KAPITAL | PARTNER

WHY DEFENCE-TECH HAS BECOME A NEW INVESTMENT CATEGORY

From the drone-dominated kill zone to AI-enabled autonomy

KAPITAL PARTNER INSIGHT · JULY 2026

Contents

Executive Summary

Defence-tech has moved from the periphery of the defence industry to become a distinct investment category. The change has been driven by rising defence expenditure, advances in commercially available technology and, above all, the operational lessons from Russia's full-scale invasion of Ukraine in February 2022.

The term defence-tech is sometimes used broadly to describe any innovative defence business. In this Insight, it primarily refers to companies developing comparatively affordable, software-enabled and increasingly autonomous unmanned systems, together with the technologies required to operate, connect and protect them.

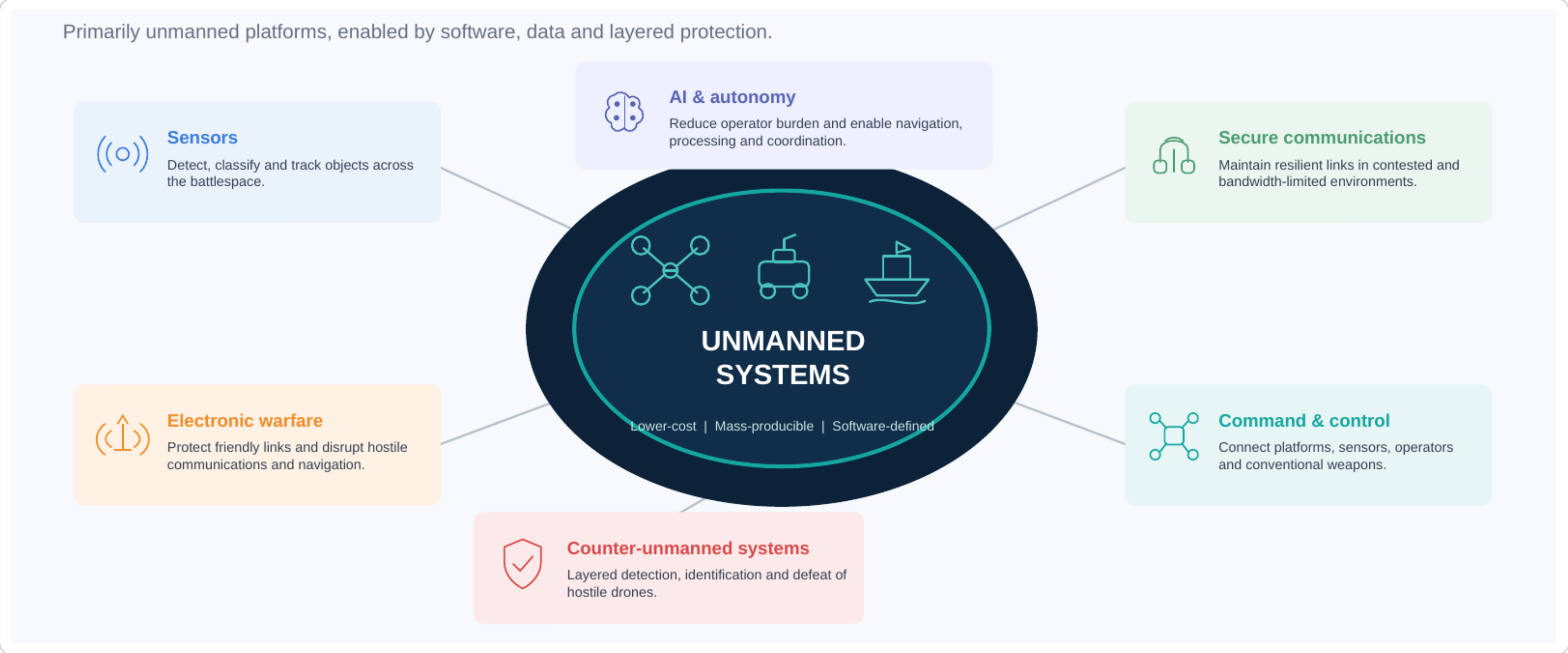
The core products are unmanned aerial, ground, surface and underwater systems. Around these platforms sits an enabling technology layer comprising sensors, artificial intelligence, secure communications, electronic warfare, command-and-control software and counter-unmanned-system solutions.

Defence 2.0 does not make conventional defence platforms such as combat aircraft, warships, missiles, artillery and armoured vehicles irrelevant. It does, however, challenge the way in which these Defence 1.0 systems have traditionally been designed and employed.

A modern tank remains valuable when it is protected by air defence, electronic warfare, reconnaissance drones, infantry and counter-drone capability. A tank operating without these supporting systems is now comparatively easy to detect, track and attack. It may be struck long before it is close enough to use its main weapon effectively.

The same applies to other large and visible platforms. Their traditional operating model has become partly obsolete, even where the platforms themselves have not.

Defence 2.0 at a glance



Executive Summary

Continued

The frontline in Ukraine is surrounded by a widening drone-dominated area commonly referred to as the kill zone. In the most intensively contested sectors, persistent aerial surveillance, FPV strike drones, artillery and electronic warfare can make exposed movement extremely dangerous at distances of 10–20 kilometres or more from the conventional line of contact. Personnel, vehicles, supply movements and casualty evacuations may be detected and attacked within minutes.

This environment has reduced the ability of tanks and other conventional systems to concentrate and manoeuvre freely. It has also accelerated the use of unmanned ground systems for logistics and evacuation, because tasks that were previously performed by soldiers or crewed vehicles have become too dangerous.

The defining feature of Defence 2.0 is not simply that its products are technologically advanced. It is that many of the systems are comparatively inexpensive, capable of being manufactured in high volumes and designed to be continually modified.

A current US procurement programme initially targeted small-drone costs of approximately USD 5,000 per unit, falling towards USD 2,300 at higher production volumes. By comparison, a 2024 US Army contract for 600 counter-drone interceptors had a value of USD 75 million, equivalent to approximately USD 125,000 per interceptor. A NATO procurement contract covering up to 1,000 Patriot GEM-T missiles had a potential value of USD 5.

6 billion, although that amount also included test equipment, spares, updated components and expansion of production capacity.

These figures are not directly comparable product prices. They nevertheless illustrate the exceptionally wide cost spectrum in modern defence and the economic need to match inexpensive threats with correspondingly affordable defensive systems.

Executive Summary

Continued

Russia's full-scale invasion forced Ukraine to accelerate the development of unmanned systems, electronic warfare and military software. This development was not primarily driven by investors or a long-term industrial policy. It was a military necessity.

Ukraine could not rely on sufficient quantities of aircraft, missiles, artillery, armoured vehicles and other conventional systems to counter a much larger adversary. Technology was therefore used to extend the reach of Ukrainian units, maintain battlefield surveillance, reduce the exposure of personnel and compensate for shortages of conventional equipment.

Ukraine has subsequently developed an exceptionally large and decentralised defence ecosystem. Depending on whether the count includes established manufacturers, incorporated defence companies, engineering teams, start-ups and projects under development, the broader ecosystem may comprise up to approximately 2,000 manufacturers, companies and development teams.

This is an indicative upper range rather than a precise corporate count. Official Ukrainian statements have separately referred to approximately 800 manufacturers and more than 1,000 teams developing defence solutions, and the two groups may overlap.

The Ukrainian procurement system is similarly decentralised. Combat brigades and other military units receive dedicated budgets and a degree of autonomy to select the drones, electronic-warfare systems and other equipment that meet their immediate operational requirements. The Ukrainian Ministry of Defence began providing UAH 2.5 billion (EUR 49.

0 million) per month directly to combat units for drone procurement in 2025, allowing commanders to choose the systems most relevant to their missions.

Executive Summary

Continued

Orders initiated at brigade or unit level can be small. A unit may need a limited number of drones with specific frequencies, cameras, payloads or electronic-warfare characteristics for a particular part of the frontline. These purchases can give manufacturers rapid access to users and valuable operational feedback, but they may provide limited revenue visibility.

The largest orders generally come through the Ministry of Defence, its procurement agencies or international financing programmes. These orders may cover hundreds of thousands or millions of units and can be financed by Ukraine's national budget, direct partner procurement or support mechanisms such as the Danish Model.

Under the Danish Model, partner-country funds are used to procure weapons directly from Ukrainian manufacturers for delivery to the Ukrainian Armed Forces. Ukraine reported more than USD 2 billion of manufacturing support through the mechanism in 2025.

Non-governmental organisations, charities and crowdfunding platforms represent a further procurement channel. Organisations such as UNITED24 and Come Back Alive have financed or procured drones, electronic-warfare equipment and other systems for particular units. NGO-funded purchases may range from small, highly specific orders to contracts covering thousands of systems.

The different sources of demand mean that reported Ukrainian revenue must be analysed carefully. A sale financed by a brigade, a charity, the central Ministry of Defence or an international support scheme may involve the same end user, but the contract size, payment security, purchasing process and likelihood of repetition can be materially different.

Executive Summary

Continued

Ukraine estimated domestic production capacity of approximately 4.5 million FPV drones in 2025 and allocated more than UAH 110 billion (EUR 2.15 billion) to drone procurement for that year. By 2026, the official production-capacity estimate for FPV drones had increased to more than eight million annually across more than 160 companies.

This scale also creates new constraints. Armed forces cannot increase the number of trained operators at the same rate as the number of platforms. Nor can they assume that reliable radio communications and satellite navigation will remain available in an environment characterised by jamming, spoofing and attacks on communications infrastructure.

Artificial intelligence and autonomy are therefore becoming operational requirements rather than optional product enhancements. They enable unmanned systems to navigate, process sensor data, recognise objects and continue parts of a mission when communications are lost.

AI and autonomy are also necessary if large numbers of drones are to operate together as coordinated groups or swarms. A human operator cannot manually control every movement of dozens or hundreds of platforms while simultaneously processing their sensor data and adapting the mission.

The expansion of Defence 2.0 also changes the traditional logic of military stockpiling. Artillery shells, spare parts and conventional ammunition can be stored for extended periods if appropriately maintained. Fast-changing drones, communications modules and electronic-warfare systems may become operationally outdated within months or, in some cases, weeks.

An armed force cannot therefore rely solely on purchasing a fixed drone configuration and storing it for a future war. By the time it is needed, its frequencies, navigation system, software or communications link may already be vulnerable to available countermeasures.

Executive Summary

Continued

The resulting model is based less on warehousing large quantities of finished systems and more on maintaining production capacity, adaptable designs, modular components, access to critical materials, software-update capability and contracts that can respond rapidly to changing requirements.

The addressable market extends well beyond Ukraine. NATO Allies in Europe and Canada spent approximately USD 486 billion on defence in 2024 and USD 574 billion in 2025. EU Member States spent EUR 343 billion in 2024, including more than EUR 100 billion classified as defence investment.

Not all of this expenditure is accessible to defence-tech companies. Major platforms, personnel, infrastructure, conventional ammunition and maintenance will continue to absorb substantial parts of national budgets. Nevertheless, drones, counter-drone defence, electronic warfare, resilient communications, software and autonomy have become recognised capability priorities.

The market can be divided into three connected but materially different segments: Ukraine and other active-conflict markets; NATO and other national defence markets; and civil security and critical-infrastructure protection. Each has different customers, procurement procedures, prices, product requirements and investment risks.

Ukrainian defence-tech companies frequently have superior access to battlefield users, operational data and real-time testing. Their products may be developed more quickly and at lower cost than comparable systems outside Ukraine.

They also tend to make extensive use of Chinese-origin commercial products and components. Chinese cameras, motors, batteries, flight controllers, communications components and complete consumer drones have historically offered the lowest combination of price, performance and immediate availability. In a war of attrition, where equipment is consumed in very large quantities, this has frequently outweighed longer-term supply-chain concerns.

Executive Summary

Continued

NATO markets have a very different approach. Allied armed forces are increasingly unwilling to accept Chinese-origin critical components in military systems because of cybersecurity, supply-chain and strategic-dependency concerns. This creates both a challenge and an opportunity for Ukrainian manufacturers. A low-cost, battle-tested product may require a substantially redesigned supply chain before it can be sold to NATO customers.

Non-Ukrainian defence-tech companies generally benefit from more familiar corporate structures, stronger compliance, better access to institutional capital and established routes into NATO procurement. Their products may, however, be more expensive, take longer to develop and have less exposure to realistic operational testing.

The greatest commercial opportunity may lie in combining the two ecosystems: Ukrainian technology, speed and operational knowledge with international capital, production, governance, certification and market access.

Demand will not end with the war in Ukraine. European and allied armed forces must replenish inventories, develop permanent drone and counter-drone capabilities, strengthen electronic warfare and redesign force structures around the lessons from the war. Ukraine is also likely to remain an important defence producer, testing environment and technology partner after active hostilities have ceased.

Defence-tech is not a formal asset class in the same sense as listed equities, bonds or property. It is more accurately described as a new investment category with its own demand drivers, technology cycles, capital requirements, risk factors and valuation considerations.

Executive Summary

Continued

That does not make every defence-tech company an attractive investment. The category includes scalable software companies, industrial manufacturers, early-stage development projects, component suppliers and businesses dependent on one customer or one temporary product advantage.

Investors must assess not only whether the technology works, but whether the company can manufacture it, continually update it, sell it across different procurement systems, finance its growth and create governance structures that meet international standards.

1. From traditional defence to Defence 2.0

1.1 The traditional defence industry

The traditional defence industry is built around major platforms and long-term national capability programmes.

Its products include combat aircraft, warships, submarines, missiles, integrated air-defence systems, artillery and armoured vehicles. These systems remain strategically essential. Small unmanned systems cannot independently replace air superiority, strategic air defence, protected mobility, naval power or the ability to deliver large quantities of firepower.

Traditional platforms are designed to remain operational for decades. Reliability, safety, interoperability, certification and lifecycle support are therefore central requirements.

Their development and procurement commonly involve long programmes, high unit values, limited production quantities and close relationships between government customers and a relatively small number of major contractors.

This model provides advanced and reliable capability, but it can also limit the speed of adaptation. Requirements may be established years before a product enters service. Modifying software, sensors or components may involve renewed certification and extensive integration work.

1.2 A complementary industrial model

Defence 2.0 represents a complementary industrial and operational model.

It is primarily built around unmanned platforms, commercially available components, software-defined capabilities and shorter development cycles. Many of the products are designed to be manufactured in relatively large numbers and modified repeatedly in response to changing threats.

1. From traditional defence to Defence 2.0

Continued

A small FPV drone is not a direct substitute for a combat aircraft, missile or artillery system. It performs a different mission at a different cost and level of risk.

A relatively inexpensive unmanned system can be used in situations where deploying a high-value crewed platform would be economically disproportionate or expose personnel unnecessarily. It can also be accepted that the system may not return from its mission.

The distinction between traditional defence and Defence 2.0 is therefore not simply one of old and new technology. It concerns the economics of production, deployment, replacement and adaptation.

From traditional defence to Defence 2.0

A complementary model that changes how capability is produced, deployed and protected.

TRADITIONAL DEFENCE

Major crewed platforms
Long development programmes

High unit values
Limited production quantities

Long service lives
Centralised procurement

Warehousing & lifecycle planning
Hardware-led integration

DEFENCE 2.0

Primarily unmanned platforms
Rapid, iterative development

Lower unit values for many systems
Mass production & replacement

Frequent hardware/software updates
Greater unit-level purchasing influence

Adaptable production capacity
Software, data & AI as core capability

Defence 2.0 supplements—and increasingly protects—traditional platforms.

1. From traditional defence to Defence 2.0

Continued

1.3 The drone-dominated kill zone

The combination of persistent surveillance drones, FPV strike systems, artillery, mines and electronic warfare has created a broad area around the Ukrainian frontline in which visible movement is extremely dangerous.

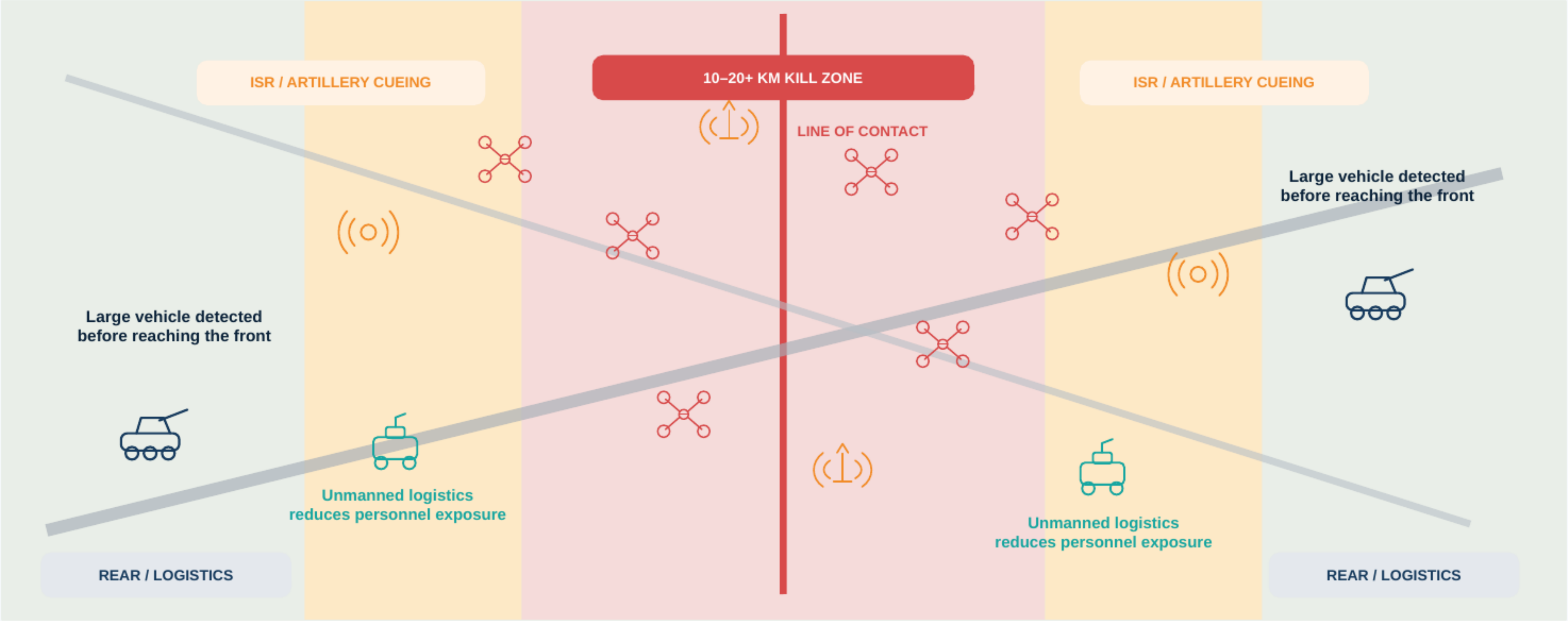
This area is commonly described as the kill zone.

Its exact depth varies according to terrain, weather, available drone systems, electronic-warfare coverage and the capabilities of the opposing units. In heavily contested areas, the zone may extend 10–20 kilometres or more from the conventional line of contact.

Within this zone, surveillance drones can observe roads, tracks, tree lines and defensive positions for extended periods. Once movement is detected, strike drones or artillery may be directed towards the target.

The drone-dominated kill zone

Persistent surveillance and low-cost strike systems expose movement well before the line of contact.



1. From traditional defence to Defence 2.0

Continued

The consequences extend beyond direct combat. Supply vehicles may be unable to approach positions during daylight. Casualty evacuation can be delayed because ambulances and medics are themselves exposed. Troops may have to travel on foot in small groups, while equipment is transported by unmanned ground vehicles.

The kill zone has therefore become both a tactical and a logistical phenomenon.

1.4 The changing role of Defence 1.0 platforms

The kill zone has not made tanks, infantry fighting vehicles or artillery obsolete in an absolute sense. It has made their traditional use increasingly difficult.

A tank is large, creates heat, noise and tracks, and is comparatively easy to identify from the air. Once detected, it may be attacked by several drones from different directions, tracked for artillery or forced to withdraw before reaching an effective firing position.

Concentrating large formations of vehicles also creates a visible target. This reduces the ability to conduct the kind of massed armoured manoeuvre traditionally associated with mechanised warfare.

Defence 1.0 systems increasingly require a Defence 2.0 protection layer comprising reconnaissance drones, electronic warfare, short-range air defence, counter-drone systems, camouflage and deception, rapid intelligence, unmanned logistics and distributed command and control.

The platform itself has not necessarily become obsolete. The assumption that it can operate effectively without this supporting technology has.

1. From traditional defence to Defence 2.0

Continued

For investors, this distinction is important. Defence-tech is not growing only because governments want to purchase new categories of equipment. It is also growing because existing high-value platforms require new layers of protection, sensing and integration to remain operationally relevant.

1.5 The importance of mass

The value of many defence-tech systems comes from their ability to be produced and deployed in large numbers.

Mass provides geographical coverage, redundancy and the ability to absorb losses. It can also overwhelm detection and defensive systems by presenting more threats than the opponent can engage economically.

However, mass does not mean that any inexpensive drone automatically has military value.

A low-cost system that cannot navigate, communicate, identify its target or resist electronic warfare may be ineffective. The Defence 2.0 model depends on combining affordable scale with sensors, software, electronic protection and operational integration.

1.6 Software-defined capability

Many Defence 1.0 products are also highly dependent on software. The distinction is that Defence 2.0 systems are often designed from the outset to be modified through frequent software releases and relatively simple hardware changes.

Software may determine how a system navigates, processes sensor information, communicates, reacts to jamming, identifies objects or coordinates with other platforms.

A product’s physical appearance may therefore remain almost unchanged while its military effectiveness changes substantially.

1. From traditional defence to Defence 2.0

Continued

This creates an investment characteristic familiar from other technology sectors: a meaningful part of the company's value may reside in code, algorithms, data and system integration rather than solely in the airframe, vehicle or vessel.

1.7 Production flow rather than conventional warehousing

Rapid technological obsolescence changes the procurement model.

Traditional ammunition and many mechanical components can be stored for long periods. Fast-changing drones and electronic-warfare systems may become operationally unsuitable because the opponent has learned to detect their frequencies, jam their navigation or exploit their communications architecture.

For these systems, no armed force can sensibly rely exclusively on purchasing a fixed configuration and storing it for several years.

This does not mean that armed forces should maintain no stocks. They require reserve equipment, components and immediate replacement capacity. The difference is that readiness increasingly depends on maintaining an adaptable industrial base rather than only a warehouse of finished products.

The most valuable reserve may consist of production lines that can be expanded, modular designs, non-obsolescent components, software-update capability, access to secure supply chains and procurement contracts that can be changed quickly.

Ukraine's DOT-Chain Defence model reflects this logic. Units select systems based on their current operational needs, and products available from manufacturers can be delivered within approximately ten days. The Ministry of Defence has stated that conventional procurement for stock does not work for such rapidly changing requirements.

2. What defence-tech comprises

2.1 Unmanned aerial systems

Unmanned aerial systems are the most visible part of the defence-tech category.

They range from small quadcopters and FPV systems to fixed-wing reconnaissance aircraft, communications relays, heavy payload carriers, interceptor drones and long-range strike platforms.

A small reconnaissance drone can provide a unit with immediate information about enemy movement. An FPV drone can deliver a relatively precise strike at a fraction of the cost of many conventional weapons. Larger systems can carry advanced sensors, act as communications relays or attack targets hundreds of kilometres away.

The investment characteristics differ materially between product types.

A small FPV system may be assembled from commercially available components and produced in very high volumes. A long-range platform requires more advanced navigation, payload integration, communications and production quality. A reconnaissance system may derive more of its value from its sensors and data-processing software than from the airframe itself.

Investors should therefore not analyse all drone companies as one group. Their technical complexity, product cost, barriers to entry, gross margins and customer relationships can be entirely different.

2.2 Unmanned ground systems

Unmanned ground vehicles are increasingly used to perform tasks that have become too dangerous for soldiers or conventional vehicles inside the kill zone.

2. What defence-tech comprises

Continued

Their most common uses in Ukraine are logistics and casualty evacuation. A small tracked or wheeled vehicle can carry ammunition, food, batteries or other supplies to a position without exposing a driver. On the return journey, it may evacuate a wounded soldier.

Other applications include mine detection, engineering, surveillance, communications relay and remote weapon operation.

Ground systems face considerable technical challenges. They must operate through mud, damaged roads, trenches and obstacles while maintaining communications and carrying a useful payload.

Ukraine's procurement indicates that the category has moved beyond experimental use. By July 2026, the Ukrainian Defence Procurement Agency had contracted more than 22,000 unmanned ground vehicles for the year. Most were logistics platforms, with smaller numbers designed for engineering and combat functions.

2.3 Unmanned maritime systems

Unmanned maritime systems include surface vessels and underwater vehicles.

They can be used for coastal surveillance, harbour protection, mine clearance, intelligence collection, logistics, infrastructure inspection and offensive operations.

Ukraine's use of unmanned surface vessels in the Black Sea has demonstrated that comparatively inexpensive, uncrewed platforms can restrict the freedom of action of a conventionally stronger navy.

The broader investment opportunity extends beyond strike vessels. Ports, naval bases, offshore energy installations, pipelines and subsea cables all require improved monitoring and protection.

2. What defence-tech comprises

Continued

Maritime systems generally require more capital and engineering than small aerial drones. They must withstand water, weather, waves and extended missions while maintaining navigation and communications.

2.4 Sensors and intelligence

An unmanned platform is only useful if it can observe, navigate or deliver an effect.

Relevant technologies include optical and thermal cameras, radar, acoustic detection, radio-frequency sensors, signal intelligence, satellite data and alternative navigation systems.

The value increasingly lies in combining information from several sensors.

A radar may detect an object but be unable to classify it. A camera may identify it but have limited range or be affected by weather. A radio-frequency sensor may detect the control link of one drone but fail to identify a fully autonomous system.

Sensor fusion combines these inputs into a more reliable operational picture. This is an important application of software and artificial intelligence.

2.5 Electronic warfare

Electronic warfare concerns the detection, protection, exploitation and disruption of electromagnetic signals.

It includes locating transmitters, intercepting signals, jamming communications, disrupting satellite navigation and transmitting false navigation information through spoofing.

Electronic warfare is central to the drone market because many inexpensive systems depend on radio communications and satellite positioning.

2. What defence-tech comprises

Continued

This creates a continuous cycle of measure and countermeasure. A new drone or communications method is introduced, the opponent develops a countermeasure, and the manufacturer must change frequencies, components, software or operational procedures.

The commercial life of a specific technical configuration may therefore be short. A successful company requires not only an effective current product but also an organisation capable of continual adaptation.

2.6 Communications and command systems

Unmanned systems achieve their greatest value when connected to military units, sensors and conventional weapons.

Command-and-control systems allow users to share sensor information, assign missions, coordinate several platforms and connect drones with artillery, air defence or ground units.

A stand-alone drone can solve a narrow task. An integrated network can change how an entire formation operates.

For investors, this creates opportunities beyond the physical platform. Software licences, integration, maintenance, data services and fleet management may provide more predictable and scalable revenues than one-off hardware sales.

2.7 Counter-unmanned systems

The growth of unmanned platforms has created a corresponding market for systems that detect, identify and neutralise them.

No single countermeasure is effective against every type of drone.

2. What defence-tech comprises

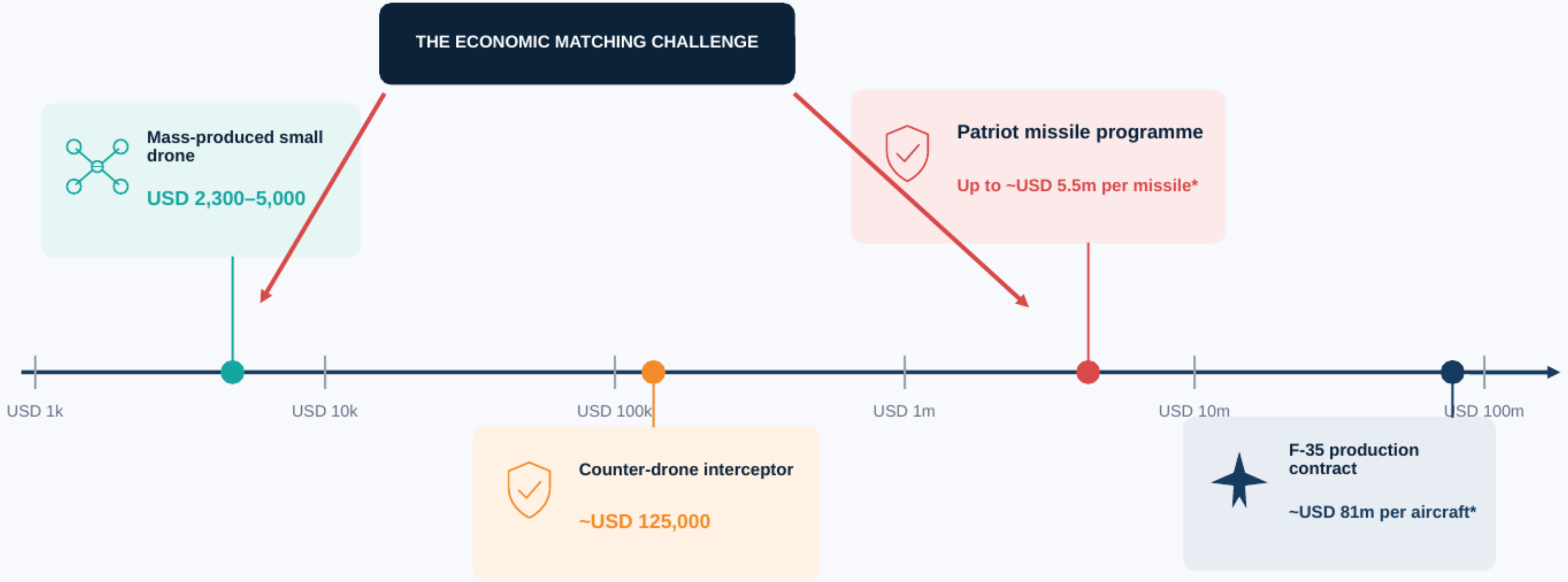
Continued

Jamming may defeat a radio-controlled platform but have limited effect on an autonomous or fibre-optic-controlled drone. A kinetic interceptor may be effective but too expensive for repeated use against basic targets. A laser may offer a low marginal engagement cost but requires power, line of sight and suitable atmospheric conditions.

Counter-drone defence therefore needs to be layered.

The cost and scale spectrum

Illustrative contract-level values demonstrate why defence needs a layered economic response.



Low-cost threats cannot be defeated economically with the most expensive effector every time.

2. What defence-tech comprises

Continued

The system must detect and classify the threat before choosing the least expensive effective response. This makes sensors and command software as important as the final interceptor.

The economics are central. A sophisticated air-defence missile may be justified against a ballistic or cruise missile but economically unsuitable against a drone costing a few thousand dollars.

3. Ukraine as the catalyst

3.1 The February 2022 inflection point

Defence innovation did not begin with Russia's full-scale invasion.

Ukraine had accumulated operational experience since Russia's initial aggression in 2014, and drones, military software and electronic warfare were already being developed internationally.

The full-scale invasion nevertheless changed the speed, scale and strategic importance of defence-tech.

Ukraine faced a larger opponent with substantial inventories of artillery, missiles, aircraft and armoured vehicles. Western military assistance was essential, but delivery volumes and political decision-making could not always match immediate battlefield requirements.

Ukraine therefore had to create additional capability through domestic innovation.

Technology extended the reach of individual units, maintained surveillance over a long frontline, reduced dependence on scarce conventional ammunition and allowed operations to be carried out without exposing high-value crewed platforms.

Defence-tech became essential to Ukraine's ability to avoid defeat.

3.2 Development under operational pressure

A conventional defence-development programme may take several years to move from requirements to design, testing, certification and procurement.

In Ukraine, the sequence can be compressed to weeks.

A military unit identifies a problem. Engineers develop or modify a product. It is tested operationally, the unit provides feedback and a new version is introduced.

3. Ukraine as the catalyst

Continued

This provides direct evidence of relevance. It also creates commercial and organisational weaknesses.

Product changes may be insufficiently documented. Quality can vary between production batches. Intellectual-property ownership and formal agreements with engineers or military users may not have been prioritised.

The characteristics that make a company effective in wartime do not automatically make it ready for international investment or NATO procurement.

3.3 The scale of the ecosystem

Ukraine’s defence ecosystem includes established manufacturers, start-ups, engineering teams, software developers, volunteer initiatives, state-owned businesses and component suppliers.

Depending on the definition applied, the broad ecosystem can be described as comprising up to approximately 2,000 manufacturers, companies and development teams.

The upper figure should not be understood as the number of mature or investable businesses. Official Ukrainian statements have separately referred to approximately 800 manufacturers and more than 1,000 development teams. The categories may overlap and include organisations at very different stages of development.

A more selective indicator is the number of suppliers that have obtained meaningful procurement contracts.

Scale of Ukraine’s defence-tech ecosystem

A broad innovation base—but the headline counts measure different and overlapping populations.

UP TO

~2,000

manufacturers, companies and development teams

Broad ecosystem estimate
Categories overlap and include projects at very different stages.

~800
Manufacturers
Earlier official ecosystem count

1,000+
Development teams
Advanced defence solutions

600+
Brave1-supported companies
Grant support during 2025

160+
FPV producers
Reported active in 2026

8m+
Annual FPV capacity
Potential output—not deliveries

500 / 140+
Systems / manufacturers
DOT-Chain catalogue, March 2026

DIFFERENT MEASURES — NOT ADDITIVE

The broad ecosystem count is not the number of mature or investable businesses. Procurement access, production scale and governance remain important filters.

3. Ukraine as the catalyst

Continued

The Ukrainian Defence Procurement Agency had signed UAV supply contracts with 76 domestic manufacturers during 2024 and 2025. By March 2026, the DOT-Chain Defence catalogue contained nearly 500 products from more than 140 domestic manufacturers.

The difference between the broad ecosystem estimate and the number of contracted suppliers illustrates the importance of commercial due diligence.

3.4 Decentralised brigade procurement

Ukraine has developed a procurement model in which combat brigades and other military units have their own budgets and substantial influence over the equipment they receive.

The Ministry of Defence began allocating UAH 2.5 billion (EUR 49.0 million) per month directly to combat units for drone procurement in 2025. Commanders were given flexibility to select the systems most relevant to their operational tasks.

The DOT-Chain Defence marketplace has extended this model. Units can select products from a digital catalogue, while the central procurement agency manages the contract, payment and delivery process.

This decentralisation has several advantages.

The brigade knows the electronic-warfare environment, terrain and tactical requirements in its sector. It can select a drone with the appropriate range, frequency, payload or camera rather than accept a standard system selected centrally months earlier.

It also gives manufacturers direct market feedback.

A product that performs well may receive repeat orders from the same or neighbouring units. A product that fails can lose demand quickly.

3. Ukraine as the catalyst

Continued

Unit-level orders may be relatively small. A brigade might initially request a limited batch for testing or for one specific mission. From the manufacturer's perspective, this can create valuable validation but fragmented revenues and uneven production planning.

3.5 Central Ministry of Defence procurement

The largest and most standardised orders generally come from the Ministry of Defence and its procurement agencies.

Central procurement is suitable when Ukraine requires large quantities of proven systems, when prices can be negotiated on volume, or when funding must be coordinated across international partners.

The Defence Procurement Agency delivered approximately 500,000 items through DOT-Chain Defence during its first seven months, with a total value of UAH 23.3 billion (EUR 456 million). The wider procurement system also places much larger orders outside the digital marketplace.

These central contracts can provide manufacturers with volume and revenue visibility, but they may also require greater documentation, production capacity and financial resources.

3.6 Internationally financed orders and the Danish Model

A significant share of Ukrainian defence procurement is financed by international partners.

Under the Danish Model, partner-country funding is used to procure products directly from the Ukrainian defence industry. The equipment is manufactured in Ukraine and delivered to the Ukrainian Armed Forces.

3. Ukraine as the catalyst

Continued

The model combines military assistance with industrial support. It can provide faster delivery, lower costs and maintenance closer to the frontline while preserving Ukrainian employment and production capacity.

Ukraine reported more than USD 2 billion of funding for Ukrainian manufacturing through the Danish Model during 2025. The mechanism has also used contributions from the EU, Canada and other countries, including revenues associated with frozen Russian assets.

For a manufacturer, these orders may appear commercially similar to Ministry of Defence sales, but the underlying financing and approval process can be different.

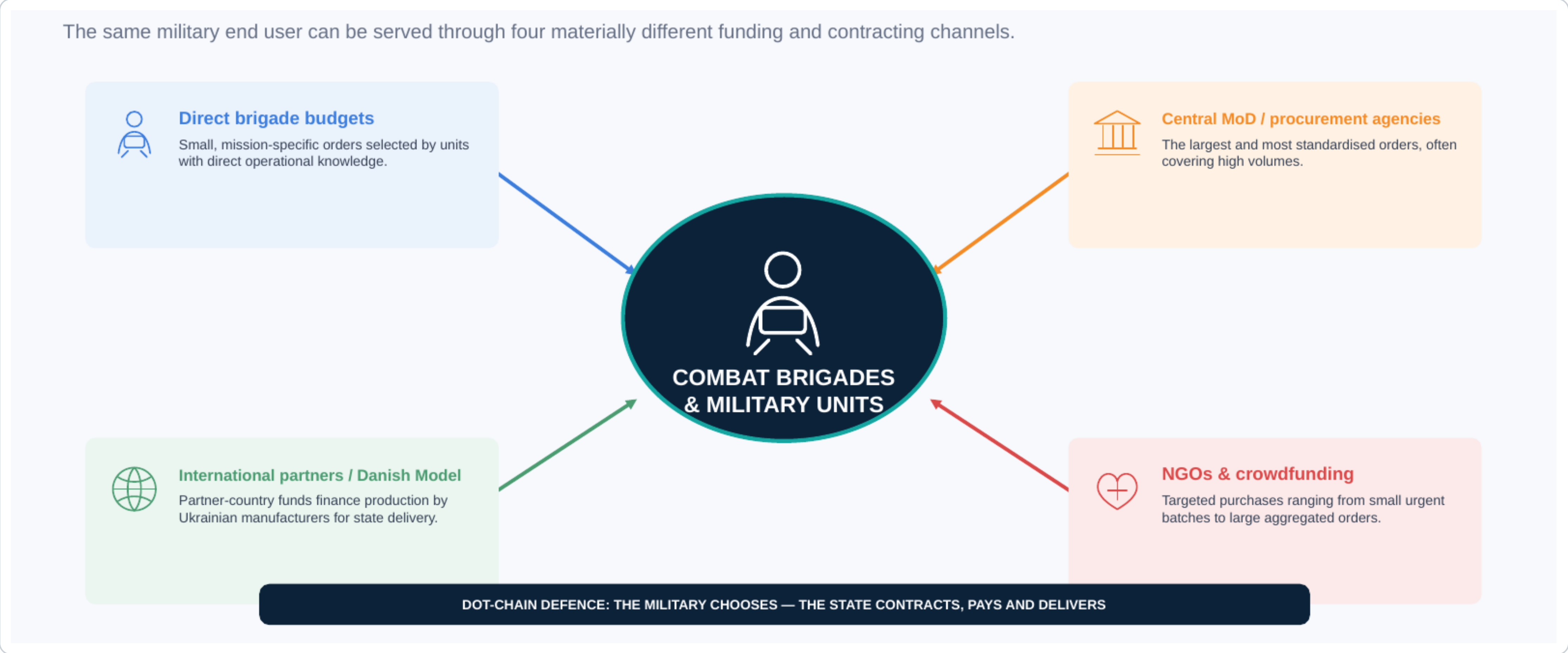
3.7 NGOs, charities and crowdfunding

NGOs and charities have played an unusually important role in Ukrainian defence procurement.

UNITED24, Come Back Alive, the Serhiy Prytula Charity Foundation and numerous smaller initiatives have financed drones, vehicles, communications equipment and electronic-warfare systems for military units.

The funding source may be Ukrainian citizens, international donors, companies or targeted crowdfunding campaigns.

Ukraine's defence-tech procurement system



3. Ukraine as the catalyst

Continued

Some purchases are small and directed towards one unit. Others are large. In 2026, Come Back Alive reportedly signed contracts for approximately 16,500 long-range FPV drones with a total value of approximately UAH 1.37 billion (EUR 26.8 million).

NGO purchases can allow urgent needs to be met quickly and may introduce new manufacturers to military users.

From an investor perspective, however, NGO-financed revenue must be assessed separately from recurring state procurement. A successful fundraising campaign does not necessarily establish a durable public budget or future order programme.

3.8 Production and procurement volumes

Ukraine's production scale has increased dramatically.

The Ministry of Defence estimated 2025 domestic capacity at approximately 4.5 million FPV drones. By 2026, the National Security and Defence Council reported annual capacity exceeding eight million FPV drones across more than 160 companies.

These figures measure capacity rather than actual deliveries.

Market analysis must distinguish between potential production capacity, procurement budgets, signed contracts, delivered quantities and actual end-user consumption.

The distinction is important because the Ukrainian industry has at times had more production capacity than funded procurement demand.

4. Why AI and autonomy are becoming necessary

4.1 The operator constraint

A manually controlled drone requires an operator, training, communications equipment and organisational support.

This model can work when systems are deployed in limited numbers. It becomes difficult when armed forces seek to operate thousands or millions of platforms.

Personnel cannot be expanded at the same rate as hardware production. Operators are also vulnerable because their radio transmissions and antenna positions may reveal their location.

AI and autonomy can automate take-off, navigation, obstacle avoidance, landing, route planning and routine sensor analysis.

This does not necessarily remove humans from decisions concerning the use of force. It can allow one operator to supervise several systems rather than manually flying one platform throughout its mission.

4.2 The communications constraint

Remote control depends on a functioning communications link.

That link may be jammed, intercepted, located or obstructed by terrain. Satellite navigation may also be jammed or spoofed.

A platform with no autonomous capability may become ineffective as soon as it loses contact with its operator.

A more autonomous system can continue along a pre-planned route, navigate using visual or inertial information, identify a landing area or return safely.

Autonomy is therefore an important form of resilience.

4. Why AI and autonomy are becoming necessary

Continued

4.3 The data constraint

Large numbers of drones, cameras, radars and other sensors generate more information than human operators can process in real time.

AI can filter irrelevant information, compare several sensor feeds, identify anomalies and prioritise possible threats.

The operational advantage is not necessarily that the machine makes the final decision. It is that the human decision-maker receives more relevant information more quickly.

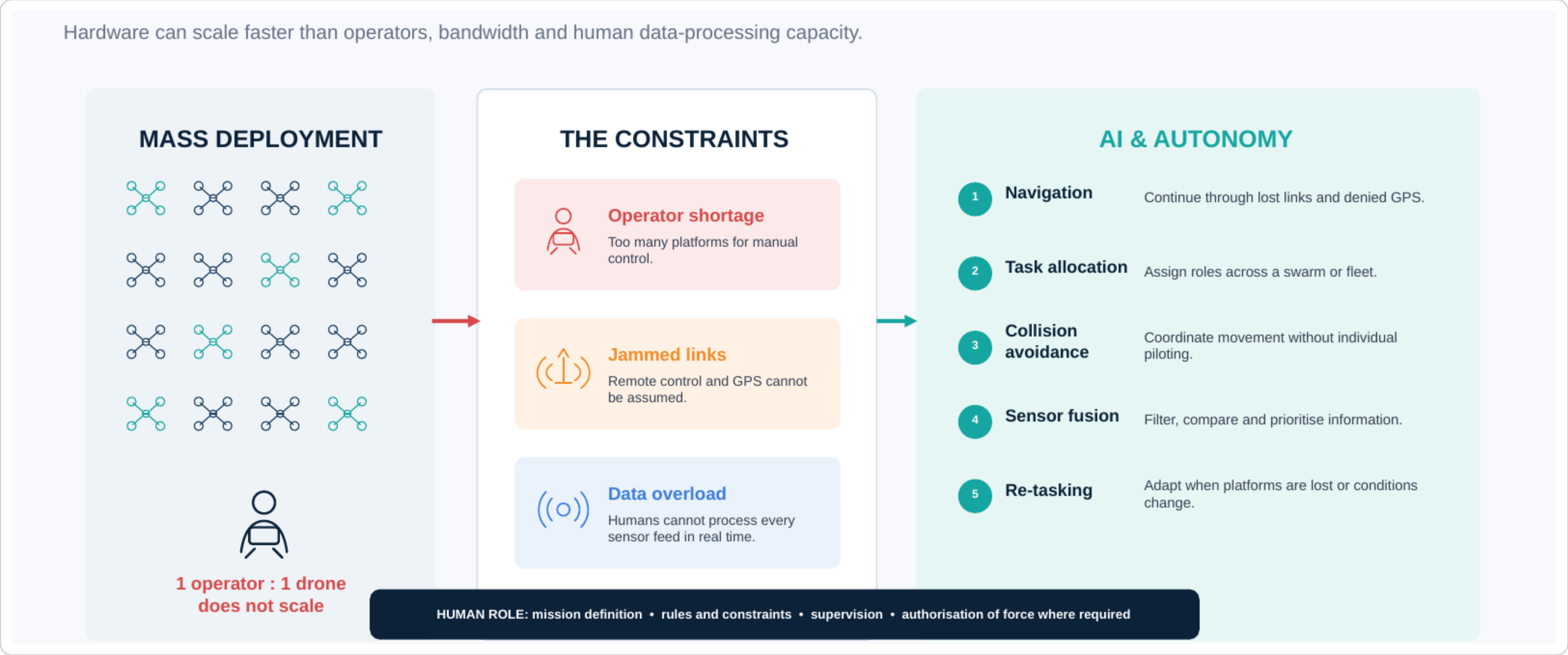
4.4 Drone swarms

A drone swarm consists of multiple unmanned systems operating as a coordinated group.

The systems do not necessarily need to fly in a visually dense formation. The defining feature is that they share tasks, information or mission objectives and coordinate at least part of their operation.

A swarm might distribute reconnaissance across a large area, approach a target from several directions or allocate different systems to communications, sensing and strike functions.

Why mass and swarms require autonomy



4. Why AI and autonomy are becoming necessary

Continued

Manual control is not scalable in this environment.

An operator cannot individually pilot dozens or hundreds of drones while maintaining coordination and responding to losses, electronic warfare and changing targets.

AI and autonomy are therefore essential to maintain formation or task distribution, prevent collisions, reallocate missions when individual drones are lost, identify routes, combine sensor information, coordinate timing and reduce the number of operators required.

Human control may remain at the mission or authorisation level, while the systems manage movement and coordination.

The development of practical swarms will increase demand for software, communications, edge computing and command systems rather than only for additional airframes.

4.5 The economics of autonomy

Hardware and software have different economic characteristics.

Every additional drone requires components, assembly, testing and logistics. Software can potentially be deployed across a fleet at a much lower marginal cost.

This creates opportunities for recurring licences, fleet updates, mission-planning software, data services and integration fees.

The investment case depends on whether the software is proprietary and commercially separable.

A company should not receive a software valuation merely because its physical product contains code. Investors must establish whether customers pay for updates, whether the company owns the relevant algorithms and whether the software creates meaningful switching costs.

4. Why AI and autonomy are becoming necessary

Continued

4.6 The limits of autonomy

AI and autonomy create technical, legal and ethical risks.

Systems may misclassify objects, fail in unfamiliar conditions or be manipulated by deceptive signals and images. Algorithms trained on one battlefield may perform differently in another environment.

Customers will therefore require testing, cybersecurity, traceability, defined human-control mechanisms and clear procedures for system failure.

The most credible companies will be able to explain precisely which functions are autonomous, under which conditions they operate and how their performance has been validated.

5. The three defence-tech markets

5.1 Ukraine and active-conflict demand

Ukraine is both a substantial customer market and a unique development environment.

Its defining characteristics are immediate operational demand, rapid testing, high consumption and frequent changes in product specifications.

A company may obtain direct user access and initial revenue faster than it could in a Western procurement system. However, orders may be small, short term and dependent on the needs of an individual brigade.

The market also places exceptional pressure on prices.

Products are consumed in very large numbers, and many are lost during missions. A system that is technically advanced but too expensive to deploy at scale may have limited relevance.

5.2 NATO and other national defence markets

International defence markets offer significantly larger aggregate budgets and the possibility of multi-year contracts.

NATO Allies in Europe and Canada spent approximately USD 486 billion on defence in 2024 and USD 574 billion in 2025. EU Member States spent EUR 343 billion in 2024, of which more than EUR 100 billion was classified as defence investment.

NATO’s 2025 Hague commitment requires Allies to work towards investment equivalent to 5% of GDP by 2035, including at least 3.5% for core defence requirements.

Only part of this expenditure will be available to defence-tech companies. However, drones, counter-drone systems, electronic warfare and resilient communications are now established procurement priorities.

5. The three defence-tech markets

Continued

These markets generally require formal tenders, certification, security compliance, interoperability, production planning and long-term support.

The sales process may take several years. A successful demonstration does not guarantee a production order.

Once a company enters an established programme, however, it may obtain larger contracts, longer revenue visibility and recurring service or software revenues.

5.3 Civil security and critical infrastructure

Defence-tech also has applications outside the armed forces.

Airports, ports, energy installations, border authorities, police, emergency services and owners of subsea infrastructure require better surveillance, drone detection, autonomous inspection and secure communications.

Civil markets can diversify revenue and reduce dependence on defence budgets.

However, a military product is not commercially dual-use merely because a theoretical civil application can be identified.

A credible civil-market case requires a specific customer need, an available budget, regulatory permission, acceptable liability characteristics and an effective route to market.

5.4 Movement between the markets

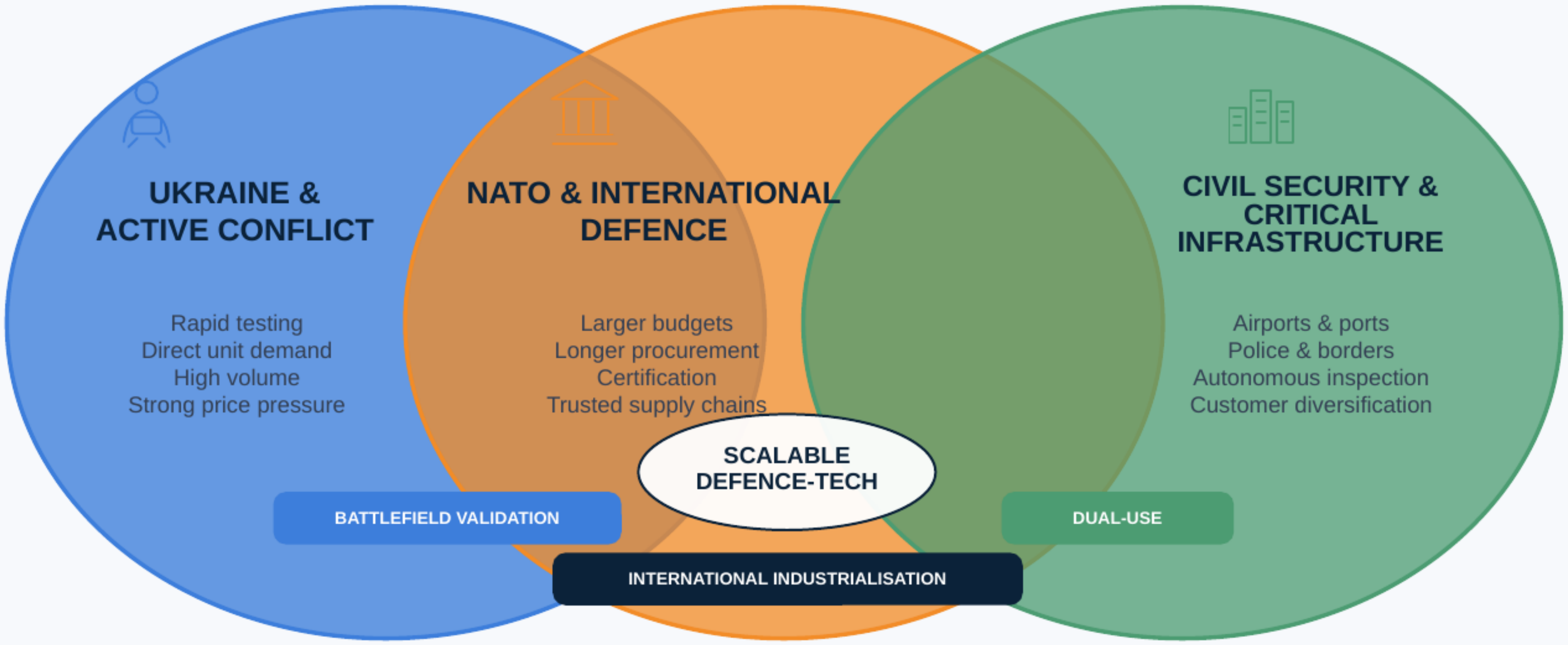
The three markets provide different forms of value.

Ukraine provides rapid operational validation and user feedback.

International defence markets provide larger contracts, higher prices and long-term programmes.

The three defence-tech markets

The same technology can move between markets—but customer needs and procurement logic differ.



Three markets — three procurement logics

5. The three defence-tech markets

Continued

Civil-security markets can provide diversification and recurring infrastructure demand.

The principal commercial challenge is translating success in one market into acceptance in another.

A product that performs well in Ukraine may still require redesign, cybersecurity work, documentation and certification before it can enter NATO procurement.

A Western product that meets formal specifications may require lower costs and greater resistance to electronic warfare before it is competitive in Ukraine.

6. Ukrainian and non-Ukrainian producers

6.1 Ukrainian producers

The principal advantage of Ukrainian companies is their proximity to the user and the operational problem.

Many receive feedback directly from military units and can observe how their products perform against current enemy countermeasures.

Typical strengths include rapid iteration, lower costs, operational testing, understanding of electronic warfare and a strong focus on practical performance.

Typical risks include war exposure, limited working capital, incomplete documentation, immature governance, customer concentration and uncertain international market access.

Some companies are still organised around founders, individual engineers or military relationships rather than a scalable institution.

Investors must determine whether the technology and customer access belong to the company or depend on a small number of individuals.

6.2 Non-Ukrainian producers

Non-Ukrainian defence-tech companies generally benefit from established legal structures, stronger financial reporting, clearer intellectual-property ownership and greater access to institutional capital.

They are more likely to understand certification, export control and the requirements of NATO procurement.

Their weaknesses may include slower development, higher production costs and limited access to realistic battlefield testing.

6. Ukrainian and non-Ukrainian producers

Continued

A well-governed company can still consume large amounts of capital developing a product that customers ultimately decline to procure.

6.3 Different testing opportunities

Ukraine provides testing conditions that cannot be reproduced fully on a controlled range.

Products encounter active jamming, spoofing, enemy detection, difficult weather, high usage rates and changing countermeasures.

This provides strong evidence of operational relevance.

It does not replace formal qualification.

International customers may still require controlled performance data, cybersecurity testing, safety documentation and supply-chain certification.

Battlefield validation and formal certification answer different questions. Strong businesses will be able to provide both.

6.4 Different sales and production models

Ukrainian companies may obtain rapid initial orders from brigades, charities or central agencies. Production is often optimised for low cost, rapid assembly, field repair and frequent modification.

Western products are more commonly designed for repeatable quality, documented components, cybersecurity, warranties, maintenance and longer service lives.

Neither model is inherently superior.

A short-lived FPV drone should not be designed according to the same lifecycle assumptions as a reusable military aircraft. Conversely, a system protecting a civilian airport cannot be accepted with inconsistent production quality or undocumented software.

6. Ukrainian and non-Ukrainian producers

Continued

6.5 Chinese products and components

The difference in supply-chain requirements is particularly visible in relation to China.

Ukraine has relied extensively on Chinese-origin commercial products and components because they are generally the cheapest and most readily available at scale.

The supply chain has included complete consumer drones as well as motors, cameras, batteries, flight controllers, radios and electronic components.

This reliance is rational in the immediate context of a war of attrition. Ukrainian units need large quantities quickly, and a more expensive allied component may not be available in sufficient volumes.

It also creates strategic vulnerability. China controls substantial parts of the global commercial-drone supply chain and can restrict exports, alter pricing or prioritise other customers.

NATO armed forces have substantially less tolerance for Chinese-origin products.

The exact rules vary by country, but US military procurement in particular applies strict restrictions to Chinese airframes and critical components. Trusted-drone programmes require secure, NDAA-compliant products, and allied countries are increasingly seeking sovereign or trusted supply chains.

A Ukrainian product containing Chinese components may therefore be entirely suitable for immediate use in Ukraine but unacceptable to a NATO customer.

Replacing the components can increase cost, change performance and require substantial redesign and testing.

Supply-chain localisation is consequently both a barrier and a value-creation opportunity.

6. Ukrainian and non-Ukrainian producers

Continued

6.6 The combined model

The strongest future businesses may combine the advantages of both ecosystems.

Potential structures include joint ventures, technology licensing, co-development, contract manufacturing and production outside Ukraine.

Ukrainian and non-Ukrainian defence-tech producers

AREA	UKRAINIAN PRODUCERS	NON-UKRAINIAN PRODUCERS
Operational testing	Continuous battlefield access	Exercises, ranges and customer trials
Development speed	Often weeks or months	Commonly months or years
Product cost	Generally lower	Generally higher
Procurement	Brigades, central MoD, partners and NGOs	Ministries, frameworks and prime contractors
Order sizes	Small unit orders to very large state contracts	Generally larger but slower contracts
Chinese components	Often accepted due to price and availability	Frequently restricted or prohibited
Governance	Often developing	Generally more established
Certification	May be limited	Usually stronger
Physical risk	High	Lower
Market access	Strong in Ukraine	Stronger in NATO markets
Investor opportunity	Institutionalisation and internationalisation	Validation, cost reduction and procurement acceleration
Principal risk	War, governance and exportability	Valuation, cash consumption and slow orders

6. Ukrainian and non-Ukrainian producers

Continued

The objective should not be simply to relocate an existing Ukrainian product.

It should be to preserve Ukrainian speed, operational knowledge and cost discipline while adding trusted components, governance, scalable production, compliance and international sales capability.

7. The investor perspective

7.1 Investing in Ukrainian companies

Ukrainian companies may offer access to battle-tested technologies, experienced engineering teams, lower entry valuations and significant international revaluation potential.

The investment thesis is commonly based on transformation.

A company begins as a supplier to the Ukrainian war effort and develops into an internationally governed defence business with production, partnerships or sales outside Ukraine.

Value creation may come from improved governance, financial reporting, intellectual-property protection, production financing, trusted supply chains and access to NATO customers.

7.2 Investing in non-Ukrainian companies

Non-Ukrainian companies may offer easier due diligence, familiar corporate structures, better access to capital and established routes into defence procurement.

They nevertheless face substantial commercial risk.

A company may spend years completing development and certification without receiving a major contract. Procurement decisions can be delayed by budgets, political priorities and changing requirements.

The investor is therefore exchanging some Ukrainian geopolitical and governance risk for valuation, development and procurement risk.

7.3 Valuation

Defence-tech companies cannot be valued using one standard multiple.

7. The investor perspective

Continued

Relevant factors include product maturity, contracts, gross margin, customer concentration, software content, production capacity, market access and working-capital requirements.

A prototype company should not be valued like a scaled manufacturer.

A company with high revenue from emergency or charity-funded purchases may have less predictable future income than a smaller company embedded in a funded multi-year programme.

7.4 Revenue quality and funding source

The source of an order is central to revenue analysis.

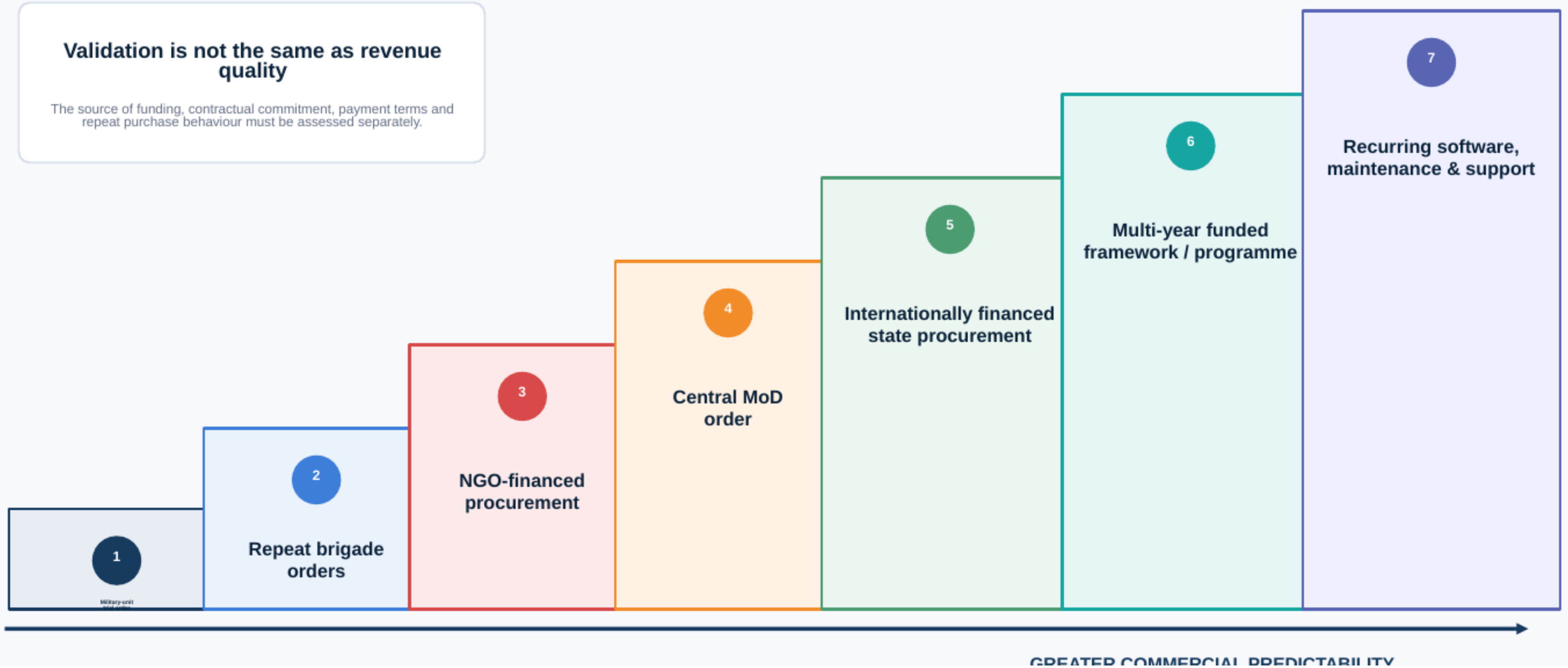
Ukrainian sales may be financed through direct brigade budgets, central Ministry of Defence procurement, the Danish Model or other partner programmes, foreign-government direct procurement, NGOs and charities, crowdfunding, grants and paid development programmes.

A small brigade order can be highly valuable as operational validation but may have limited financial significance.

An NGO-financed order can be substantial and commercially valid. It may nevertheless depend on a successful fundraising campaign rather than a recurring public budget.

Revenue quality and procurement maturity

Validation can arrive quickly; commercial predictability usually builds through repeated and funded procurement.



7. The investor perspective

Continued

A central Ministry of Defence contract may offer greater volume but still be subject to annual appropriations, delivery milestones and changing specifications.

Internationally financed orders may provide attractive payment security but depend on partner-country approvals and the continued availability of support programmes.

Investors should distinguish between pilot purchases, repeat unit orders, charity-funded purchases, framework agreements, committed minimum volumes, central state contracts, internationally financed programmes, grants, software and support revenues.

The key questions are who is legally responsible for payment, whether the funding is committed, how much volume is guaranteed and whether the customer has made repeat purchases.

7.5 Exit opportunities

Potential exits include sales to major defence contractors, mergers with specialist platforms, growth-equity recapitalisations and public listings.

Strategic value may reside in the company’s intellectual property, operational data, engineering team, customer access or production capacity.

Companies must therefore establish clear ownership of these assets before seeking institutional investment or an exit.

8. Demand after the war in Ukraine

8.1 Replenishment and rebuilding

An end to active hostilities would change the composition of demand but would not remove the underlying security requirement.

Ukraine and its partners will need to replenish inventories, rebuild military capacity and maintain deterrence.

European countries must also replace equipment transferred to Ukraine and correct capability gaps revealed by the war.

NATO’s 2035 expenditure commitments and EU defence initiatives extend beyond any near-term assumptions about the duration of active fighting.

8.2 Changes in military doctrine

The war has demonstrated that future forces require large inventories of reconnaissance and strike drones, electronic-warfare systems, resilient communications and autonomous logistics.

These capabilities will require permanent units, training, budgets and procurement processes.

They will no longer be treated merely as experimental equipment purchased for one conflict.

8.3 Continuous replacement rather than static stockpiles

Demand will also continue because many Defence 2.0 systems have short operational and technological lives.

A drone may be lost during its first mission. A reusable platform may become ineffective because a new countermeasure has been introduced.

Armed forces therefore need continuous access to current product generations.

8. Demand after the war in Ukraine

Continued

They cannot prepare for a future conflict by filling warehouses exclusively with today's fixed drone designs.

The more sustainable model combines a limited operational reserve with industrial capacity, modular components and rapidly updateable software.

This creates continuing demand for production, upgrades, components, maintenance and development even where the total number of systems required in active combat declines.

8.4 Continued technology competition

The cycle of measure and countermeasure will continue after the war.

Potential adversaries will continue to develop improved jamming, spoofing, autonomous navigation, drone swarms and counter-drone systems.

Current products will not remain effective indefinitely.

A defence-tech company must therefore continue investing in research and development after achieving initial product-market fit.

8.5 Civil-security demand

The diffusion of drone technology also creates security challenges beyond warfare.

Airports, public events, prisons, borders and critical infrastructure increasingly need the ability to detect and respond to unauthorised drones.

Subsea and remote infrastructure also requires autonomous monitoring and inspection.

These requirements will continue independently of the outcome of the war.

8. Demand after the war in Ukraine

Continued

8.6 Ukraine’s long-term industrial role

Ukraine has developed engineering talent, production capacity and operational knowledge on a scale that is unlikely to disappear.

After the war, Ukraine may become an exporter, manufacturing base, development partner and testing environment for European and allied defence companies.

Its success will depend on whether Ukrainian companies can meet international requirements for governance, trusted components, certification and service.

9. Why defence-tech is a new investment category

Defence-tech combines characteristics from software, industrial technology and deep tech.

It may resemble software because value is created through algorithms, data and updates. It resembles industrial technology because physical products require manufacturing, supply chains and working capital. It resembles deep tech because development may involve long periods of technical uncertainty and specialist engineering.

The sector also has distinct demand drivers.

Revenue is shaped by geopolitics, public budgets, military doctrine and changing threats rather than ordinary consumer demand.

The market remains fragmented, with up to approximately 2,000 Ukrainian manufacturers, companies and development teams under the broadest definition and a large international population of specialist SMEs and start-ups.

This fragmentation creates opportunities for consolidation, platform building, licensing and strategic acquisitions.

It also creates significant due-diligence requirements because many companies may have similar products, incomplete documentation and limited commercial histories.

Defence-tech is not a formal asset class. Investors obtain exposure through ordinary equity, venture capital, private equity, debt or listed securities.

It has nevertheless become a distinct investment category because it requires specialised knowledge of technology, procurement, regulation, industrialisation and geopolitical risk.

10. What investors should assess

Investors should begin with the customer problem rather than the sophistication of the technology.

The product must solve an operationally important and funded requirement. Evidence may include battlefield deployment, repeat orders, formal trials and measurable improvements in cost or performance.

Product maturity must then be established. A concept, prototype, field-tested product and scaled production system represent very different levels of risk.

Investor assessment framework

A technically impressive product is not sufficient: the company must also be producible, sellable and financeable.

10. What investors should assess

Continued

Cost-effectiveness must be considered in relation to the mission. A cheap system is not attractive if it fails under jamming. An expensive system may be justified if it protects a much more valuable asset.

The company's competitive advantage must also be identified. This may reside in software, data, manufacturing, system integration, customer access or continual development rather than a patent.

For companies claiming AI or autonomy, investors should establish which functions are actually autonomous, whether they have been tested and whether the company owns the relevant code and data.

Production diligence should cover output, component dependence, quality assurance, working capital and vulnerability to physical disruption.

Market-access diligence should cover procurement routes, export licences, trusted-component requirements and integration with larger systems.

Governance diligence should establish ownership, financial reporting, intellectual-property rights, compliance and decision-making structures.

Finally, the financing plan should link the capital raised to identifiable milestones such as certification, production expansion, delivery of a contract or entry into a new market.

11. Principal investment risks

11.1 Customer concentration

Many companies depend on one government, programme or military unit.

A change in budget, specification or political priority can have a significant effect on revenue.

11.2 Procurement risk

Government procurement can be slow, complex and politically influenced.

Operational interest or successful testing does not guarantee a production contract.

11.3 Technology obsolescence

A successful product may lose effectiveness when the opponent introduces new jamming, detection or interception methods.

The company’s ability to continue developing may therefore be more valuable than its current product.

11.4 Manufacturing risk

Rapid growth can reveal quality problems, supplier dependence and working-capital constraints that were not visible during prototyping.

Orders do not automatically translate into revenue or positive cash flow.

11.5 Regulation and export control

Defence and dual-use products may require export licences, security approvals, sanctions screening and end-user documentation.

11. Principal investment risks

Continued

Failure to comply can prevent delivery and expose the company and its investors to liability.

11.6 Intellectual-property risk

Ownership may be unclear where products have been developed by founders, contractors, military personnel, universities or volunteer initiatives.

Investors must confirm that the company owns or controls the assets on which its valuation depends.

11.7 Ethical and reputational risk

Investors have different policies regarding offensive weapons, autonomous systems and controversial weapon categories.

A clear investment policy should be established before individual opportunities are considered.

11.8 War, governance, corruption and integrity risk

Ukrainian investments involve direct war and country risks, including physical damage, loss of personnel, disruption of logistics, currency restrictions and difficulties enforcing contracts.

They may also involve governance and integrity risks.

Some businesses have developed very rapidly without institutional financial controls, independent boards or formal procurement procedures. Ownership structures, related-party transactions and payments to agents or intermediaries may require particular scrutiny.

Corruption remains a relevant risk in Ukraine, including within defence procurement, although Ukraine has also strengthened its digital procurement systems, anti-corruption institutions and compliance infrastructure.

11. Principal investment risks

Continued

The appropriate investor response is not to assume that all Ukrainian companies are affected by corruption. It is to conduct deeper diligence than might be required in a lower-risk jurisdiction.

Mitigation should include verification of ultimate beneficial ownership; background checks on founders, managers and key counterparties; review of political and military connections; sanctions and adverse-media screening; forensic accounting; reconciliation of procurement contracts, deliveries and bank payments; review of related-party transactions; verification of intellectual-property ownership; investigation of agents, distributors and intermediaries; anti-bribery policies and contractual protections; and continuing audit and compliance rights.

Forensic work is particularly important where historical financial statements are incomplete, cash transactions have been used or reported margins appear inconsistent with procurement prices.

Strong due diligence cannot eliminate war or corruption risk, but it can distinguish institutionalisable companies from businesses whose valuation depends on unverifiable relationships or transactions.

12. Conclusion

Defence-tech has become a distinct investment category because the structure of modern warfare and defence procurement is changing.

The central development is the rise of comparatively affordable, mass-producible unmanned systems.

These platforms distribute surveillance, strike, logistics and protection across far greater numbers of systems than traditional defence economics normally permits.

They have also created the drone-dominated kill zone.

Persistent surveillance and low-cost strike systems now expose personnel and vehicles long before they reach the conventional frontline. Tanks and other Defence 1.0 platforms remain important, but their traditional employment has become increasingly difficult without drones, electronic warfare, counter-drone protection and rapid command systems.

Artificial intelligence and autonomy are becoming essential because mass cannot be controlled manually.

Armed forces cannot provide a separate operator for every drone, maintain uninterrupted communications or process every sensor feed with human analysts. AI is also required if drones are to operate as coordinated swarms rather than isolated platforms.

Russia’s full-scale invasion in February 2022 accelerated this transformation and made defence-tech critical to Ukraine’s continued defence.

Ukraine has built a broad ecosystem that may comprise up to approximately 2,000 manufacturers, companies and development teams, depending on definition. The ecosystem is supported by direct brigade budgets, central Ministry of Defence procurement, international programmes such as the Danish Model and NGO-funded purchases.

12. Conclusion

Continued

This procurement structure provides rapid market access but creates different levels of revenue quality. A small brigade order may provide strong validation but limited predictability. A large Ministry of Defence or internationally financed contract may support industrial scale. An NGO order may be substantial but depend on future fundraising.

Ukraine also illustrates the importance of cost and supply chains.

Chinese-origin products and components have been widely used because they offer the lowest prices and immediate availability. NATO customers generally have significantly lower tolerance for Chinese critical components because of cybersecurity and strategic-dependency concerns.

Internationalisation therefore requires more than exporting the Ukrainian product. It may require redesigning the supply chain, documenting the system, strengthening governance and establishing production outside Ukraine.

Demand will continue after the war.

Inventories must be rebuilt, military doctrine is changing and European forces need permanent drone, counter-drone, electronic-warfare and autonomous capabilities.

Fast-changing defence-tech products cannot simply be purchased today and warehoused for a future conflict. Readiness will depend increasingly on flexible production capacity, modular products and the ability to update systems continuously.

The strongest investment opportunities may arise where Ukrainian operational knowledge and cost discipline are combined with international governance, trusted supply chains, capital and market access.

The companies most likely to create sustainable value will not necessarily be those with the most advanced current product.

12. Conclusion

Continued

They will be those capable of adapting as threats change; producing at an economically sustainable cost; controlling critical technology and data; navigating different procurement channels; complying with international requirements; and building governance that can withstand institutional due diligence.

Defence-tech's long-term attractiveness is based on structural demand, rapid technological change, industrial fragmentation and the need for private capital.

Its risks arise from the same characteristics.

Understanding both sides is what distinguishes defence-tech investment from general exposure to the traditional defence industry.

Data and terminology note

The term defence-tech has no universally accepted statistical definition.

Market figures frequently combine traditional defence, cybersecurity, aerospace, artificial intelligence, dual-use technology and civil security.

The financial figures used in this Insight also measure different concepts:

- defence expenditure;
- investment expenditure;
- procurement budgets;
- contracted order values;
- delivered quantities;
- production capacity;
- NGO-financed purchases.

12. Conclusion

Continued

They should not be aggregated without considering their definitions.

The estimate of up to approximately 2,000 Ukrainian manufacturers, companies and development teams is an indicative ecosystem range. It includes different types of organisations and may involve overlap between official manufacturer counts, start-ups and development teams.

Product-price illustrations are based on publicly disclosed contract values and may include spares, support, training, testing and production investment. They should be treated as indicative orders of magnitude rather than standard unit prices.

A Specialised Corporate Finance Partner for Defence-Tech

Kapital Partner is a specialised corporate finance partner for small-cap companies and investors.

Based in the Nordic region—one of Europe’s leading technology environments and a major contributor to Ukraine’s defence—Kapital Partner combines extensive small-cap finance and growth-IPO experience with expertise in direct listings, strong knowledge of defence-tech markets and an international and Ukrainian network supporting defence-tech companies and investors alike.

This combination gives Kapital Partner a distinctive position at the intersection of defence technology, capital and public markets.

Kapital Partner Insights

Kapital Partner Insights provides analysis of investment, financing, capital raising, IPOs, direct listings, stock markets and corporate actions.

The platform will increasingly cover defence-tech investment, Ukrainian and international defence-tech companies, market development, procurement, scaling, funding and public-market opportunities.

READ KAPITAL PARTNER INSIGHTS

https://kapitalpartner.dk/en/insights/

SIGN UP FOR KAPITAL PARTNER NEWS

https://kapitalpartner.dk/en/newsletters/

Receive new Insights, investment opportunities, IPO updates and other Kapital Partner news directly.

KAPITAL | PARTNER

Defence-Tech Contact

JESPER ILSØE

Partner and Kapital Partner’s go-to contact for defence-tech

ji@kapitalpartner.dk

+45 26 80 27 28

https://kapitalpartner.dk/en/