155-171

CONVERGENCE OF SPACE WARFARE AND INFORMATION WARFARE FOR COUNTERING A2/AD OPERATIONS

Gp Capt (Dr) Dinesh Kumar Pandey (Retd)

Abstract

With the progress of contemporary military skills Anti Access/Area Denial (A2/AD) operations keep evolving over time. A2/AD approaches will maintain their influence on the future of battlefields and regulate the ways nations apply their power and tackle security threats. For military strategists and commanders to address the challenges introduced by these fast-paced advancements comprehensively they need deep insights into today's A2/AD landscape. By combining Information Warfare (IW) with space strategies military forces can efficiently respond to A2/AD behaviours improving their operational resilience. Military forces will be able to navigate A2/AD operations smoothly by being knowledgeable about emerging technologies with respect to IW. The study focuses on how IW with space warfare may act as formidable mission for soft as well as hard kills, to accomplish the military objectives.

INTRODUCTION

Modern warfare is not reliving in the battle field alone, but it is also fought in cyberspace. The Russia-Ukraine and Israel-Hamas are other examples of cognitive warfare in information domains which has a close tie with perception strategy. Through social media, the public has been able to interact mostly with warfare in informing the population about propaganda, as well as providing responses to fake news. Handling the

issue of whether the material published on the web is genuine or not is still significant, but here virality might be of even greater value than the content, as far as the search for support is concerned.[1]

Information in the form of resource and weapon is central to contemporary conflicts. It is a dimensionally condensed war that is also temporally compressed in terms of time and space. The 'management' of information in direction of optimal utilisation for the purpose of achievement of military objectives is key determining factor. The IW is the utilisation of information and communication technology to influence the information process and hence impair an opponent.[2]

In military operations, IW means all actions that are taken for the purpose of denying, exploiting, depreciating, or destroying the information, and thus the functioning of the opponent. It also covers defending ourselves from those acts and using own military information functions. Cyberwarfare, electronic warfare and cyber-attack are part and participle of IW. When the activities of counter forces exist in space, cyber and the electromagnetic domain, the response will be soft kill of the intended targets. Expanding the concept of warfighting domains to incorporate space and cyberspace has greatly added to its scope, and conduct of information operations.[3]

BRIEF HISTORY OF IW

Using information as one of the key weapons is not an innovation, but military missions indicate noticeable and emergent problems in information operations. Data is pervasive, but aggravates the C2C interaction. IW is information, deception, cyber actions, and public activities, while conventional forces rely on air supremacy, force and mobility. Conventional warfare refers to the use of firepower both individual and team fired systems within a tightly knit fire control network, to rapidly destroy enemy formations and fire control nodes. Air power has a splendid record in fighting, but it shows a consistent failure in the attempts to adequately harness the information environment as a strategic, operational, and tactical weapon.

If warfare is governed by the strategy and missions, which is then governed by intelligence, it is the business of the military to anticipate and counter probable contingencies. From the media point of view, the reduction on the Iraqi route of death, which is a strategic mileage in Iraq that was highly attacked and destroyed during the First Gulf War, are thought of as taken a determinant in lessening the coalition attacks.[4]

The falsification, or 'hiding' of the events at the battlefield has become a characteristic feature of war since ancient times. For this reason, the First World War may be viewed as one of the key moments in the use of information operations. For the first time it used electronic warfare by intercepting the wireless communication. The inputs, like during the start of the war Great Britain cut all cables from Germany and they had none at all. It is known that such a strategic decision in informational confrontation was exactly used in intercepting the Zimmerman telegram.[5]

To effectively counter A2/AD operations, information warfare and space warfare must come hand in hand to enhance the mission productivity.[6] The following are a few examples of contemporary wars:

In the 2014 Ukrainian conflict, Russia disrupted Ukraine's satellite communications to hinder command and control. Russia combined space-based Intelligence, Surveillance, and Reconnaissance (ISR) with cyber-attacks were carried out to disrupt Ukraine's command and control, during the Russia-Ukraine conflict (2014).[7]

Russia's 2015 cyber-attack on Ukraine's power grid demonstrated the potential for information warfare to disrupt critical infrastructure.[8] In the 2018 Syrian conflict, Russian forces employed electronic warfare to disrupt coalition communications. ISIS effectively used social media for psychological operations, recruiting, and propaganda. The US used space-based ISR assets to track ISIS movements in Iraq and Syria.[9]

In US-China Conflict (2020), The US used space-based assets to detect and disrupt Chinese anti-ship missile systems. During Israeli-Hamas Conflict (2021), Israel used space-based ISR and cyber capabilities to disrupt Hamas's command and control.[10]

To prevent the use of Ukrainian drones and direct coordinate strikes on Russian targets, Russia was also able to interfere with GPS in Ukraine. Number of satellites are employed for a variety of purposes, including navigation and mapping. To disrupt the Ukrainian operations, GPS satellite signals are being targeted by Russian forces from ground stations. On February 24, 2022, the Russia-Ukraine conflict commenced, but jamming was already underway. In the course of their operations in Crimea, which was previously part of Ukraine, the Russians employed GPS interference. A2/AD operations are equally affected with such threats.[11]

ANTI-ACCESS/AREA DENIAL

A2/AD is a concept that is intended to achieve a goal of denying adversaries, a particular geographical region while at the same time making it easier to exploit vulnerabilities in regard to operations within the region. A2/AD is relevant in the air, ground and at sea environments or any fusion of these environments.[12]

Current and potential future adversaries are purposefully designing A2/AD envelopes to keep the enemy forces from approaching key tactical areas. A2/AD is also a combination of sensors, antiship, antiaircraft and ground defences and a long-range fire which are deployed and established by one country to make sure that the aggressor does not advance for the fight. The positions that these zones have are very strategic because they can change the balance of power in a region after.[13]

For Examples: China is building A2/AD zones to deny US forces access to Taiwan and the South China sea. Russia is developing A2/AD zones in the Kaliningrad, Crimea, the Kola Peninsula, and the Kuril Islands to deny the sea lanes necessary for entry.[14]

TARGETING A2/AD FROM SPACE

It was observed that the extent of A2/AD zones' weakness was their command-and-control nodes, which operated as a unique point of

failure, due to disruptive vulnerabilities to Network Centric Operations and communications. However, the US has potential strategies such as precision guided technology for a brief low-cost decapitation initiative targeted at these nodes, that could counter these weaknesses and store the balance. The offence-defence ratio has been squarely seated on the offence for decades. As technology in networks, Artificial Intelligence (AI), and space is advancing, it is having the effect of making these zones more perilous by restoring the upper hand to defence.[15]

Space is an important force multiplier in the area of warfare by providing essential needs for operation that include intelligence, surveillance reconnaissance, communication, navigation, and cyber operations. Tactical assets located in space enable militaries to gain information superiority, provide safe and efficient command and control, and coordinate operations across space and cyberspace, land, maritime, and air on a global scale. However, with the rising use of space for information operations, there are vast weaknesses that expose fundamental infrastructure, and therefore there is a need for precocious defence of such crucial resources. More so, with the improvements in countries and their integration of space-based technologies into their military doctrines, the importance of space in support of the facilitation of information superiority will rise progressively taking its place as one among the main battle grounds in future conflicts.

IW is an essential element of an integrated system of informational assets and informational power. Today, space / info as a domain of warfare has transformed the overall warfare and has provided unprecedented power projection and influence over an opponent. There are variety of applications for the integration of the space and information domains that improves operations, providing instances of the effectiveness of each domain.

THE ROLE OF SPACE IN CONTEMPORARY IW

The space as a strategic domain for military operation, which offers such importance functions as communication, navigation, and intelligence.

Securing physical control and domination of space instruments can enhance significantly a state's military effectiveness. For example, the American GPS supports precise locality and aiming in military operations around the world. In the same manner, reconnaissance satellites deliver timely information that is so valuable in formulation of strategies.

The number of cases of disruption to the communications, navigation, and missile systems of space assets during the Gulf War in 1991 were observed. To a large extent United States benefited from satellite communications and GPS to organise multi-contingency successive sophisticated strategies and accurately co-ordinate the tactical layouts. This method also illustrated the influence of space capabilities within evolving warfare systems.[16]

INFORMATION WARFARE: SHAPING PERCEPTIONS AND INFLUENCING OUTCOMES

Information war is the intentional manipulation, disruption or control of information systems in an effort to affect target adversaries. Cyber operations, psychological operations and electronic warfare can be narrowed down within this strategy. The purpose is altering perceptions, sapphire, and gaining tactical advantages without actually going toe to toe.[17]

At the same time, the conflict between Russia and Ukraine gives evidence of the significance of the informational aspect as the type of war. Among them are highly sophisticated cyber warfare and disinformation as the weapons that have been applied to mobilise public opinions in order to incite unrest. Various elements of IW, with relevant examples are appended below.[18]

- **Cyber-attacks.** Cyber-attacks designate a conventional method of information warfare, in which adversaries use malware, viruses, or misleading software to either stop, harm, or illegally exploit information systems. Discovered in 2010, the Stuxnet worm greatly damaged the centrifuges at Iran's nuclear facilities.

- **Disinformation Campaigns.** Disinformation is characterised by the relentless supply of the public with false or fake news with an aim of modifying their attitudes or eliminating social integration. The case of Russia's part in the 2016 United States Presidential election is still relevant. In order to have an effect on the election results, Russian operatives put out both issues that divide and misleading information through social media.
- **PSYOPs.** Information psychological operations' aim is to change the targeted audiences' general mood, plans, and behaviour patterns. The fliers dropped by the US military over the Iraqi troops during Gulf War encouraged them to surrender and was able to guarantee them good treatment. In demoralisation of Iraqi forces and leading to many large surrenders, the method used did succeed.
- **Electronic Warfare.** In warfare, good communication is beneficial, yet it can sometimes create a vulnerability. In 2007, the Israeli Air Force used electronic jamming to break down Syrian radar defences, permitting Israeli jets to complete a strike on a suspected nuclear reactor without alerting anyone.
- **Social Media Manipulation.** Using social media for propaganda dissemination or the shaping of public beliefs is a new variation on information warfare. More than just exposing the Facebook data collection from millions of users, the Cambridge Analytica case revealed that it had used that data to impact voter behaviour during the 2016 U.S. Presidential Election.[19]
- **Economic Disruption.** One can target economic systems in information warfare. In response to the film 'The Interview', North Korea's cyber-attack on Sony Pictures in 2014 served two purposes: to inflict economic damage and to intimidate other organisations.[20]

Like other systems, to develop and set A2/AD zones, requires ISR components apart from the strike systems even in offence as well as defence. ISR systems are used to search for outgoing threats that can

attack by Defensive Strike Systems. Preventing actions against attack systems has a goal to slow down build-up against US force in enemy structures, supplies and focal points. Bait and deception operations that epitomise efficiencies of A2/AD bubbles, rise guarantor's ground sparring probability. Along with such an approach, the use of these techniques jointly with the technologies that make defence a more powerful kind of warfare, will indicate the extent of the impact at the strategic level in the following years. The first and central tactful aim of the defender is not to beat the United States in a conflict but to get to a point that the cost for every extra user erodes the political gain than the cost per user to United States.

The primary strategic goal of the defender is to uphold, not to outperform the United States in battle, but to raise the costs to the United States until the likely political gain lessens compared to the loss.

A2/AD practises are about using weaponry, sensors, and strategies to obstruct an adversary's entrance or operations in a specific geographic area.

Electronic warfare operational end-to-end capabilities are long-range precision weapons designed for limiting the movements of the enemy forces to a certain extent, or denying the opponent forces to a definite geographical area. Various missile systems, electronic warfare capabilities, air defence networks & long-range precision weapons all are used to challenge the mobility of potential opponents.

Engaging IW it is shown that military forces can effectively counter, limit, deceive or nullify the operations of their adversaries in the A2/AD contexts.

INTEGRATION OF IW WITH SPACE WARFARE AGAINST A2/AD

The space and IW feed off of the synergy that exist between the two and enhances the abilities of the military capabilities. Objects placed in space lie at the basis of information operations, providing people around the globe with internet connections and real-time information transfer. In addition to its other functions, IW is also responsible for protecting the

operational capabilities of space assets from threats that are digital and electronic, thus lending some reassurance about the future of space.

One of the clear examples of synergy in space is the application of ASAT weapons that is anti-satellites weapons. China, in 2007 criticised all tests in this regard and at the same time conducted a live ASAT test demonstrating off how it could wipe out satellites in orbit.[21] It threw light on the vulnerability of space assets and the need for strong IW just to protect those assets. Imposition of cyber defence and electronic countermeasure remain significant, critical for a militarns forces to effectively safeguard space assets while maintaining tactical advantage and dominance.

IW, when integrated effectively, enhances both operational effectiveness and survivability through the following mechanisms:

- **Disruption of C4ISR Networks**. The systems focused on A2/AD operations greatly depend on C4ISR networks—command, control, communications, computers, intelligence, surveillance, and reconnaissance—for both targeting and coordination. By employing Electronic Warfare (EW) and cyber operations, military forces can unleash the full disruptive potential of IW, effectively disrupting or degrading these networks:[22]
    - **Electronic Jamming and Spoofing.** Interfering with enemy radar and communication systems to stop the organisation of missile defence manoeuvres or diminish sensor precision.
    - **Cyberattacks on Data Networks.** Gaining access to or incapacitating principal information networks can confuse the early warning systems of the enemy or misrepresent their command-and-control functions.
    - **Deception Operations.** Militaries are able to misguide their opposition about the locations or goals of their forces, minimising the ramifications of A2/AD targeting, by introducing false information into their information framework.

- **Example.** Blending advanced EW systems including the U.S. EA-18G Growler and others reveals the promise of shielding sensor and radar assets necessary for A2/AD tactics.[23]

- **Denial of Situational Awareness**. Denying the enemy to have accurate situational awareness for decision making, is a crucial part of countering A2/AD strategies. The IW has the potential to do so. For the purpose of achieving this goal, IW might follow different approaches, which may include both cyber and kinetic operations on monitoring infrastructure, use of decoys or fake targets and the monitoring of activities in the electromagnetic spectrum.

  - **Cyber and Kinetic Attacks on Surveillance Assets.** By making adversary satellites unusable (soft kill) or destroying (hard kill) them, as well as the disabling or destruction of drones and ground-based sensors (radar) facilities on earth, one can impair the detection and engagement abilities of incoming forces.[24]

  - **Use of Decoys and False Targets.** Saturating an adversary's sensors with physical or digital decoys enables a push for them to thinly distribute their resources or to target fraudulent targets. During the Gulf War, the coalition military resorted to quite an elaborate camouflage – fake formations such as inflatable tanks and radio chatter to limit the enemy's ability to achieve A2/AD advantages.[25]

  - **Electromagnetic Spectrum Management.** Adjusting the spectrum to achieve electromagnetic silence or to deceive signatures can obscure information on military actions for the adversary.[26]

  - **Example.** In the Gulf War the actual operations of the coalition also decreased the A2/AD control of Iraq with decoys and fakes including inflatable tanks and false radio traffic.

- **Influence Operations and Psychological Warfare.** Psychological operations can be directed at the decision making of the adversary's leadership, as well as the will of the adversary's forces.
    - **Psychological Operations (PSYOPs).** The job of propaganda, misinformation, and disinformation is to sow confusion, cast doubt, or obstruct the movement of opponents in their decisions. The misunderstanding of hazards may result in a misuse of resources.[27]
    - **Cyber and Social Media Operations.** By using web platforms to disseminate disinformation and to create doubt about how truly effective A2/AD defences are. Making political and military leadership a target could require a rethink of the A2/AD assets.
    - **Perception Management.** Engaging in covert information operations that quietly modify an enemy's perspective of the operational environment and thus slow their decision-making and reduce confidence in their A2/AD systems. For example, the utilisation of Russian IW tactics of a hybrid kind in Crimea led to improved coordination among Ukrainian forces and shaped international narratives in ways that advanced the delay of international responses.
- **Achieving Benefits of Cyber Superiority for Improved Command and Control.** The friendly forces gain superiority of the cyber domain, enhance their own operations in the operational area under A2/AD conditions. This involves:
    - **Securing Communication Networks.** Affording friendly forces unhindered access to continue manoeuvre and not to be interrupted or intercepted in certain parts of the battlespace requiring unambiguous command and control.
    - **Cyber-physical Integration.** Combining this information in real time at a faster rate than the adversary utilising

advanced AI and machine learning techniques to counter active A2/AD threats on the battlefield.

- **Resilient Networked Warfare.** Introducing mesh or regional, multiplexed networks of 'last mile' communication hopscotching, and prognosticated sensory nodes or taps that can operate autonomously or redundantly in the occurrence of aggressor cyber or EW surges.

- **Offensive Cyber Warfare and Kinetic Integration.** Offensive cyber operations can be synchronised with kinetic strikes to disable or degrade A2/AD capabilities:
  - **Pre-emptive Cyberattacks on Key Nodes.** Military forces can succeed by locating and penetrating this system's cyber support structures; the A2/AD systems' operation will be hindered as a result. This may refer to blunting air defence command structures, logistics structures or power sources for A2/AD systems.
  - **Integration with Precision Strikes.** Equally, cyber operations can mute the A2/AD command centres and radars which gives the precision targets for kinetic attack and deny the other side any airborne or missile response.
  - **Example.** In 2007, the cooperation between physical and cyber was shown during Israel's Operation Orchard in Syria when the silent breach of Syrian air defences is said to have been accompanied by cyber sabotage that allowed the Israeli aircraft to attack a suspected nuclear site.[28]

- **Net-Centric Warfare and Decision Superiority.** IW supports NCW, where a faster decision cycle defeats A2/AD systems of the adverse party.[29] This is achieved by:
  - **Shared Battlespace Awareness.** Connecting all sensors and shooters in different domains such as air, maritime, space and cyberspace to generate operative picture on a common VTC.

- **OODA Loop Acceleration.** Far from deploying A2/AD systems as a separate mode of warfare, by accelerating the OODA loop friendly forces disrupt the decision-making cycle of the adversary and strike before the adversary can respond.
- **Multi-Domain Operations (MDO).** Inclining towards a synchronised actions approach across different domains (space, cyber, and kinetic) to saturate and outrun A2/AD systems.[30]
- **Example.** The United States and NATO have aimed to improve the multi-domain command and control to acquire decision advantage and overcome A2/AD bubble, which provides forces nonlinear opportunities.

To develop a robust line of defence against the varied threats from IW, different approaches may be exploited subject to availability of resources and feasibility of mission.

WAY AHEAD

Convergence of space warfare and IW is the need of the hour for the successful conduct of the countering A2/AD operations. Considering lessons learnt from the history of air warfare, formulation of conducive standard operating procedures for exploiting available resources merits consideration.

- **Doctrine and Strategy.** Developing a comprehensive and integrated doctrine to address IW and space warfare is essential for the accomplishment of missions to counter A2/AD operations. An explicit command-and-control structure is vital for such operations.
- **Capacity Building.** The conduct of the exercises and training for all joint operations, particularly joint exercises in space and IW, plays a pivotal role. These training sessions will make crew to

feel part of the strategy. The use of space-based assets to carry out space-based ISR capabilities also necessitates advanced satellite communications systems, ensuring a more secure and well-equipped systems. Availability of anti-satellite missile defence systems is of paramount importance.

- **Cyberwarfare.** The cyberwarfare capabilities may be enhanced to continue information warfare. It is necessary to develop an AI environment for information operations that can be used in automated data analysis, identify potential threats for correct decision-making, develop EW capabilities for uninterrupted operations, maintain good cybersecurity practices, provide an anti-satellite missile defence system and conduct regular vulnerability assessments.

- **Convergence.** Ensure that information warfare and space systems are seamlessly integrated to achieve the contemplated results successfully. There should be standards and a common data architecture to conduct information warfare and joint space exercises.

CONCLUSION

The integration of space operations and IW specifies a major change in military strategies. Militaries are better able to complete their tactical objectives more efficiently by maximising the specific traits of space warfare as well as IW, in their efforts relating to power projection and control. As technological progress continues, the collaboration between space and IW will become ever more important in the development of future warfare.

IW is a potent and effective tool against A2/AD strategies and its applications span from the tactical level through operational; and even up to the strategic level of war. By attacking the information system of the adversary, Jamming's deception, control of own and denial of adversary’s network, physical destruction of key enemy nodes, and

co-ordination of cyber operations with physical attacks, military forces could combat efficiently in redundant A2/AD zones. Such operations depend on specific cyber, electronic, and psychological features of warfare recognised by them and to gain informational advantage over adversaries and focus on their vulnerabilities. The armed forces and combatant commands must better organise and prepare themselves to act in the information domain.

★★★

Gp Capt (Dr) Dinesh Kumar Pandey (Retd) was a Group Captain in IAF. He had served in the IAF for more than three decades. He has an experience of more than 2500 Air combats. He was the Director Air Staff Inspections and retired as Director, Joint Control and Analysis Centre. He has written research papers for journals and websites. Presently he is a Senior Fellow at the Centre for Air Power Studies (CAPS).

NOTES

1 *Benjamin Jensen and Divya Ramjee, "Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs", December 20, 2023, https://www.csis.org/analysis/beyond-bullets-and-bombs-rising-tide-information-war-international-affairs. Accessed on September 3, 2024.*

2 *Col Andrew Borden, "What is Information Warfare?", Air University, 1998, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf. Accessed on September 5, 2024.*

3 *"Decoding Anti-Access/Area Denial (A2/AD) Strategy", Military Sphere, June 10, 2024, https://militarysphere. com/anti-access-area-denial-a2-ad/. Accessed on September 4, 2024.*

4 *Nick Brunetti-Lihach, "Information Warfare Past, Present, and Future", The RealClear Defense, November 14, 2018, https://www.realcleardefense.com/articles/2018/11/14/information_warfare_past_present_ and_future_113955.html. Accessed on August 28, 2024.*

5 *Gordon Corera, "How Britain Pioneered cable-cutting in World War One," BBC, December 15, 2017, http://www.bbc.com/news/world-europe-4236755. Accessed on April 3, 2018.*

6 *Dorothy Sherwood, "Integrating space into Information Warfare", US Cyber Command, January 16, 2024, https://www.cybercom.mil/Media/News/Article/3647026/integrating-space-into-information-warfare/. Accessed on October 3, 2024.*

[7] *Alexander Salt and Maya Sobchuk, "Russian Cyber-Operations in Ukraine and the Implications for NATO", August 2021, https://www.cgai.ca/russian_cyber_operations_in_ukraine_and_the_implications_for_nato. Accessed on October 24, 2024.*

[8] *"Cyberattack on Ukraine grid: here's how it worked and perhaps why it was done", The Conversation, January 18, 2016, https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802. Accessed on October 24, 2024.*

[9] *Anna Varfolomeeva, "Signalling strength: Russia's real Syria success is electronic warfare against the US", May 1, 2018, https://thedefensepost.com/2018/05/01/russia-syria-electronic-warfare/. Accessed on October 24,2024.*

[10] *Robert Ashley, John M. Bednarek, "Gaza Conflict 2021 Assessment: Observations and Lessons", JINSA, https://jinsa.org/wp-content/uploads/2021 /10/ Gaza-Assessment.v8.pdf. Accessed on October 6, 2024.*

[11] *Elizabeth Howell, "How Russia's GPS satellite signal jamming works, and what we can do about it", SPACE, April 14, 2022, https://www.space.com/gps-signal-jamming-explainer-russia-ukraine-invasion. Accessed on October 24,2024.*

[12] *Douglas Barrie, "Anti-access/area denial: bursting the 'no-go' bubble?", Institute for Strategic Studies (IISS), https://www.iiss.org/ar-BH/online-analysis/military-balance/2019/04/anti-access-area-denial-russia-and-crimea/. Accessed on September 6, 2024.*

[13] *Alex Vershinin, "The Challenge of Dis-Integrating A2/AD Zone: How Emerging Technologies Are Shifting the Balance Back to the Defense", National Defense University Press, March 31, 2020, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106488/the-challenge-of-dis-integrating-a2ad-zone-how-emerging-technologies-are-shifti/. Accessed on September 6, 2024.*

[14] *Jon Lake, "China's Stealthy Area Denial", Asian Military Review, March 14, 2023, https://www.asianmilitaryreview.com/2023/03/chinas-stealthy-area-denial/. Accessed on September 3, 2024.*

[15] *Ibid (Alex).*

[16] *Frank Gallegos, "After the Gulf War: Balancing Spacepower's Development", September 18, 1997, https://apps.dtic.mil/sti/pdfs/ADA329263.pdf. Accessed on September 3, 2024.*

[17] *Alcazar and Thomas, "A Role for Land Warfare Forces in Overcoming A2/AD", Military Review, Nov-Dec 2013, https://www.armyupress.army.mil/Portals/7/military-eview/Archives/English/MilitaryReview_20131231_art014.pdf. Accessed on September 6. 2024.*

[18] *Margaret Rouse, "Information Warfare", Techopedia, January 4, 2017, https://www.techopedia.com/definition/29777/information-warfare. Accessed on September 3, 2024.*

[19] *Ibid (Techopedia).*

[20] *Ibid (Techopedia).*

[21] *Carin Zissis, "China's Anti-Satellite Test", Council on foreign Relations, February 22, 2007, https://www.cfr.org/backgrounder/chinas-anti-satellite-test. Accessed on September 4, 2024.*

[22] *Ibid (Alcazar).*

[23] *Stefano D'Urso, "Let's Talk About The Digital Evolution Of Electronic Warfare", The Aviationists, October 26, 2020, https://theaviationist.com/2020/10/26/lets-talk-about-the-digital-evolution-of-electronic-warfare/. Accessed on September 3, 2024.*

[24] *Ibid (Alex).*

[25] *"Decoys: The Art of Disguise", L.A. Times Archives, February 11, 1991, https://www.latimes.com/archives/la-xpm-1991-02-11-mn-839-story.html. Accessed on September 1, 2024.*

[26] *Ibid (Alex).*

[27] *MG Yevtodyeva, "Development of the Chinese A2/AD System in the Context of US–China Relations", Springer Link, September 29, 2022, https://link.springer.com/article/10.1134/S1019331622120048. Accessed on September 9. 2024.*

[28] *Mohan B. Gazula, "Cyber Warfare Conflict Analysis and Case Studies", MIT, May 2017, https://cams.mit.edu/wp-content/uploads/2017-10.pdf. Accessed on September 3,2024.*

[29] *Alberts, Garstka & Stein, "Network Centric Warfare: Developing and Leveraging Information Superiority", NCW, February 2000, http://www.dodccrp.org/files/Alberts_NCW.pdf. Accessed on September 9,2024.*

[30] *Shaun Cannon, "The Alliance's Transition to Multi-Domain Operations", JAPCC, Edition 37, 2024, https://www.japcc.org/wp-content/uploads/JAPCC_J37_screen.pdf. Accessed on September 3, 2024.*