Introduction

Roy Hamans, Marc Gouw, Edwin Dado, René Janssen and Kerry Malone

NATO's original definition of Anti-Access Area Denial (A2/AD) as "warfighting strategies focused on preventing an opponent from operating military forces near, into, or within a contested region"[1] no longer captures the realities of contemporary conflict. This volume argues that A2/AD has evolved from a predominantly defensive military deterrent into a technologically advanced, integrated, multidomain system for denial as well as coercion, whose effects increasingly extend into social, political and economic domains or the 'whole-of-society'. This evolution demands fundamental conceptual and practical reappraisal.

The threat of A2/AD is not new, nor does it alter military capabilities per se.[2] What is new is that recent developments show A2/AD is no longer solely about blocking an enemy's military access to a country or operational theatre. Instead, capabilities – military and otherwise – that are traditionally associated with A2/AD are increasingly used beyond the battlefield, beyond military targets, and outside of a declared war. These capabilities are now actively employed to target critical infrastructure, digital systems, and societal cohesion that support open democratic societies. This volume emphasises this shift and addresses it by combining academic and practitioner perspectives on how A2/AD capabilities are utilised today and how they should be countered: not solely as a military issue, but as a technological advancement and strategic concern for entire societies.

Reassessing A2/AD in the Light of Hybrid Warfare

A stark illustration of this shift is the sabotage of Norway's Bremanger dam in April 2025, which marks one of the first formally attributed attacks against a NATO ally's critical infrastructure. The deliberate opening of a dam's floodgate, releasing 500 litres of water per second to flow unnoticed for hours,[3] led Norwegian authorities to formally attribute this state-sponsored sabotage to a hybrid warfare strategy[4] that blends cyber, physical and informational means. According to Beate Gangås, head of the Norwegian Police Security Service PST, such acts aim not only to disrupt infrastructure and demonstrate capability but "to exert influence and

create fear or unrest in the population"[5]. These operations are part of adversaries' non-kinetic and kinetic multidomain A2/AD systems, now employed offensively as elements of hybrid warfare campaigns.

Similar dynamics are observed in the ongoing war against Ukraine, where the strategy of systematically targeting critical civilian infrastructure is 'unmistakable' and has been condemned as 'unlawful.[6] Human rights organisations have highlighted how deliberate attacks on energy facilities, water systems and other essential services aim to make daily life impossible and the "sole purpose of terrorizing civilians is a war crime"[7]. In response, the International Criminal Court in The Hague has issued warrants for the arrest of individuals "responsible for the war crime" of "directing attacks at civilian objects" and "causing excessive incidental harm to civilians" as well as "the crime against humanity of inhumane treatment"[8]. These developments show that the use of A2/AD capabilities now extends beyond military conflicts and the battlefield, reaching into society at large, especially in legal, moral, and humanitarian areas, as enemies deliberately target the civilian domain as part of their operational strategy.

A2/AD, Hybrid Wars and the Grey Zone

The examples of Norway and Ukraine show how A2/AD capabilities have advanced beyond traditional targeting of military forces in the theatre to include civilians, critical infrastructure, and digital systems. These attacks are not isolated incidents, but as part of a broader pattern of 'hybrid wars'[9] that blur the distinctions between war and peace, state and non-state actors, combatants and non-combatants, with adversaries employing physical, virtual and cognitive tools in a synchronised way. As the analysis of hybrid warfare already noted, such campaigns combine military and non-military instruments, all forms of warfare and tactics, to exploit vulnerabilities across multiple domains 'simultaneously'[10].

Political leaders increasingly acknowledge that European democracies are operating in a 'grey zone'. As a Dutch minister of Defence observed "we are not living in a state of war […] but we are not living in peace any more either. In this grey zone, we need to defend against hybrid attacks"[11]. Intelligence officials have similarly begun to warn that adversaries are "testing us in the grey zone with tactics that are just below the threshold of war," according to Blaise Metreweli, the head of MI6, on December 15th 2025,[12] and probing resolve and resilience while avoiding clear triggers for collective defence. In this environment, A2/AD is no longer seen as a way to keep military forces out of a region but as a tool to restrict political decisions, influence public opinion, and weaken confidence through sustained, ambiguous pressure.

A2/AD and the Vulnerability of Open Democratic Societies

Open democratic societies such as Norway and the Netherlands are particularly exposed to these developments because their prosperity and legitimacy depend on the transparent, reliable operation of complex infrastructures and institutions. Medium-sized, trade-dependent economies like the Netherlands rely on open seas, free skies, and the unrestricted movement of people, goods, and data. Such unimpeded movement is facilitated by accessible ports, communication cables and satellites, digital systems, energy grids and sectors that are increasingly targeted by adversaries.[13] Their openness is further reinforced by international agreements, the rule of law and robust regulatory and oversight mechanisms. Yet this very openness makes them vulnerable[14] when data is widely available in the public domain, or can be illicitly accessed through infiltration and hacking.

The interconnectedness of critical infrastructures and related systems amplify the ripple effect of disruptions,[15] magnifying the societal impact of attacks that may initially appear local or technical. Recent global cybersecurity assessments show that geopolitical instability is reshaping the threat landscape, with critical infrastructure increasingly targeted as an entry point for broader coercive strategies. Following such acts, the erosion of confidence is measurable. A 2025 survey by the World Economic Forum, involving hundreds of leaders and academics from 92 countries, reports that 31% now lack confidence in their nation's ability to manage major cyber incidents, up from 26% in 2024.[16] The prominence of these concerns in mainstream publications like those used here, rather than niche military or technical ones, indicates that uncertainty and vulnerability are spreading throughout society at large.

From Military Deterrence to Multi-Domain Coercion

Traditionally A2/AD was understood as a defensive military posture aimed at raising the costs of intervention by a stronger adversary. Earlier definitions of A2/AD distinguished anti-access (A2) measures, designed to prevent an opponent from deploying its forces into a given area, from area-denial (AD) measures intended to keep them from operating freely in that area.[17] In this context, A2/AD aimed to challenge military dominance by establishing 'contested zones'[18] where damage could be inflicted on approaching forces, thereby deterring or complicating intervention, particularly for actors like the United States operating in forward theatres and western force projection in general.[19] Such contested zones would typically be within a few hundred kilometres of the coast, on land and below 15,000 feet in the air. Adversaries have demonstrated that it is possible to engage U.S. forces

in this manner, and although few have achieved victory, others have managed to impose costs and retain some advantage for their forces.[20] This illustrated the logic of A2/AD as a defensive deterrent aimed at neutralising physical threats by opposing military forces within defined geographic areas.

Strategic intent aside, technological advancements and cross-domain integration have fundamentally transformed the nature and application of A2/AD systems. These advancements encompass intelligence, surveillance, and reconnaissance (ISR) technologies, long-range and precision strike capabilities, hypersonic systems, cyber warfare (EW), and the formal inclusion of the space domain within military forces. These technologies, which have converged into increasingly integrated multidomain capabilities, also seem to have enhanced their use for more offensive purposes. In recent years, adversaries have also potentially surpassed NATO's defensive systems[21] thereby threatening the European homeland, and reducing the technological advantage of Western forces, including US precision strike capabilities and global force projection.[22]

Threats are thus no longer only physical in theatre or deterrent, as virtual intrusions into cyber and information space pose increasing challenges to public and private systems alike. Because modern economies, administrations and communities depend on networked digital infrastructures, the offensive use of cyber A2/AD alone can jeopardise the functioning of entire societies,[23] with cascading effects that would make effective crisis management or military response difficult. Given their substantial impact on the 'whole of society', it is likely that A2/AD systems like these will be employed during military conflicts. Yet even the perceived threat to economies and societies in a pre-conflict environment risks escalating crises into armed conflict[24] as actors respond to coercive pressure that remains intentionally ambiguous in origin.

Societal Systems, Coherence and Cognitive Targets

As societal systems become more digital, open, and transparent under democratic oversight and market efficiency, their vulnerabilities have become more visible and exploitable. Critical assessments emphasise how geopolitical instability is reshaping cyber risk and how adversaries increasingly target critical infrastructure[25] as part of broader strategies to coerce societies. While high-profile acts of sabotage against pipelines, cables, or dams attract public attention, and given their physical nature can be repaired albeit at significant cost, more subtle activities may be even more consequential.

Less publicly visible threats include orchestrated disinformation campaigns, support for radical or fringe movements and the deliberate transformation of

demonstrations into serious security challenges.[26] These activities undermine social trust, polarise political debate, and erode confidence in institutions and international law and order, without producing clearly attributable 'events'. Together with more visible physical and cyber-attacks, they challenge the cognitive and societal aspects of resilience,[27] making deterrence, crisis management, and collective defence more complicated. As a result, A2/AD must be understood as operating along physical, virtual, and cognitive axes, with effects that are both cumulative and immediate. This calls for a re-evaluation of the concept of anti-access/area denial (A2/AD).

Re-appraising A2/AD: Through Technological Advancements to a Whole-of-Society Approach

The reality outlined above underscores the need for a paradigm shift in how A2/AD is conceptualised and addressed. A2/ AD can no longer be regarded merely as a bounded, theatre-specific military challenge focused on access to, and control of, defined operational spaces. Instead it must be understood as a strategic component of hybrid warfare, that targets physical, virtual and cognitive dimensions, with the aim of undermining society as a whole and putting societal resilience under sustained pressure.[28] In this context, modern A2/AD can be viewed as a collection of multidomain capabilities which can be used for damaging both military and civilian systems, eroding cohesion within societies and alliances, and constraining political decision-making under pressure.

The analysis set forth in this introduction thus reframes A2/AD not solely as a military challenge to be confronted during the initial stages of an overt conflict, but as a critical component within a broader, active hybrid confrontation that remains undeclared. In principle, the threat of A2/AD is not new, nor is the way military capabilities are used per se.[29] What is new is that advancements have substantially extended and integrated these capabilities into multidomain systems, which have shifted from a defensive to an offensive nature and extend far beyond the battlefield, ever more into society, as part of active hybrid warfare.

This means, and this is a shift, that while military assets such as tanks, HIMARS, and well-trained and equipped military forces prepared to conduct kinetic operations remain crucial for deterrence, they are no longer sufficient on their own. The effective deployment of these forces increasingly depends on non-military technologies, infrastructure, systems, and personnel, which, as demonstrated here, are vulnerable to being targeted due to the inherent weaknesses of open democratic systems societies. Consequently, military forces can no longer be regarded as shields to safeguard societal security, since such shields are inherently susceptible

to circumvention. Contemporary and active confrontation involves synchronised and integrated activities across civilian, military, and informational capabilities to actively coerce open democratic societies.

Since coercion through A2/AD capabilities effectively targets a society, the response should also begin as a social response[30] on the whole-of-society level. Addressing this societal challenge thus calls for a new response[31] based on integrated multidomain A2/AD capabilities that include non-military capabilities[32] and actors, rather than relying solely on traditional military deterrent assets. Countries, such as the Netherlands, would "benefit from a proactive, anticipatory and comprehensive approach to national security" as their "response to an acute threat is too sector-based and often focused on damage limitation"[33]. And such a whole-of-society approach is necessary sooner rather than later, as the longer that visible and 'invisible' risks of A2/AD are denied, "the harder it will be to recover" not unlike the "slow boil of the frog"[34].

Technological Advancements and Overview of the Volume

The proposed re-evaluation of A2/AD forms the core of this edited volume, which explores how to address A2/AD by shifting from a 'defence-only' perspective, via technological advancements, to a 'whole-of-society' approach, as emphasised in the subtitle. The chapters collectively illustrate how A2/AD systems are developing, how they are utilised as part of hybrid warfare strategies, and how they threaten the infrastructure and institutions that underpin open societies. They also consider how states and societies can adapt by enhancing resilience, improving situational awareness, and developing legal, technological, and organisational strategies capable of countering the coercive use of A2/AD capabilities.

This volume is organised to move from conceptual and strategic blind spots to tangible technological, operational, and legal challenges. Early contributions assess the development of A2/AD thinking and emphasise how analysis has often underestimated technological progress and its societal and hybrid aspects. Subsequent chapters explore how to counteract A2/AD as it evolves from static shields to flexible, technologically advanced hybrid warfare systems. They also examine how to overcome emerging threats such as increasingly advanced technological challenges, from hypersonic glide vehicles and drone swarms to missile systems. Additional contributions address specific domains and technological innovations, including multi-band neutralisation of drones using high-power microwave radar, the electromagnetic domain as an unseen foundation of modern A2/AD, navigation warfare targeting positioning, navigation, and timing information, and hydraulic warfare as a low-tech method of area denial in high-tech conflicts, along with the

critical condition of cyberspace and decision-making for resilient logistics in A2/AD environments.

The volume also explores the legal aspects of A2/AD technology developments, including self-defence zones in outer space under international law, and the implications of missile tests for national security and international standings. It discusses how to address A2/AD, shifting from a solely defensive, technological advancement approach to a 'Whole-of-Society' perspective, as indicated by the subtitle. Answering this question requires not only a renewed appreciation of A2/AD as a military challenge but also recognising it as a technological, strategic, and society-wide issue. More importantly, it involves bridging the gap between those who simply hope that situations will not worsen significantly and those who actively defend existing infrastructure and prepare to counter further A2/AD-enabled transgressions by adversaries.

Collectively, these chapters explain how A2/AD transforms from mainly defensive military measures aimed at neutralising more capable adversaries, into technologically advanced, integrated, multidomain systems that increasingly extend beyond the battlefield to involve the 'whole-of-society' as part of hybrid warfare. The final chapter synthesises these insights into a policy-oriented call to action for policymakers, military strategists, industry stakeholders, and civil society, emphasising the need to recalibrate existing thinking and adapt strategies and practices to better counter ongoing and future A2/AD threats. The speed and level of adversaries' technological advancement require NATO to follow suit, reviewing doctrine and practice to achieve the integrated joint level necessary to counter A2/AD.[35] This also emphasises the importance of developing capabilities for effective deterrence and intervention. Today's security landscape no longer depends solely on the quantity of tanks or missiles, but also on the effective use of technological advancements and society's ability to adapt in new ways for a different kind of war and peace: a paradigm in which A2//AD occupies an intersectional space that includes military operations, technological developments, infrastructure resilience, and the functioning of democratic institutions within the 'whole-of-society'.

Notes

1 Lasconjarias, "*How to Respond to Anti-Access*", based on Tangredi, "Anti-access Warfare: Countering A2/AD Strategies".

2 Schmidt, "Countering Anti-Access / Area Denial".

3 World Economic Forum, *Global Cybersecurity Outlook 2026*.

4 Ribeiro, "*Oslo Warns of Escalating Russian Cyber Threat*".

5 Ibid.
6 Amnesty International, *"Ukraine: Russian Attacks on Critical Energy"*.
7 Ibid.
8 International Criminal Court, *"Situation in Ukraine"*.
9 Hoffman, *Conflict in the 21st Century.*
10 Ibid.
11 Government of The Netherlands, *"Government Works to Increase Resilience"*.
12 *The Economist*, *"A Rash of Baltic Cable-Cutting"*.
13 Advisory Council on International Affairs, *Hybrid Threats and Societal Resilience*.
14 Ibid.
15 World Economic Forum, *Global Cybersecurity Outlook 2026.*
16 Ibid.
17 "Anti-access/area Denial (A2/AD)," *Wikipedia*, 2026; Lasconjarias, "How to Respond to Anti-Access/Area Denial (A2/AD)? Towards a NATO Counter-A2/AD Strategy".
18 Posen, "Command of the Commons".
19 Schmidt, "Countering Anti-Access / Area Denial".
20 Ibid.
21 Kemp, "Strategic Security in Northern Europe".
22 Schmidt, "Countering Anti-Access / Area Denial".
23 Russell, "*Strategic Anti-Access/Area Denial in Cyberspace*".
24 Ibid.
25 World Economic Forum, *Global Cybersecurity Outlook 2026.*
26 Advisory Council on International Affairs, *Hybrid Threats and Societal Resilience*.
27 Ibid.
28 Ibid.
29 Schmidt, "Countering Anti-Access / Area Denial".
30 Zeman, "Social Anti-Access/Area-Denial".
31 Ibid.
32 Sukhankin, "David vs. Goliath".
33 Advisory Council on International Affairs, *Hybrid Threats and Societal Resilience*.
34 Zeman, "Social Anti-Access/Area-Denial".
35 Schmidt, "Countering Anti-Access / Area Denial".

References

Advisory Council on International Affairs (AIV). 2024. *Hybrid Threats and Societal Resilience*. The Hague: AIV, 4 June. https://www.adviesraadinternationalevraagstukken.nl/site/binaries/site-content/collections/documents/2024/06/04/hybride-dreigingen-en-maatschappelijke-weerbaarheid/aiv-hybrid-threats-and-societal-resilience-4jun2024.pdf.

Amnesty International. 2022. *"Ukraine: Russian Attacks on Critical Energy Infrastructure Amount to War Crimes."* News release, October 20. Amnesty International. https://www.amnesty.org/en/latest/news/2022/10/ukraine-russian-attacks-on-critical-energy-infrastructure-amount-to-war-crimes/

Government of the Netherlands. 2024. *"Government Works to Increase Resilience Against Military and Hybrid Threats." Government.nl*, December 6. https://www.government.nl/latest/news/2024/12/06/government-works-to-increase-resilience-against-military-and-hybrid-threats

Hoffman, Frank G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

International Criminal Court. 2024. *"Situation in Ukraine: ICC Judges Issue Arrest Warrants Against Sergei Ivanovich Kobylash and Viktor Nikolayevich Sokolov." International Criminal Court*, March 5. https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-sergei-ivanovich-kobylash-and

Kemp, Herb. 2020. "Strategic Security in Northern Europe." *Journal of Strategic Security* 14 (1), 78–91. Published by University of South Florida Board of Trustees. Stable URL: https://www.jstor.org/stable/10.2307/26999978

Lasconjarias, Guillaume, and Alessandro Marrone. 2016. *How to Respond to Anti-Access/Area Denial (A2/AD)? Towards a NATO Counter-A2/AD Strategy*. NDC Conference Report No. 01/16. Rome: NATO Defense College, February. Accessed. https://www.ulib.sk/files/english/nato-library/collections/monographs/ndc-conference-report/crep_01_2016_a2_ad.pdf

Posen, Barry R. 2003. "Command of the Commons: The Military Foundation of U.S. Hegemony." *International Security* 28 (1), Summer 5–46. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/posen_summer_2003.pdf

Ribeiro, Anna. 2025. *"Oslo Warns of Escalating Russian Cyber Threat after Dam Breach, Citing Moscow as Biggest Risk to National Security." Industrial Cyber*, August 15. https://industrialcyber.co/industrial-cyber-attacks/oslo-warns-of-escalating-russian-cyber-threat-after-dam-breach-citing-moscow-as-biggest-risk-to-national-security/

Russell, Alison Lawlor. 2015. *"Strategic Anti-Access/Area Denial in Cyberspace."* In *Proceedings of the 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, edited by M. Maybaum, A.-M. Osula, and L. Lindström. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Art-11-Strategic-Anti-Access-Area-Denial-in-Cyberspace.pdf

Schmidt, Andreas. 2017. "Countering Anti-Access / Area Denial: Future Capability Requirements in NATO." *Journal Edition 23*, Joint Air Power Competence Centre, January 2017. https://www.japcc.org/articles/countering-anti-access-area-denial/

Sukhankin, S. 2019. "David vs. Goliath: Kaliningrad Oblast as Russia's A2/AD 'Bubble". *Scandinavian Journal of Military Studies*, 2 (1), 95–110.

Tangredi, Sam J. 2013. "Anti-access Warfare: Countering A2/AD Strategies". Naval Institute Press.

The Economist. 2026. *"A Rash of Baltic Cable-Cutting Raises Fears of Sabotage."* January 6. https://www.economist.com/europe/2026/01/06/a-rash-of-baltic-cable-cutting-raises-fears-of-sabotage

World Economic Forum. 2026. *Global Cybersecurity Outlook 2026: Insight Report*. World Economic Forum, January 12. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

Zeman, Phil. 2021. "Social Anti-Access/Area-Denial (Social A2/AD)." *Journal of Advanced Military Studies* 12 (1), 149–164. Marine Corps University Press. https://doi.org/10.21140/mcuj.20211201007