

Asymmetric Warfare Evolution: The New Threats for Global Security

Asymmetric warfare represents not a sideshow to “real” war but its new paradigm. It challenges states to adapt or risk irrelevance in an era where adversaries win not through brute strength but through subtlety, disruption, and systemic exploitation. The nations that succeed will be those capable of building resilience, integrating across domains, and embracing innovation—not only to deter asymmetric threats but to survive and prevail in the conflicts of the future.

Dr Gustavo Scotti di Uccio¹

Redefining the Threat



Asymmetric warfare is not a marginal or inferior form of conflict; rather, it constitutes the very **core logic of contemporary strategic competition**. To dismiss or underestimate it is to prepare for the wars of yesterday, virtually guaranteeing defeat in those of tomorrow. Unlike conventional battles, where victory is measured by firepower and troop numbers, asymmetric warfare thrives on exploiting

weaknesses, undermining cohesion, and leveraging innovation in unpredictable ways.

The age of conventional conflicts, traditionally decided by numerical superiority and technological dominance on the battlefield, is steadily waning. Both **state and non-state actors** now exploit asymmetry as their central operational philosophy to challenge established powers, expanding their influence into domains ranging from cyberspace to economic warfare. For the defence and security communities, understanding and countering these strategies is no longer optional but a **strategic imperative essential to national survival**.

Today's strategic environment is shaped by **persistent volatility and unpredictability**, in which the once-clear distinctions between peace, crisis, and war have blurred into a continuous spectrum of confrontation. In this fluid environment, adversaries who recognise their conventional inferiority increasingly seek disproportionate advantages through asymmetric means. The principal aim is no longer the physical destruction of opposing armed forces (annihilation), but instead the **paralysis of decision-making processes** and the **erosion of national unity** (attrition).

¹ *Gustavo Scotti di Uccio, Ph.D., was an executive in the Finmeccanica/Leonardo group for over 30 years, working in the fields of defence, security, and critical infrastructures. For the past 15 years, he has been the President and General Manager of AOS (Atlantic Organization for Security), a security and defence engineering & program management firm based in Belgium.*

This shift in strategy weaponises the **very pillars of modern society**. Democratic openness, technological dependence, and deeply interconnected global economies are transformed into exploitable vulnerabilities. What once served as strengths—interconnected supply chains, reliance on information systems, and international economic integration—now represent points of systemic fragility that adversaries can deliberately target.

Domains of Asymmetric Conflict

Asymmetric confrontation rarely unfolds in a single theatre. Instead, it develops **across multiple operational domains, often simultaneously**, in a method now commonly termed **Hybrid Warfare**. Its effectiveness lies in combining conventional tactics with irregular, cyber, and economic measures, creating layers of complexity that overwhelm traditional defensive approaches.

- **From the Physical Battlefield to Territorial Control:** While guerrilla and insurgency tactics remain relevant, they are being reshaped through the integration of technology. Non-state actors such as the Houthis in the Red Sea have demonstrated how low-cost technologies—drones, improvised explosive devices, and anti-ship missiles—can create effective A2/AD (Anti-Access/Area Denial) zones. These tactics threaten global maritime supply routes, impose economic costs on international trade, and directly challenge even the most advanced naval powers. The lesson is clear: with ingenuity and minimal investment, smaller actors can impose **unsustainable costs on superior forces**.
- **The Cyber and Information Domains:** Cyberspace has emerged as the preferred battleground for asymmetric confrontation. Offensive cyber operations aim not only to **steal sensitive data** but also to **disrupt and disable critical infrastructure**, including energy grids, logistics networks, and financial systems. Beyond physical sabotage, adversaries employ influence campaigns to exploit social divisions,

spread disinformation, and undermine trust in public institutions. These operations erode national resilience by paralysing political decision-making and weakening societal cohesion. For militaries, the degradation of **C5ISTAR** (Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Target Acquisition, and Reconnaissance) capabilities through cyberattacks represents a direct threat to operational effectiveness.

Hybrid adversaries succeed not by confronting strength with strength, but by **turning strengths into liabilities**, striking where societies are least prepared to defend themselves.

EMP Threat: The Systemic Knockout Option

Among the spectrum of asymmetric threats, the **Electromagnetic Pulse (EMP)** stands out as a high-impact but low-probability event, representing the pinnacle of asymmetric thinking. Unlike cyberattacks, which unfold invisibly over time, or conventional military strikes, which rely on physical destruction, an EMP attack is designed to **disable the technological backbone of modern civilisation in an instant**.

A single nuclear device detonated at high altitude (HEMP – High-Altitude ElectroMagnetic Pulse) or a high-powered non-nuclear device (NNEMP) could generate a vast, destructive electromagnetic field. Unlike conventional or nuclear strikes, an EMP event is not primarily intended to cause direct casualties. Its true objective is the **systemic collapse of the “nation-system.”**

Catastrophic Strategic Consequences

The impact of an EMP attack would be immediate and devastating:

- **Decapitation of Command and Control (C2):** Civilian and military C5ISTAR networks would be paralysed, leaving armed forces unable to coordinate operations. Modern doctrines of network-

centric warfare would collapse within minutes.

- **Paralysis of Critical Infrastructure:** Power grids, telecommunications, transport systems, and supply chains would fail simultaneously. The financial system, reliant on digital infrastructure, would cease to function, leading to cascading economic collapse.
- **Neutralisation of Technological Advantage:** Nations that rely heavily on advanced technologies would see their superiority instantly erased. Conflict would regress to a primitive level where success would depend not on technological edge but on **societal resilience, adaptability, and endurance under degraded conditions.**

An EMP strike epitomises the **asymmetry of modern conflict:** a single, potentially unattributable act capable of disabling an adversary without invasion, prolonged warfare, or even large-scale conventional forces.

Geoeconomics

Beyond the battlefield, **economic power has become a central instrument of asymmetric strategy.** The concept of geoeconomics reflects how states employ financial and industrial leverage to secure national security objectives, increasingly turning supply chains and markets into tools of coercion.

- **Weaponisation of Supply Chains:** Nations that dominate the production of semiconductors, rare earth elements, or pharmaceutical ingredients can exercise coercion over dependent economies. Supply disruptions in these critical sectors create strategic vulnerabilities that rival the impact of military strikes.
- **Control of Infrastructure:** The acquisition of strategic assets such as ports, telecommunications networks (including 5G), and energy corridors by foreign state actors generates long-term dependencies. These footholds also serve as platforms for espionage, data collection, and potential sabotage.

- **Sanctions and Currency Warfare:** Financial systems themselves have become powerful weapons. Sanctions can isolate and weaken economies, while currency manipulation undermines fiscal stability. Such tools, although non-kinetic, can produce effects equivalent to those of traditional warfare, crippling the economic foundations of adversaries.

Geoeconomics underscores that **power projection is no longer confined to military strength;** control of trade, finance, and technology now shapes the balance of global security.

Adapt or Succumb

The asymmetric paradigm compels a **radical rethinking of national security strategies.** Traditional assumptions—where superiority in numbers or technology guaranteed dominance—are no longer sufficient.

- **From Superiority to Resilience:** Nations must prioritise resilience over mere superiority. This involves hardening critical infrastructure against physical, cyber, and EMP threats, diversifying supply chains, and ensuring governments and societies can operate in contested, degraded environments. Preparedness now means **building endurance, not just maintaining dominance.**
- **An Inter-domain Approach:** Effective defence requires seamless integration across land, sea, air, space, and cyber, combined with diplomatic, informational, and economic tools. Hybrid threats cannot be countered by militaries alone; they demand a **whole-of-government and whole-of-society approach.**
- **Innovation and Adaptability:** Armed forces must become more decentralised, agile, and less dependent on vulnerable technologies. Innovation must focus on dual paths: advancing sophisticated platforms while also developing **low-cost, redundant systems and unconventional tactics** capable of neutralising enemy asymmetry.

