrating decoys as a core element of modern Western military doctrine.

1. Decoys and Military Deception

Defining Their Role and Historical Context

While the roots of strategic thought on MILDEC date back to Sun Tzu's infamous teachings on the importance of misleading one's enemy, it remains a crucial principle central to ensuring modern operational effectiveness (Tzu, 1994). As Sun Tzu famously stated, "When we [the military] are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near" (Tzu, 1994, p. 3). To this effect, the decoy is a quintessential military tool in deception operations and has deep historical roots, including the use of wooden Quaker guns in the US Civil War (Chapple, 2019). One of the most famous historical examples of decoy deployment was using inflatable tanks and aircraft in World War II within Operation Fortitude (Downing, 2024). Before D-Day in 1944, the Allies used inflatable tanks mimicking 30-ton Shermans, dummy landing craft, and fake aircraft in southeast England to suggest the invasion would take place in Calais, diverting German efforts from Normandy (Hémez, 2021). By doing so, the Allies created a convincing illusion that significantly contributed to the success of the actual operation.

More specifically, the decoy is one of the three principal tools of the CCD triad: concealment,

camouflage, and decoys. (U.S. Department of the Army, 1999). Together, they seek to prevent an enemy from detecting and identifying friendly troops, military activities, equipment, and installations. Therefore, CCD is a critical element in ensuring the conservation of friendly strength and survivability, also known as operational security (OPSEC). According to US military doctrine, a decoy is "an imitation in any sense of a person, object, or phenomenon that is intended to deceive enemy surveillance devices or mislead enemy evaluation" (Joint Chiefs of Staff, 2012, GL-3).

Decoys vary widely depending on the military domain in which they are deployed. In land warfare, tactical decoys may include inflatable armoured vehicles, dummy artillery pieces, fake radars, or even decoy military installations such as runways or bridges (Hémez, 2021). In the air domain, decoys can involve drones that emit electromagnetic signatures designed to mimic attack helicopters, and in naval operations, decoy types range from dummy submarines and missile decoys to sonar countermeasures (Army Recognition, 2024a; Naval News, 2023; Rafael, n.d). Finally, with the increasing importance of cyber operations, cyber decoys have also gained prominence, accompanying the growing integration of the cyber domain into contemporary military strategies or doctrine (Scammel, 2019).

Operational

Decoys serve two primary functions. Firstly, as mentioned above, they are critical to survivability in military operations and integral to OPSEC (U.S. Department of the Army, 1999). By protecting assets through diverting enemy fire and manipulating adversary movements, decoys compel poor enemy tactical decisions, minimise strikes on real friendly targets, narrow the adversary's decision-making options, and waste their resources (Bonsegna, 2024). They achieve this by creating the illusion of a larger force, exaggerating the size of their arsenal and units. This exaggeration entails substituting equipment or personnel at the front lines to maintain the appearance of intact positions, fabricating false units to divert enemy attention, and provoking enemy fire to reveal their positions. Additionally, decoys deploy obstacles such as fake improvised explosive devices (IEDs) or mines to slow or redirect enemy movements (Rivero, 2024).

Secondly, decoys enhance situational awareness on the battlefield by drawing enemy fire, which forces adversaries to reveal their concealed positions (U.S. Department of the Army, 1999). This strategy not only provides valuable intelligence on enemy locations but also helps identify firing patterns, unit strengths, and potential vulnerabilities. By exposing these positions, friendly forces can adapt their tactics, manoeuvre more effectively, and launch precise counterattacks, gaining a tactical advantage in engagements.

Several studies conducted in the 1980s and 1990s by the US military support these effects. They found that "the presence of CCD [camouflage, concealment, and deception] greatly reduced correct target attacks, particularly when decoys were employed as part of the CCD plan" (FM 20-3, 1999). Similarly, the People's Liberation Army (PLA) recently reaffirmed the importance of decoys, claiming their use can increase the survivability of forces and equipment by up to forty per cent (Jensen, 2020). Indeed, China places MILDEC at the core of its strategy, with analysts highlighting its role as a key component of a potential amphibious invasion of Taiwan (Haydock, 2024).

Psychological

Decoys serve both operational and psychological purposes, aiming to create ambiguity about military forces' strength, positioning, and intentions, which can induce moral fatigue in adversaries (Bonsegna, 2024). By distorting the enemy's perception of reality, decoys force adversaries to question the reliability of their intelligence and situational awareness, leading to doubt and confusion.

Indeed, when an adversary falls for a decoy and expends finite resources, such as ammunition or time, on a false target, the immediate tactical losses also erode their strategic confidence. This erosion can lead to hesitation, miscalculations, and delayed decision-making in future engagements (Bonsegna, 2024). The psychological impact of sophisticated decoy systems extends beyond immediate deception; it disrupts the enemy's sense of control and situational dominance, transforming their technological and operational strengths in detection and surveillance into vulnerabilities.

Operationalising Decoys

The effective deployment of decoys depends on three key factors: fidelity, strategic placement, and cost-efficiency (U.S. Department of the Army, 1999). Fidelity refers to how realistic and convincing a decoy appears. It must replicate the visual, thermal, electromagnetic (EM), and radar signatures of the military asset it mimics (NATO Science & Technology Organization, 2024). Decoys must also balance conspicuity and plausibility, ensuring they attract enemy attention without appearing implausible or easily dismissed.

Strategic placement is equally critical. Bonsegna (2024) notes that while advancements in decoy materials have been significant, poor placement often undermines their effectiveness. The plausibility of a decoy depends on positioning it in a setting where the mimicked asset would naturally be found during wartime. For instance, during the 1999 Kosovo War, the Serbian Army employed a range of decoys, including inflatable bridges, to mislead NATO

airstrikes. However, some were placed in locations without roads or infrastructure, reducing their credibility and effectiveness (Vershinin, 2020).

Finally, cost-efficiency is an essential consideration. Hémez (2021, para. 5) highlights that "a decoy must be less expensive than the equipment it simulates and require fewer materials and less time and effort to set up than the time and effort it will cost the adversary to detect or destroy it.". This cost-benefit balance is crucial to ensuring the long-term viability and utility of decoy strategies.

2. Emerging Technological Threats to Battlefield Deception

The nature and diffusion of novel detection, tracking, and identification (DTI) technologies, which span visual, thermal, radar, acoustic, multispectral, and hyperspectral systems, have enabled persistent and pervasive intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) operations, granting adversaries near-total battlefield surveillance in real-time (Eshel, 2023; Huelss, 2024). These technologies can detect the movement and location of vehicles and personnel by identifying spectral anomalies, making the electromagnetic and physical footprint of concealed military units and assets increasingly observable. As a result, the use of decoys has become both more complex and indispensable. Russia's reconnaissance-strike complex exemplifies the severity of this threat by detecting the electromagnetic signals of two Ukrainian mechanised battalions near the town of Zelonopillya and destroying them (Mills, 2020).

Despite diversifying detection technologies, visual detection remains a critical challenge for effective decoy deployment. Advancements in high-definition imaging, optical sensors, and automated image recognition enable adversaries to identify subtle inconsistencies in decoy visual signatures, such as texture, shadowing, and geometric irregularities (Bonsegna, 2024). AI-powered image recognition further exacerbates this vulnerability by continuously improving its ability to distinguish between genuine military assets and deceptive counterparts through machine-learned patterns and anomalies (SubSea Craft, 2024).

Beyond visual sensors, thermal detection technologies exploit the distinct heat signatures emitted by vehicles, equipment, and personnel. Infrared (IR) and near-infrared (NIR) sensors can detect thermal contrasts between targets and their environments, posing a significant problem for decoys (Shephard Media, 2024). While designed to mimic the external appearance of military assets, decoys often fail to emit heat profiles consistent or dynamic enough to deceive advanced thermal sensors effectively (Hémez, 2021).

Radar and acoustic detection technologies further compound the limitations of traditional

decoys. Radar systems, including synthetic aperture radars (SARs) enhanced by automated target recognition (ATR) algorithms, can differentiate between authentic assets and decoys using complex radar cross-section (RCS) analyses (Elgamel & Abdel-Latif, 2022; Blacknell & Griffiths, 2013). Similarly, ground-based acoustic sensors can detect engine noises, mechanical movements, and other operational sounds, which decoys often struggle to replicate accurately.

AI-driven signal processing can identify inconsistencies in frequency modulation, amplitude, and temporal patterns, rendering efforts to engineer decoys that emit noise signatures mimicking real targets ineffective (Elgamel & Abdel-Latif, 2022).

Furthermore, the emergence of multispectral and hyperspectral detection systems, which integrate data from visual, thermal, radar, and acoustic sensors, represents one of the most significant threats to decoy effectiveness (Jersblad, 2024; Keller, 2024). Multispectral sensors analyse reflected radiation across 3–15 bands of the electromagnetic spectrum to detect discrepancies in various spectral signatures. Meanwhile, hyperspectral sensors capture radiation from hundreds of spectral bands, allowing the identification and quantification of material compositions, including those of decoys (Keller, 2024). However, while hyperspectral systems remain experimental, their high cost currently limits their widespread deployment, such as on drones.

Researchers are exploring the military sensor applications of quantum and interferometry technologies (Karve International, 2023; Johnson, 2024). For example, cold-atom systems detect changes in the gravity gradient, enabling sensors to identify voids. In the military sector, sensors use this capability to find underwater air pockets that may affect the detection of submarines, improvised explosive devices (IEDs), and subsurface tunnels (Karve International, 2023).

Although this technological landscape may suggest that Clausewitz's perennial 'fog of war' is diminishing and that an era of offensive dominance is emerging, deception techniques and technologies are concurrently evolving to counter these sensor threats (Savitz, 2021). Savitz (2021) argues that Western militaries must allow these threats to catalyse cultural and technological shifts, embracing deception as a critical countermeasure. Addressing these vulnerabilities will require a multilayered, multi-domain approach in which modern decoy strategies will play a pivotal role, enhancing their operational relevance in future conflicts.

3. The Development of Decoys Along the Kinetic and EM Spectrum

The proliferation of these advanced sensor and ISTAR technologies has pressured MILDEC

strategies, prompting the need for a sophisticated evolution of decoys. Despite this urgency, analysts have lamented a sluggish response among Western militaries in adapting their decoy capabilities to contemporary threats (Mills, 2020; Hémez, 2021).

In this context, the tactical effectiveness of traditional decoys is diminishing, with the reliance on simple visual decoys no longer being sufficient for effective deception. Decoys must evolve by integrating advanced technologies such as multispectral materials, AI-driven robotics, and cyber-electromagnetic deception systems to maintain operational relevance. These innovations are not just technological advancements; they represent a shift toward multi-layered, multi-domain deception strategies designed to counter increasingly sophisticated adversaries. This section explores the state of decoy development, focusing on technological progress and strategic implications across the kinetic and electromagnetic spectrums.

Multispectral

Advances in materials science and design have made modern decoys far more convincing across multiple spectrums (NATO, 2024). Companies like Inflatech have commercialised systems that replicate the radar and thermal signatures of actual military assets. For example, their decoy of the M270 Multiple Launch Rocket System uses synthetic silk fabrics and integrated heat sources to mimic the radar cross-section and thermal profile of the genuine platform (Defense News Army, 2024; Army Recognition, 2024b).

Historical examples underscore the value of multispectral deception. During a 1987 NATO exercise, a Multispectral Close Combat Decoy (MCCD) successfully misled a helicopter pilot at a range of 200 metres, causing a critical delay in identifying actual threats (Jensen, 2020). Contemporary iterations like the BQM-74F aerial drone have far surpassed these early achievements. These drones can simulate aircraft or cruise missile profiles, as demonstrated during the Gulf War and, more recently, in the Ukraine conflict (Cimsec, 2016). By integrating multispectral capabilities, tactical decoys now operate effectively across diverse environments, compelling adversaries to expend resources on identifying or neutralising false targets.

AI-Integrated Robotics and Adaptive Decoy Swarms

Furthermore, the convergence of robotics and AI has opened new dimensions in decoy technology. Robotic decoys, developed by companies like GaardTech, not only replicate the physical appearance of legitimate combat units but also mimic their movements and behaviours, enhancing their believability (Peck, 2022). For instance, autonomous land-based

decoys can simulate troop movements, while unmanned aerial vehicle (UAV) swarms can mimic the operational patterns of helicopters or attack aircraft.

AI also enables adaptive decoy formations that autonomously respond to changing battlefield conditions. These swarms can deceive adversaries by simulating heliborne operations or armoured advances. In naval contexts, unmanned underwater vehicles (UUVs) trailing 'phantom ships' can generate hydrodynamic signatures resembling large vessels, confusing sonar systems and potentially wasting costly enemy munitions (Savitz, 2021).

Ultimately, robotic decoys offer dual-use potential, serving both as deception tools and offensive assets. For example, equipping decoys with radar and missile launch detectors enables them to contribute actively to battlefield defence by triggering adversary self-protection measures and disrupting their situational awareness.

Electronic Warfare and Cyber Decoys

Finally, the integration of EW decoys into MILDEC allows for a more comprehensive approach to producing a 'ghost army.' At the intersection of the kinetic and cyber levels, future approaches may include air-droppable decoys capable of simulating the electromagnetic signature of entire vehicle formations or command centres (Hémez, 2021). These capabilities, already developed by the US in the form of its Netted Emulation of Multi-Element Signature against Integrated Sensors, or NEMESIS system, seek to overwhelm adversary sensors by saturating them with false signals, creating confusion and forcing misallocation of resources (Tingley, 2019).

Furthermore, just as inflatable tanks and fake formations confuse the enemy, cyber decoys such as honeypots create convincing but false digital environments to mislead attackers (Scammell, 2019). These strategies divert adversaries from authentic critical cyber targets, allowing defenders to gather intelligence and protect critical systems. This evolution underscores the necessity of moving beyond the traditional conceptualisation of decoys as merely physical or kinetic tools.

The trend towards robotic, multispectral decoy formations underscores their growing relevance in modern warfare. These advancements offer tactical opportunities, from saturating enemy sensors to simulating large-scale operations. The policy recommendation is to allocate one per cent of the total cost of developing high-value military assets to creating and acquiring corresponding decoys to maximise the strategic benefits of decoy systems (Bonsegna, 2024). This modest investment could significantly enhance force survivability, operational deception, and overall battlefield effectiveness.

4. Challenges and Opportunities Facing Decoy Development

More advanced decoy technologies, such as multispectral and hyperspectral systems, are significantly more expensive than traditional methods. At the forefront are metamaterials—engineered substances designed to manipulate electromagnetic waves through features like negative refractive indices and dynamic phase manipulation (Kumar et al., 2019). However, the research and manufacturing of metamaterials are still in the initial stages and remain prohibitively expensive, posing a significant barrier to widespread adoption.

Despite these challenges, metamaterials hold great promise for decoy technology. When used as coatings, they can enhance decoy effectiveness by reducing signatures for camouflage or altering spectral resonance to mimic true military assets. These capabilities make the coatings more effective at deceiving modern sensors (Kumar et al., 2019). Materials like radar-absorbing coatings and meta-surfaces can make decoys appear indistinguishable from actual platforms.

Additionally, novel decoy strategies, such as unmanned swarms, offer logistical and financial advantages over traditional methods. It is often more cost-effective to overwhelm an environment with decoys mimicking real platforms rather than attempting to completely conceal an asset's signature (Savitz, 2021). Moreover, decoy systems are more affordable than stealth technologies, which become increasingly expensive with diminishing returns. Meanwhile, conventional decoy solutions remain practical and cost-effective. Based on non-metamaterial technologies, these systems can be produced for €30,000 to €150,000, providing significant operational advantages against adversary ISTAR capabilities (Hémez, 2021; Bonsegna, 2024).

The Way Forward for Europe

For European militaries, the implications are clear: they must reinvigorate their commitment to MILDEC and make strategic investments in decoy technologies to safeguard operational effectiveness in an increasingly transparent battlespace.

First, European forces must prioritise the development of multispectral and electromagnetic spectrum decoys, leveraging AI and machine learning to outpace adversarial detection algorithms. In this vein, Germany's EUR 50 million investment in advanced infrared decoys to counter air denial strategies and Estonia's commitment to future decoy procurement are positive signs (Salerno-Garthwaite, 2024; Gosselin-Malo, 2024). Second, operational doctrines must be updated to integrate decoys seamlessly into multi-domain operations. This includes ensuring that decoys not only mimic the physical and thermal profiles of assets

but also fit into the broader context of electronic warfare, cyber deception, and counter-ISTAR efforts. Finally, the cultural perception of deception within European militaries requires updating. As adversaries, notably Russia and China, demonstrate the strategic value of deception in modern conflict, European militaries must cultivate a renewed emphasis on MILDEC as a critical component of future defence strategies. By doing so, they can reduce dependency on technological overmatch alone and enhance resilience against various adversarial tactics.

Conclusion

This paper has argued that decoys play an increasingly indispensable role in MILDEC, particularly as advancements in battlefield surveillance technologies continue to challenge traditional methods of operational security. By examining their historical significance and exploring the evolution of contemporary decoy systems across land, air, naval, and cyber domains, this analysis underscores their adaptability and strategic importance. Furthermore, by situating emerging technologies, such as drone swarms, within broader deception frameworks, it demonstrates how decoys contribute not only to operational security but also to psychological manipulation and strategic misdirection.

Ultimately, while the challenges posed by modern detection systems are formidable, the ability to mislead, confuse, and manipulate adversaries remains as critical to military success today as it was in Sun Tzu's era. Failure to adapt decoy strategies to this evolving landscape risks ceding the tactical and psychological advantages that MILDEC provides, jeopardising the survivability and effectiveness of future operations.

Bibliography

Army Recognition. (2024, August 21). Russia's wooden submarine decoy exposed by satellite images after Rostov-on-Don sinking.. Army Recognition. https://armyrecognition.com/news/navy-news/2024/russias-wooden-submarine-decoy-exposed-by-satellite-images-after-rostov-on-don-sinking

Army Recognition. (2024, February 7). Rise of military decoys at World Defense Show 2024 in Saudi Arabia. Army Recognition. https://armyrecognition.com/news/army-news/2024/rise-of-military-decoys-at-world-defense-show-2024-in-saudi-arabia

Blacknell, D. & Griffiths, H. (2013). Radar Automatic Target Recognition (ATR) and Non-Cooperative Target Recognition (NCTR). IET. 10.1049/PBRA033E.

Bonsegna, N. (2024, October 13). The strategic role of decoys in modern warfare: The conflict in Ukraine. IARI. https://iari.site/2024/10/13/the-strategic-role-of-decoys-in-modern-warfare-the-conflict-in-ukraine/

Cimsec. (2016). Deception and the Backfire Bomber: Part three. CIMSEC. Retrieved from https://cimsec.org/deception-and-the-backfire-bomber-part-three/

Downing, T. (2024, June 1). D-Day deception: Operation Fortitude: The World War Two army that didn't exist. BBC. https://www.bbc.com/culture/article/20240531-d-day-deception-operation-fortitude-the-world-war-two-army-that-didnt-exist

Elgamel, S. A., & Samir Abdel-Latif, M. (2022). Synthetic Aperture Radar Active Decoy. Advances in Military Technology, 17(1), 47-62. https://doi.org/10.3849/aimt.01520

Eshel, T. (2023, September 26). Through the Looking Glass. European Security & Defence. https://euro-sd.com/2023/09/articles/33984/through-the-looking-glass/

Gosselin-Malo, E. (2024, September 18). Estonia seeks battlefield decoys to sponge up Russian missiles. Defense News. https://www.defensenews.com/global/europe/2024/09/18/estonia-seeks-battlefield-decoys-to-sponge-up-russian-missiles/

Haydock, T. L. (2024, July 31). Defeating deception: Outthinking Chinese Deception in a Taiwan Invasion [Land Warfare Paper 162]. Association of the United States Army. https://www.ausa.org/publications/defeating-deception-outthinking-chinese-deception-taiwan-invasion

Hémez, R. (2021, April 22). To survive, deceive: Decoys in land warfare. War on the Rocks. https://warontherocks.com/2021/04/to-survive-deceive-decoys-in-land-warfare/

Huelss, H. (2024). Transcending the fog of war? US military 'AI', vision, and the emergent post-scopic regime. European Journal of International Security, 1–21. doi:10.1017/eis.2024.21

Industry Spotlight. (2024, September 30). Seeing the Unseen – The Indispensable Role of Infrared Detection in m-Modern Defense Technology. Shephard Media. https://www.shephardmedia.com/news/landwarfareintl/sponsored-seeing-the-unseen-the-indispensable-role-of-infrared-detection-in-modern-defense-tech/

Jensen, A. (2020, August 8). Deception Is Key to Chinese Military Strategies. The Diplomat. https://thediplomat.com/2020/08/deception-is-key-to-chinese-military-strategies/

Jersblad, J. (2024, October 10). Emerging solutions to beat the hyperspectral threat. Saab. https://www.saab.com/newsroom/stories/2024/october/emerging-solutions-to-beat-the-hyperspectral-threat

Gortney, W. E. (2012). Military Deception [Joint Publication 3-13.4]. U.S. Department of Defense.
https://info.publicintelligence.net/JCS-MILDEC.pdf

Johnson, S. C. (2024, June 17). US Naval Research Lab explores cold atom quantum inertial sensors for navigation. Laser Focus World.
https://www.laserfocusworld.com/test-measurement/article/55088653/us-naval-research-lab-explores-cold-atom-quantum-inertial-sensors-for-navigation

Keller, J. (2024, February 29). Navy asks Raytheon for electro-optical multispectral sensors for MQ-9, MQ-8, and other unmanned aircraft. Military & Aerospace Electronics. https://www.militaryaerospace.com/sensors/article/14305818/raytheon-technologies-corp-electro-optical-multispectral-sensors-unmanned

Kumar, N., Dixit, A., Kumar, N., & Dixit, A. (2019). Camouflage and Stealth Technology Based on Nanomaterials. In Nanotechnology for Defence Applications (155-203). Springer. 10.1007/978-3-030-29880-7_5

Mills, W. (2020, February 27). A Tool For Deception: the Urgent Need For EM Decoys. War Room - U.S. Army War College.
https://warroom.armywarcollege.edu/articles/tactical-decoys/

Mitsopoulos, D. (2023, May 23). Advanced Missile Decoys By Lacroix For The Hellenic Navy. Naval News.
https://www.navalnews.com/naval-news/2023/05/advanced-missile-decoys-by-lacroix-for-the-hellenic-navy/

NATO Science & Technology Organization. (2024). Design and Test of Multispectral Decoys for Land Warfare. NATO Science & Technology Organization. https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=17375

Peck, M. (2022, September 7). Germany is buying robots that look like Russian tanks to practice fighting the real thing. Business Insider Nederland.
https://www.businessinsider.nl/germany-is-buying-robots-that-look-like-russian-tanks-to-practice-fighting-the-real-thing/

RAFAEL. (n.d.). IDS Integrated Decoy System. RAFAEL.
https://www.rafael.co.il/system/ids/

RAFAEL. (n.d.). WIZARD. RAFAEL.
https://www.rafael.co.il/system/wizard/

Rivero, J. L. (2024, April). Decoy Warfare: Lessons and Implication from the War in Ukraine. Proceedings, 150(4/1,454).
https://www.usni.org/magazines/proceedings/2024/april/decoy-warfare-lessons-and-implication-war-ukraine

Salerno-Garthwaite, A. (2024, January 16). With €50m infrared decoy purchase, Germany seeks to outwit air denial. Airforce Technology.
https://www.airforce-technology.com/news/with-e50m-infrared-decoy-purchase-germany-seeks-to-outwit-air-denial/

Savitz, S. (2021, February). Deceive the Enemy with Emerging Technologies. Proceedings, 147(2/1,416). https://www.usni.org/magazines/proceedings/2021/february/deceive-enemy-emerging-technologies

Scammell, R. (2019, March 22). Beyond the honeypot: How military-inspired deception tactics are snaring cybercriminals. Verdict. https://www.verdict.co.uk/honeypot-military-deception-cybersecurity/

Solomon, J. (2016, June 16). Deception and the Backfire Bomber: Part three. CIMSEC. https://cimsec.org/deception-and-the-backfire-bomber-part-three/

Spencer, J. (2023, October 3). Quantum Sensing: Enhancing Situational Awareness in Defence & Military Operations. Karve International. https://www.karveinternational.com/insights/quantum-sensing-enhancing-situational-awareness-in-defence-military-operations

SubSea Craft. (2024, June 18). Autonomous Surveillance: A Game Changer For Military Intelligence. Karve International. https://www.karveinternational.com/insights/autonomous-surveillance-a-game-changer-for-military-intelligence

Sun, T., & Sawyer, R. (1994). The Art of War. Hachette UK.

Tingley, B. (2019, December 1). The Navy's Secretive And Revolutionary Program To Project False Fleets From Drone Swarms. TWZ. https://www.twz.com/29505/the-navys-secretive-nemesis-electronic-warfare-capability-will-change-naval-combat-forever

U.S. Department of the Army. (1999). Camouflage, concealment, and decoys [Field Manual No. 20-3] . BITS. https://www.bits.de/NRANEU/others/amd-us-archive/FM20-3(99).pdf

Vershinin, A. (2020, March 31). The Challenge of Dis-Integrating A2/AD Zone. Joint Force Quarterly, 97(2), 13-19. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_13-19_Vershinin.pdf?ver=2020-03-31-125227-110