ITC SECURE
Part of Collective Defence

Microsoft
Solutions Partner

itcsecure.com

WHITE PAPER

Converging Defences

A Framework for Integrated National Resilience Across Cyber Security, Counter-Drone and Anti-Missile Strategy

May 2026

Contents

Executive Summary

The conflicts of the past four years have dismantled a foundational assumption of Western defence planning: that the physical and digital battlespace are distinct domains, to be addressed by separate organisations, budgets, and doctrines. They are not. From the drone corridors above Kherson to the layered missile salvoes directed at Tel Aviv and Riyadh, adversaries are deliberately exploiting the seams between cyber security, uncrewed aerial systems (UAS), and ballistic and cruise missile threats. National resilience, in this environment, requires convergence.

This paper sets out the strategic case for treating cyber, counter-drone, and anti-missile capabilities as an integrated defence architecture rather than parallel programmes. It draws on operational evidence from the Russia-Ukraine conflict and the 2024-2026 confrontations between Iran and the US-Israeli coalition, identifies the critical vulnerabilities exposed at the intersections of these domains, and proposes a framework through which governments, NATO member states, and critical infrastructure operators can begin to close those gaps.

~14,000	**~$1B+**
Drone and missile strikes recorded against Ukraine in 2024 (CSIS / EuroMaidan Press)	Estimated coalition cost of defending the April 2024 Iranian salvo (Bloomberg / Reuters)

1 The End of Siloed Defence

For much of the post-Cold War period, Western defence establishments organised themselves around a clear separation of disciplines. Cyber security sat within signals and intelligence communities; missile defence was the preserve of tier-one military hardware programmes; counter-drone capability barely existed as a formal category before 2014. Each discipline developed its own industrial base, its own classified channels, and its own institutional culture.

This architecture made logical sense in a world where sophisticated adversaries were few and the pace of technological diffusion was slow. That world no longer exists. The democratisation of drone technology, the proliferation of precision munitions, and the integration of cyber operations into kinetic campaigns have created an environment in which the three threat vectors are not only simultaneous but mutually reinforcing.

> *"The electromagnetic spectrum is now a battlefield. Jamming a Starlink terminal, spoofing a drone's GPS signal, and launching a cruise missile at a power substation are not separate events; they are acts in the same operational sequence."*

A drone swarm tasked with saturating an air defence radar array is itself a cyber delivery mechanism; its navigation can be hijacked, its command link intercepted, and its target data manipulated. A ballistic missile arriving over a defended perimeter may be preceded by a cyber intrusion that quietly degrades the intercept calculation. And a cyber attack on a power grid does not merely inconvenience a population; it can suppress the cooling systems for a Patriot battery, the fuel logistics for a rapid reaction force, or the communications backbone that coordinates all three responses.

The implication is uncomfortable but unavoidable: a defence posture that excels in any one of these domains while remaining vulnerable in the others is, at the strategic level, a posture that has already lost.

2 Lessons from the Battlespace

2.1 Russia-Ukraine: The World's First Hybrid Air-Cyber Campaign

Ukraine has served as an unintentional but invaluable live-fire laboratory for the integrated threat. Russian forces have deployed a doctrine of deliberate domain blending that reflects a coherent, if brutal, strategic logic.

Since the full-scale invasion of February 2022, Russia has launched over 14,000 recorded drone and missile strikes against Ukraine in 2024 alone - comprising approximately 11,162 drones and 3,063 missiles - with a particular focus on energy generation and distribution. These strikes are rarely unaccompanied. Sandworm,

the GRU-affiliated threat actor, and related groups have maintained persistent access to Ukrainian energy, telecommunications, and railway networks throughout the conflict. The operational pattern is consistent: cyber intrusions pre-position access and degrade situational awareness; kinetic strikes then exploit reduced response capability.

The October 2022 attack on Ukrainian power infrastructure illustrates the model precisely. A coordinated wave of Iranian-supplied Shahed-136 drones and Kalibr cruise missiles led Ukraine's energy minister to report that approximately 30% of the country's energy infrastructure had been attacked in a single day. Subsequent analysis confirmed that cyber intrusions into grid management systems had been active for weeks prior, positioning adversary actors to observe and potentially manipulate the restoration process.

Key finding: Ukrainian defenders who integrated cyber threat intelligence feeds into their air defence command and control were demonstrably faster to reacquire targets after electronic warfare interference. Domain fusion is not a theoretical benefit; it is a measurable operational advantage.

2.2 The US-Israeli-Iran Dimension: Layered Threats, Layered Failures

The April 2024 Iranian strike on Israeli territory - the first direct state-on-state attack in decades - presented a different tactical picture but confirmed the same strategic pattern. Iran launched a combined salvo of over 300 projectiles, comprising ballistic missiles, cruise missiles, and Shahed drones. The multi-vector composition was not accidental; it was designed to stress-test the layered defence architecture of Israel and its coalition partners.

The overall intercept rate across all projectile types exceeded 99%, as reported by the IDF, and was widely reported as a success. It was. But the cost and the conditions deserve closer scrutiny. The interception required the simultaneous activation of Israeli Arrow, David's Sling, and Iron Dome batteries, US Navy destroyers, Jordanian air defences, and a coalition-wide intelligence and early warning network. The financial cost of the intercept operation was estimated at approximately $1 billion by Bloomberg and Reuters analysts - against an Iranian attack estimated to have cost a fraction of that figure.

The subsequent Iranian escalation in October 2024, the June 2025 Twelve-Day War (Operation Rising Lion / True Promise III), and the US strikes on Iranian nuclear facilities (Operation Midnight Hammer, June 2025) culminated in the US and Israel launching Operation Epic Fury on 28 February 2026 - the most significant US military action in the Middle East since the Iraq War. Throughout this escalatory arc, Iran's strategy consistently incorporated cyber operations as a precursor and enabler. Attacks attributed to Iranian state actors (including APT33, APT34, and affiliated groups) targeted US and Gulf state defence contractor networks in the months prior to each physical escalation, seeking targeting data, logistics timelines, and system vulnerabilities.

300+	**99%+**
Projectiles launched in April 2024 Iranian strike on Israel (IDF)	Percentage of all incoming projectiles intercepted by the coalition (IDF)

The lesson is not that layered missile defence is ineffective. It demonstrably works. The lesson is that it works only under conditions of complete integration: shared intelligence, unified command architectures, and cyber security hardening of every node in the kill chain. Remove any of those conditions and the mathematics of a massed salvo begin to favour the attacker.

3 The Convergence Gap: Where Nations Remain Exposed

Despite the clarity of the operational evidence, most national defence architectures continue to treat cyber security, counter-drone, and missile defence as functionally separate programmes. The consequences of this gap are predictable and already visible.

3.1 Command and Control Fragmentation

The organisations responsible for cyber defence, air traffic security, and missile intercept typically report to different ministerial structures, operate on different classification levels, and consume different intelligence streams. In a time-critical scenario; a coordinated drone and cyber attack on a major port or energy hub; the latency introduced by inter-departmental coordination can be decisive. The 2022 attack on Viasat's KA-SAT network, which degraded Ukrainian military communications at the precise moment of the invasion,

demonstrated how a single cyber action can suppress the command-and-control layer that all other defences depend upon.

3.2 Electronic Warfare as the Pivot Domain

Counter-drone systems depend heavily on radio frequency (RF) detection, jamming, and spoofing capabilities. So do many of the communications and data-link architectures that underpin both missile defence and cyber security monitoring. This creates a fundamental tension: the electromagnetic environment in which you conduct counter-drone operations is the same environment through which your cyber security sensors and early warning data flows. Adversaries who understand this - and Russia, Iran, China, and North Korea all demonstrably do - will prioritise EW disruption precisely because it degrades all three defensive domains simultaneously.

3.3 Critical Infrastructure as the Soft Target

The single most consistent finding across both conflicts is that civilian critical infrastructure, energy grids, water treatment, telecommunications, and transport logistics, is the preferred target for integrated attack. This is rational adversary behaviour: infrastructure is harder to defend than military assets, its destruction creates cascading political and economic effects, and it is overwhelmingly operated by private sector entities whose cyber security postures were not designed with nation-state threat actors in mind.

National resilience cannot be built on the assumption that critical infrastructure operators will self-organise their defence. The threat they face is state-grade. The response must be state-coordinated.

4 A Framework for Integrated National Resilience

Closing the convergence gap does not require the abolition of existing organisational structures. It requires the deliberate construction of integration mechanisms at each level of the defence architecture. The following framework reflects emerging best practice across NATO member states and draws on lessons from the conflicts examined above.

4.1 Unified Threat Intelligence Architecture

The first requirement is a common operating picture that spans all three domains. Threat intelligence relevant to counter-drone operations (RF signatures, drone manufacturer supply chains, operator TTPs) must flow into the same analytical environment as cyber threat intelligence and missile early warning data. This is technically achievable today; it is organisationally and politically challenging. National cyber security agencies, defence intelligence organisations, and military air defence commands must operate with shared taxonomies, shared data standards, and - where classification permits - shared analysis platforms.

4.2 Hardened Kill Chains

Every node in a counter-drone or missile defence kill chain is a potential cyber target. Radar systems, intercept command systems, logistics platforms, and communications networks must be assessed not merely for their primary military functionality, but for their cyber security exposure. The integration of offensive cyber threat modelling into the certification process for air defence systems is not a complexity addition; it is a baseline requirement for systems that will be targeted by adversaries who have already demonstrated this capability.

4.3 Critical Infrastructure Resilience Partnerships

Governments cannot defend national infrastructure without the active participation of the private sector entities that operate it. This requires more than information-sharing frameworks; it requires the extension of state-grade threat intelligence and defensive capability to operators of designated critical infrastructure. Utilities, telecommunications providers, port operators, and financial institutions should be treated as forward elements of the national defence perimeter, with corresponding access to threat intelligence, incident response support, and resilience planning assistance.

4.4 Doctrine, Exercises, and Red Teaming

Convergence must be exercised, not merely planned. National resilience exercises that test only cyber incident

response, or only military air defence, without integrating the other domains, will produce plans that fail at the first moment of genuine convergence. Red team exercises that simulate coordinated cyber-drone-missile scenarios - of the type now routinely used by adversary planners - are an essential tool for exposing the gaps that doctrine documents cannot anticipate.

5 The Path Forward

The strategic case for convergence is settled. The operational evidence from Ukraine and the Middle East removes reasonable doubt that adversaries are already fighting in the integrated domain. The question is not whether national defence architectures must adapt, but at what pace, and at what cost.

There are encouraging signals. NATO's adoption of its integrated air and missile defence (IAMD) framework, the establishment of dedicated cyber-physical threat units in several member states, and the growing maturity of the commercial counter-UAS sector all represent meaningful progress. The legislative frameworks around critical infrastructure protection - the EU's NIS2 Directive, the UK's forthcoming Cyber Security and Resilience Bill, and US CISA's cross-sector coordination mandate - create the regulatory foundation for deeper public-private integration.

What is needed now is the organisations and expertise capable of operating at the seams; entities that understand the cyber domain, the physical threat domain, and the intelligence architecture that must connect them. This is not a problem that any single government department, defence prime contractor, or cyber security vendor can solve in isolation. It demands a genuinely converged approach, from strategy through to operational delivery.

The nations that build converged defence architectures now will not merely be better protected. They will define the standards, the doctrines, and the industrial partnerships that shape collective security for the next generation.

Conclusion

The convergence of cyber security, counter-drone operations, and anti-missile strategy is no longer a speculative future requirement. It is the present reality of the threat environment, demonstrated in blood and infrastructure damage across two of the most consequential conflicts of the modern era.

Governments, NATO institutions, and critical infrastructure operators that continue to organise their defences in silos are not merely inefficient; they are offering adversaries a predictable and exploitable advantage. The framework outlined in this paper does not require the invention of new capabilities. It requires the integration of existing ones, supported by the political will, the organisational design, and the cross-domain expertise to make convergence operational rather than aspirational.

Collective Defence was established at the intersection of these challenges. Our work brings together deep expertise in cyber security operations, intelligence analysis, and the emerging counter-UAS and physical threat landscape. We are committed to working with governments, alliances, and private sector partners to build the integrated resilience architectures that this moment demands.