

CHACR *DIGEST* #59

AUTHOR: Professor Andrew Stewart, Head of Conflict Research



The views expressed in this Digest are not those of the British Army or UK Government. This document cannot be reproduced or used in part or whole without the permission of the CHACR. chacr.org.uk

In Europe, the threat of limited Russian territorial land-grabs between 2026 and 2029 highlights NATO's urgency. Russia's grey-zone campaign complicates collective defence. To adapt, front-line states are restructuring: Estonia is redirecting its armour budget into a comprehensive unmanned ecosystem, while Poland combines its 'East Shield' with low-cost, artificial intelligence-enabled networks under the Eastern Flank Deterrence Initiative. These moves counter Russia's long-term attrition strategy, which seeks to endure decades-long Western confrontation. Globally, concerns continue about receding American hegemony, prompting massive regional realignments across Asia and the Middle East. Facing an ongoing 'irregular world war', there are calls for the US to adopt a whole-of-society 'total defence' model to secure fragile domestic power grids and rebuild civil defence. There is also an argument for Taiwan to replace short-term rotational US advisers with a permanent, stay-behind advisory cadre to prepare for prolonged, asymmetric resistance. There are also warnings of severe, low-visibility fragilities in Western munitions, specifically the unscalable chemical precursors and single-point production sites for explosives like RDX. Concerns are also growing about 'electrotech' – the hardware and software driving the digital grid – and the need to secure against Chinese dominance. Finally, it is being argued that AI-driven 'Cognitive Operational Networks' must serve, not replace, human judgement and decentralised mission command to overcome the "last mile of command".

EUROPE

Newsweek has published a report based on US intelligence which [warns Russia could launch a 'limited' or hybrid attack on NATO territory](#) between autumn 2026 and 2029. This critical threat emerges before many European allies can fully rearm their domestic militaries, and amid deep concerns that American commitment to defending Eastern Europe might fracture under Trump's administration. Instead of a large-scale invasion, analysts anticipate a small-scale land-grab in Poland, the Baltic states or the strategic Suwałki Gap. Using specialised electronic warfare and advanced air defences to secure seized territory, Moscow would aim to test NATO's political resolve rather than trigger an overwhelming military retaliation. A realistic simulated Lithuanian wargame demonstrated that, with just small forces, Russia could successfully seize territory if NATO allies dither or fail to invoke Article 5. Simultaneously, Russia is already conducting aggressive hybrid attacks. These escalating grey-zone tactics include persistent cyberattacks, damaging Baltic Sea undersea cables, plotting cargo plane arson and planting explosive devices at major logistics hubs like Germany's Leipzig airport. Although Moscow dismisses these threats as "nonsense", Russia has begun constructing dozens of military facilities near the Finnish border. Meanwhile, NATO is actively wargaming Baltic defences and prioritising resilience against escalating grey-zone campaigns.

Russian hybrid warfare is the subject of a [report](#) produced for the US Congressional Research Service, which details Russia's escalating campaign of hybrid warfare across Europe following its 2022 invasion of Ukraine. It describes this as a multi-domain strategy employing asymmetric tactics below the threshold of armed conflict, including sabotage, assassinations, cyberattacks, GPS jamming, airspace violations and weaponised migration. This has been done to undermine European support for Ukraine and fracture transatlantic unity. To conduct these brazen, kinetic operations, Russia's intelligence agencies (SVR, FSB and particularly the

military GRU) have increasingly relied on contracted, low-level proxies, saboteurs and criminal networks. This adaptive, outsourced approach compensates for the expulsion of more than 750 Russian diplomatic officers across Europe. Russia's activities heavily target NATO's eastern flank. Poland and the Baltics face election interference, arson, railway sabotage and parcel bomb plots designed to cause public panic. Additionally, critical undersea telecommunication and power cables in the Baltic Sea have been severed by commercial ships linked to Russia. Romania and Bulgaria experience constant Black Sea GPS jamming and frequent airspace incursions by weaponised drones. The report notes that the US is considering responses, such as the SHADOW Act, and debating whether a mix of domestic law enforcement, coordinated intelligence or conventional military strategies is most effective to safeguard vital US and European national security interests.

Following the recent confirmation that [the UK is expanding its Estonia-based forces](#) to 1,200 troops and transitioning to a highly mobile Mobile Anti-Armour Force, Baltic security has been [analysed](#) by Reuben Stewart. The IISS senior researcher discusses Russia's anti-access/area denial (A2/AD) capabilities, which operate across two mutually reinforcing dimensions. As he explains, the first of these, the A2 measures, block NATO reinforcement. At sea, Russia utilises mines, submarines and long-range missiles to disrupt shipping lines while, on land, the 65-kilometre Suwałki Corridor is heavily exposed to Kaliningrad and hostile Belarus. Second, AD constrains forces already inside the Baltics. Pervasive Russian surveillance makes troop concentration highly dangerous, leaving assembly areas and logistics hubs vulnerable to precision strikes. The writer notes that, since 56 per cent of Baltic territory lies within 100 kilometres of Russia or Belarus, movement is highly restricted. He concludes that, because Russia's dispersed, mobile network of sensors and launchers can rapidly reconstitute after losses, NATO cannot rely on a single, decisive opening knock-out blow. Instead, it must treat regional movement as a continuous campaign, focusing on securing temporary windows of local superiority and maintaining logistical throughput, even if forced to route military supplies through austere, low-profile alternatives.



A British soldier watches his AR3 Evolution reconnaissance drone come in for landing during this year's Spring Storm – the largest annual exercise of the Estonian Defence Forces.

Writing for *The Jerusalem Post*, Dr Doron Feldman details [Estonia's military revolution](#) as it redirects its €500 million armoured vehicle budget into advanced drones and air defence systems. Facing severe manpower constraints with only 7,000 active soldiers, its Unmanned Vehicles Roadmap (2026-2030) coordinates government, industry and academic drone development. With a comprehensive, border-wide counter-drone surveillance system being deployed, and peacetime drone interception permitted, a strategic agreement with Ukraine enables joint local manufacturing of battle-tested defence tech. By building this high-tech unmanned ecosystem, the author argues that Estonia is proactively addressing its geographic vulnerabilities, countering Russian hybrid threats and strengthening NATO's regional deterrence.

A report in *Defense News* outlines [Poland's dual military initiatives to strengthen European border defence and security](#). First, Poland will host the inaugural joint military drills for the 'Coalition of the Willing', the informal French and British-led alliance formed to prepare security guarantees for post-war Ukraine by testing command, control and logistical interoperability. Second, Poland is advancing its 10 billion zloty (\$2.6 billion) 'East Shield' initiative to construct diversified, modern defensive fortifications along its entire 800-kilometre border with Kaliningrad and Belarus, incorporating advanced anti-drone systems with immediate operational support from rotational German, French, Baltic and Nordic and American troops. Andrew A. Michta has explained [the value of the Eastern Flank Deterrence Initiative](#) (EFDI), a land-warfare concept established in late 2024 to protect NATO's Northeast Corridor. Developed by USAREUR-AF and LANDCOM, the EFDI integrates unmanned systems, AI-enabled networks and low-cost capabilities to counter Russian mass and momentum on transparent battlefields. It shifts the cost curve – avoiding expensive interceptors against cheap drones – and preserves human combat power. Crucially, the initiative supports Washington's push for transatlantic burden-sharing, offering a credible defence strategy that lowers security costs while utilising regional allies and essential US strategic enablers.

A number of reports have focussed on current Russian strategic thinking and its potential implications for European security. *Northern Defence Affairs* has published an analysis of [the strategic blueprint of Andrei Bezrukov](#). Authored by an influential member of Russia's security establishment, this outlines a prolonged, multi-domain confrontation with the West expected to last for decades. Bezrukov posits that because decisive battlefield victories are no longer attainable with mass armies, conflict has shifted to a permanent war of attrition to determine who can outlast the opponent. Rather than advocating for direct military escalation or an invasion of NATO territory, he proposes a dual strategy centred on conventional deterrence and domestic endurance. Modern conflict, in his view, is waged continuously across cyber, financial and diplomatic domains, aiming to destabilise the adversary by eroding their resource base. First, Bezrukov argues that Russia's nuclear weapons are effectively unusable against the West's low-intensity campaign of 'slowly boiling the frog' through sub-threshold proxy pressure and sabotage. Consequently, he argued Russia must establish a conventional deterrent by holding high-priority Western assets, such as gas carriers, terminals, satellite constellations and financial data centres, at risk of long-range strikes. Second, Russia must transform into a hardened "warring society". This requires dispersing critical infrastructure, adopting domestic secure-by-design systems and decentralising command to local leaders while maintaining a central coordinating body. He also demands extensive intelligence reforms, including fusing multi-source data streams and building a dense domestic informant network. He believes that in an era of demographic decline, human capital like scientists and decision-makers must be protected as finite, high-value assets. The analysis concludes by arguing this strategic vision has severe vulnerabilities. Its success relies entirely on the belief that the West is in irreversible decline. Moreover, the demand for mutual trust and decentralised initiative is fundamentally undermined by Bezrukov's call for pervasive domestic surveillance, which breeds paranoia and mutual suspicion. Lastly, expecting unconsulted citizens and entrenched elites to willingly sustain a "warring society" for decades remains highly unrealistic.

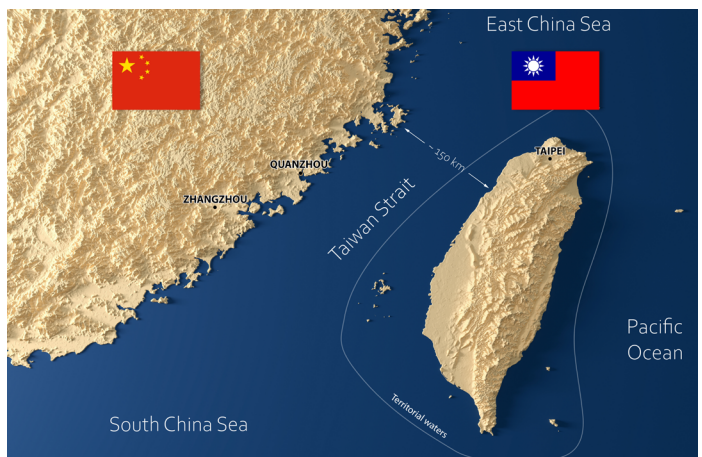
THE AMERICAS

Andrew C. Kuchins, and Fenna de Vos, writing in [The National Interest](#), examine how leading Russian foreign policy analysts, including Fyodor Lukyanov, Dmitri Trenin and Ivan Timofeev, have interpreted the February US and Israeli military strikes against Iran. They conclude that the conflict has not altered Russian strategic thinking, but has instead reinforced four deeply held narratives and anxieties. First, it highlights the decay of international norms, demonstrating that military power has displaced international law. Unlike past interventions in Serbia, Iraq or Libya, the strikes against Iran occurred without any UN mandate or legal justification, signalling a dangerous return to a 19th-century 'might makes right' paradigm. Second, the conflict strengthens Moscow's belief that Western pressure is forging a more cohesive network of strategic partners. Third, it bolsters the perception that the Western alliance lacks political unity. Fourth, the war exacerbates acute anxieties over Russian regime security. Analysts highlight the dangerous precedent of the direct external elimination of leaders, such as the assassination of Ali Khamenei. Unlike the domestic trials or internal collapses that ended Saddam Hussein's and Muammar Gaddafi's regimes, the strike on Iran represents the normalised, direct targeted killing of a head of state by external military force. Ultimately, this makes Western policy even more unpredictable, fuelling Putin's fears that Russia could be next.

An essay in *Engelsberg Ideas* has argued [the US is at risk of losing an ongoing 'irregular world war'](#) waged in the grey zone by adversaries Russia, China and Iran. Because conventional US military power remains superior, these rivals increasingly deploy asymmetric hybrid warfare. This includes cyberattacks on water municipalities and power grids, Russian sabotage campaigns in Europe and Chinese cyber-operations. To defend against these high-frequency, low-risk threats, the authors urge Washington to abandon its passive stance and adopt a whole-of-society 'total defence' model. They propose three essential steps to build resilience. The first is to harden domestic infrastructure, which will require addressing a \$3.7 trillion infrastructure funding gap and rebuilding virtually non-existent civil defence programmes. International partnerships also need to be bolstered and cooperating with and reinforcing key allies using successful initiatives like US Cyber Command's proactive 'hunt forward' cybersecurity operations. Finally, lessons from experts need to be learned and integrated, such as emulating Finland's national civil preparedness training and Sweden's scalable civil defence templates. The author concludes the US must prioritise resilience and invest in security at home before another major hybrid attack exploits domestic vulnerabilities.

INDO-PACIFIC

A recent analysis in the [Modern War Institute](#) noted: "The global security environment is reshaping, forcing military planners to contend with the prospects of large-scale conflict. That has led to significant debate regarding the future of US Army Special Forces and their role in such a conflict." Former US Army Special Forces officer [Brian Petit](#), writing for *War on the Rocks*, argues the US must overhaul its military advising model for Taiwan by replacing short-term rotational teams with a small, permanent advisory cadre. The author warns that the current rotational approach is poorly suited to the deep institutional, linguistic and political preparation Taiwan needs to survive an amphibious invasion across the Taiwan Strait. To resolve this, he proposes 'Detachment Taiwan', a model based on the Berlin Cold War-era Detachment A. From 1956 to 1990, 'Det A' maintained under 100 plain-clothed Special Forces operators who lived in the city. Designed as an unconventional and highly sensitive stay-behind force, their mission was to prepare anti-communist resistance networks, conduct sabotage and slow any Soviet advance behind enemy lines. Applying this model to Taiwan would yield several critical benefits. Rather than matching Chinese military mass, it complicates Beijing's plans by presenting a dedicated detachment prepared to wage a prolonged, costly campaign and demonstrating that an invasion would not end on the beaches. Permanent advisers can also better impact deep strategic planning about the transition to urban and rural fighting and whole-of-society defence. The author concludes that small-scale advisory efforts have historically achieved outsized success and the proposed Detachment Taiwan offers a low-cost, high-impact strategic move that hardens defence while respecting critical escalation boundaries.



[Australia's 2026 National Defence Strategy](#), published earlier this year, emphasises a strategy of denial to hold adversaries at risk from a distance. It was reported as balancing self-reliance with reliance on US technology and intelligence, with long-range strikes and semi-autonomous systems prioritised. Writing for the Australian think-tank ASPI, Carl Janz examines in more detail [the country's strategic posture](#) during what is described as a global 'interregnum', a period between international orders where US hegemony has receded and competing great powers vie to shape the emerging global order. He argues that, while recent military-technological advancements like drones, AI and real-time satellite surveillance currently favour the defender and temporarily hinder rapid territorial conquest, history warns this tactical advantage will not last forever and further technological developments could once again alter strategic calculations. As a democratic middle power with limited influence over great power competition, the author argues Australia must navigate this instability by prioritising 'self-reliance', the cornerstone of its National Defence Strategy. This at the same time as [actively deepening](#) defence relationships with Britain, Germany, France and, even, Finland. With concerns that defence policy suffers from a dangerous [strategic imbalance](#), prioritising high-intensity conventional warfare over crucial peacekeeping, while a US\$30 million US Marine Corps war reserve stockpile in the country's south-east creates a severe [logistical bottleneck](#) with incomplete rail networks and vulnerable civilian transport corridors, the conclusion is that Australia must strengthen its sovereign capabilities and pragmatically prepare for the unknown.

With [Iranian warnings](#) that American military installations in Europe, such as Bezmer Air Base in Bulgaria, could face retaliatory strikes if the United States escalates the war, [Ved Shinde](#), writing in *Engelsberg Ideas*, analyses a major geopolitical shift in the Greater Middle East. This is marked by the emergence of two competing strategic alliances linking the Aegean Sea to the Indian subcontinent. The first is the 'Mecca Joint Defence Agreement', a new pact between Turkey, Saudi Arabia and Pakistan. Signed under the banner of Islamic solidarity, this NATO Article 5-style mutual defence pact signals that regional players are prepared to defend their own interests amid perceived US security ambivalence. For Turkey, the alliance serves as a shield against Israel and supports its naval expansion into the Indian Ocean. For Pakistan, it offers international status amidst economic turbulence. For Saudi Arabia, it represents a strategic reconciliation with Turkey, driven by mutual concerns over Iran and Israel, despite historic rivalry and past diplomatic spats. The second is the informal 'Indo-Abrahamic' coalition consisting of the UAE, Israel and India. With American backing, this pragmatic alliance is united by moderation, religious toleration and opposition to radical Islamist movements. It has fostered unprecedented cooperation, such as Israel deploying Iron Dome and Iron Beam air defences on Emirati soil and India deepening critical military partnerships with Israel. While historic divisions persist (such as the dissolution of the Baghdad Pact in 1979) these competing axes demonstrate Southwest Asia's rising strategic integration. Security in the Middle East has become deeply intertwined with the Indian subcontinent, leaving regional players hedging while the US remains Israel's ultimate security guarantor.

DEFENCE

Harry Krejsa and Phoebe Benich argue in *War on the Rocks* that '[electrotech](#)' – the hardware and software that digitally generates, stores and directs electricity – has become the master metric of modern military power. From battery-powered autonomous drones in Ukraine to AI-driven cyber operations that guzzle massive wattage, the modern battlefield and home front have converged on electricity. However, America's chief strategic competitor, China, dominates the global electrotech stack. By leveraging its robust consumer electronics base (such as smartphones and electric vehicles), Beijing has rapidly accelerated its military 'intelligitization'. In contrast, Washington is fumbling its response due to cultural and political friction. While the Pentagon scrambles to secure defence supply chains, US policymakers have systematically undermined the domestic transition by gutting civilian clean energy initiatives, like electric vehicle tax credits. Historically, military deterrence requires massive civilian industrial scale, such as Detroit's car manufacturers who served as the crucial 'Arsenal of Democracy' during the Second World War. To build a resilient American 'arsenal of electricity' and secure critical digital control layers against Chinese cyber-sabotage, the authors explicitly call for an urgent alliance between 'war hawks' and 'climate hawks'. This requires integrating national defence priorities with clean energy innovation to scale domestic manufacturing and secure America's fragile power grid.

Morgan Bazilian and Matt Isler, writing for the Modern War Institute, detail the [low-visibility frailties in the United States' munitions industrial base](#), using the standard military explosive RDX to illustrate severe supply chain vulnerabilities. Since 1941, the Holston Ordnance Works in Kingsport, Tennessee has remained the sole domestic producer of RDX. Two active global conflicts have heavily depleted stockpiles, straining this single site. Furthermore, critical chemical precursors like hexamine, nitric acid and acetic anhydride face major supply constraints and tight international export controls, with basic chemical manufacturing increasingly shifted to China. The munitions shortage extends beyond explosives. The US Army's attempt to scale 155mm artillery shell production has fumbled, producing just 36,000 rounds monthly against a target of 100,000, primarily due to manufacturing delays at a new plant in Mesquite, Texas. Additionally, the US has lacked a domestic TNT producer for decades, relying on allies like Poland's Nitro-Chem, while Russia has aggressively expanded its own drone-safe RDX capacity in Siberia. Ultimately, the authors warn that vital wartime operational endurance depends less on how many weapons the military can afford and more on securing the fragile, unscalable chemical supply chains and single-point production sites that underpin all modern ordnance.





FUTURES

According to an article in *The Jerusalem Post*, [artificial intelligence is not replacing human commanders but is fundamentally changing how they think](#), decide and fight by redefining the division of labour between humans and machines. The source identifies two complementary, ongoing AI revolutions that are unfolding simultaneously. First, inside command headquarters, AI provides critical cognitive augmentation. It reduces cognitive overload for staff by continuously filtering, correlating and fusing immense, multi-domain data flows from hundreds of sensors into a near-real-time common operational picture. This dramatically compresses early OODA [observe, orient, decide, act] loop stages, freeing commanders to focus on uniquely human tasks like understanding operational context, managing uncertainty and exercising professional military judgement. Second, at the tactical edge, AI supports autonomous execution under human command. In high-tempo, communication-denied operational environments where decision windows are measured in seconds, AI enables unmanned systems to navigate independently, fuse tactical sensors, identify targets and employ combat power autonomously: it enables the commander's strategic intent to be executed at speed. Ultimately, these two revolutions are converging into a single, comprehensive 'Cognitive Operational Network'. Rather than maintaining a traditional, rigid hierarchy, this integrated ecosystem seamlessly links humans, intelligent machines and sensors together, making any future military battlefield advantage entirely dependent on how effectively they think, learn and fight together.

Roger N. McDermott, writing for the West Point Modern War Institute, argues that despite the unprecedented transparency and lethality of modern drone-filled battlefields like Ukraine, [technological modernisation has not solved the fundamental human challenge of military command](#). Drawing on the insights of Russian military theorist Aleksandr Svechin, the author highlights the "last mile of command", the immense operational distance between a written headquarters directive and its physical execution by exhausted, real-world troops. While contemporary digital sensors can populate a common operational picture with blue icons, they fail to capture critical human factors, such as commander fatigue, troop morale, unit trust or electronic warfare protection. This mismatch often creates a dangerous "illusion of control", tempting senior headquarters into technologically-enabled micromanagement of tactical decisions from afar. Ultimately, the source asserts that true battlefield decision advantage requires decentralised command. This model must rely on competent, trusted subordinate commanders who can interpret commanders' intent and act independently when communication networks are degraded. Modernisation must serve human judgement and initiative rather than trapping commands in bureaucratic, rigid, data-heavy systems. The conclusion is that an army can become highly skilled at employing drones while remaining structurally weak at command, and simply accumulating vast quantities of raw battlefield data does not automatically achieve a real decision advantage.