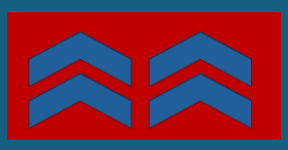
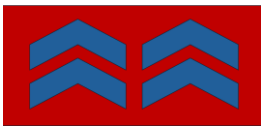
The integrated battlefield

Diana Popa

Red Sky 4



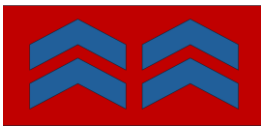
www.redsky4.nl



© Red Sky 4, 2026

Popa, Diana (2026). The integrated battlefield.

Table of Contents



Executive summary

The paradox of the integrated battlefield is that while it is made transparent by its digitalisation, it expands to sizes or territories that make it extremely difficult and resource intensive to keep in constant overview. The perimeter of the integrated battlefield expands, requiring a constant flow of resources to monitor it and to enable timely responses and decisions. The battlefield thus turns into an eco-system, where drones, satellites and maritime autonomous systems create a technological network in which sensors, communications channels and effector systems complement each other (Wennink, 2025). The integrated battlefield is an elongation of the front lines in terms of technological development and deployment, with encounters with the enemy's technology and lateral technological encounters being needed for driving development further at exponential speed. This integration is resource intensive, especially for the deployer defending the home front, who needs to add the management and logistical chains for the deployment and development of the novel technologies to its war effort. The battlefield in Ukraine thus provides a unique testing ground for emerging technology and shortens innovation cycles, allowing for cascading incorporation of results in Western armies. Faster deployment of technology to the end users on the front lines is wanted, needed and undertaken, weather in the physical or digital battlefield. With the growing manifestation and overlapping effects of grey warfare, cyber-attacks and geopolitical re-alignments disrupting supply chains, autonomy in the technological and digital space becomes one element of the integrated battlefield that increases state defence capabilities.

Introduction

The world as we see it today presents multiple hot conflicts, some that turned from cold to hot and others that manifested directly as hot conflict without public awareness over potential build-up of tensions. The multiplication of global conflicts is not uniform in terms of immediate regional or global impact, that is to say some conflicts have wider geographical impact in multiple domains: military, technological, economic, political or social, while others have a narrower impact. The increase in number of conflict points has triggered the increase of defence spending and defence procurement, and made vulnerabilities such as dependency on external parties visible. In the same time, security and defence technologies determine the stability in this world of increasing geopolitical tensions (Wennink, 2025). The war in Ukraine and proximity of the hot conflict have determined an uptake in defence readiness initiatives and defence posturing in Europe. Incursions into NATO airspace and drone incidents have ramped up national and regional defence initiatives. Yet in terms of defence production, the defence industry suffers from a reaction lag, requiring time to scale up capacity, even more so when required to produce at scale alternatives for what it previously imported. With concomitant conflicts flaring up globally, large defence manufacturers have a longer and longer backlog of orders, especially in the case of exquisite systems. Reports of lead manufacturers in the defence sector such as SAAB (2025, a) attest to this: a backlog increase of 35% in 2025 compared to 2024, a 14% increase foreseen for 2026 and a 23% foreseen increase in 2027 (SAAB, 2025, b). The increased backlog volume on weapons system production is observed across different segments (aeronautics, dynamics, surveillance, submarines) is one indicator of unbalance between the reaction time and production span of the defence sector in relation to increasing threat levels.

Defence procurement slows down speed of decision and action, further exacerbating delays in contracting brought forward by the fact that increasing volumes of orders placed simultaneously by many states with large defence manufacturers increase backlogs and further delay delivery times. Delivery deadlines of contracts for defence products are often exceeded, reflecting also perhaps a lack of urgency or a mentality still functioning in a perceived peace environment, focused on long term stockpiling and deterrence not immediate consumption. Cultures and methods of defence procurement must change with attention shifting towards the start of the process and with different types of procurement being adopted. Initiatives include short cycle acquisition processes. An accelerated procurement process is observed in the case of material acquisition for Ukraine in the “Task Force Ukraine”, where reallocation of budget to following year is not possible, thus requiring simultaneous fast processing of orders and rigorousness (Ministry of Defence, 2025).

The degree of centralisation at government level and in the procurement processes influences the length of the procurement processes. Of note here are reports from Ukraine, where decentralisation of procurement at unit level was implemented as means to quicken deliveries to the personnel at ground deployment level. The defence market thus observes decentralisation and flattening. This can have opposing, antagonistic effects: on the one hand it could lead to

diminished real time overview by national governments and international defence structures on weapons and defence capabilities stockpiles. On the other, the procurement and data ecosystem such as the Brave1 platform observed in Ukraine in which developers, deployers on the battlefield and the government feed and extract data and feedback from the same system shortens procurement processes and innovation cycles (Howe, 2026).

The defence industry has thus seen a consistent revival in the last years, but what is more pronounced is the privatisation of the industry. Defence industry related events expand in occurrences and size, worldwide private developers showcasing their technical solutions in large pavilions, indicating that the defence industry is more and more resembling the free market than the centralised government directed functioning (Popa, 2025, b). Even if regional in their umbrella, these defence events are attended by defence developers and manufacturers from all over the world. The national defence industry thus serves not only financial and diplomatic objectives, but it also becomes a way of signalling capability and posturing by the sheer presence at such international specialized events. The ecosystem of the defence sector is present at such events, from government officials explaining policy lines and observed geopolitical trends, military specialists, researchers and media to developers of different sizes. This market transformation observes risks if leading to lack of control over stocks of weapons, while for governments it can serve as a mechanism of unblocking procurement processes caused by bottlenecks and backlogs.

The matter of opportunity costs for increasing defence spendings and reaching the targeted of 5% of expenditure as aimed for at NATO level have determined national discussions on the associated costs for the population, including increasing taxes or redirecting funds from internal / national oriented spending such as health or social care, with reverberations in the political domain. The 5% NATO wide defence spending target was long negotiated, with states like Spain receiving exemptions. Dividing the total percentage in 3.5% dedicated to core spending and 1.5& for additional or lateral activities and purposes such as infrastructure supporting defence can be labelled as an artifice making commitment faster and implementation easier within national budgets. This facilitates answering questions regarding what is considered defence spending, from building or consolidating bridges to measures for increasing population resilience.

Not least, national regional defence structures face multiple challenges when aiming to collaboratively take on similar defence goals:

- Outdated (national) legislation that is not suited for conflict or wartime decision making;
- Political stakes and political instability influencing decisions on contracting, collaborations and suppliers in the technology and defence fields;
- Specific national needs and backgrounds inducing differences in priorities and solutions for redirecting more funds to defence (tax increases, redirecting from education, social and health care).

The cyber space

The transposition of kinetic conflicts into the cyber domain has brought the enemy on one's own virtual territory and thus extended the sense of the battlefield. No longer is war or conflict bound to a clear contact line. The modern warfare is fought as much in the cyber space as in the physical one and the digital impulse can be the difference between peace and conflict (Commission for Defence, 2026). States are therefore upscaling their cyber defensive and offensive programmes and capacities.

Technology itself is being weaponised in more ways than one:

- in itself, in terms of capabilities and supremacy, that more obvious in the defence field;
- in terms of dependencies from external suppliers in absolute terms but also only in specific parts of the supply chain (for example software updates that are periodically needed for exquisite systems such as F35 platforms);
- in terms of the vulnerabilities that deployed technologies bring with themselves when obtained from external supplier or when vulnerable to attacks;
- in terms of the overall vulnerability introduced in the system through the volume of usage of the given technology, the level of overall resilience of the system.

Given data sensibility, the defence sector observes additional risks in the cyber domain if having to rely on third party data, with the potential to endanger operational security. Relying on systems that require periodical software updates has inherent vulnerabilities, either of vendor lock-ins or of loss of access to the asset or system. On the battlefield, (origin of) the supplier of deployed standard or commercial drones influences the choice of installing or not installing the software updates of the developer.

On the background of permanent rivalry, actors aggressively deploy their cyber capabilities in order to reach their strategic goals (Dutch Minister of Defence and Dutch State Secretary of Defence, 2026). The enemy is looking for the weakest point to enter the system. As such, in an interconnected system the weakest link becomes the vulnerability point for the entire system. This in turn determines what information is shared between partners in that system, seen risks of spillover effects of any breach. Interconnectivity across military alliances such as NATO incurs the risk of affecting the entire system (in different degrees even if just through second or third order effects), with the weakest link in the chain becoming the exploited vulnerability. NATO exercises its cyber capacity among partners in structures such as the Cyber coalition, while in the same time members with more advanced cyber capacity help other states with less cyber capacity (Dutch Minister of Defence, Commission for Defence, 2026).

The Netherlands has developed a programme for cyber – reservists and dedicated programs such as the Cyber Academy Cyber reservists need to keep up to date in the cyber domain and work on issues and challenges that are not available in the private domain. This is the advantage of having such a bridge and represents the additional motivation for participants. The latest Dutch Defence Cybersecurity strategy (2025) focuses in a greater extent than the previous

versions on cyber offensive activities, thus signalling a change in the defensive posture, with more focus on the forward defence in the cyber domain, as well as signalling capacity to enemies as forms of deterrence. Given the acute level of threats in the cyber space, the observing of aggressive behaviour, penetration and sabotage attempts of state and non-state malign actors, there is a high pressure on contra-intelligence and defence organisations towards position taking. Having been the host of the NATO top in the summer of 2025, the Netherlands had to build a strong cyber shield in anticipation for being a target of cyber-attacks, thus testing and developing its cyber capabilities in a real scenario.

Technological developed states and markets face specific challenges, being interesting points of attention for both benign foreign investors and malign actors. Digitally advanced societies are more vulnerable to disruptions facilitated by cyber-attacks, especially there where there is no clear perception on the existing threat ("far from by bed" perspective) or where there are no analogue redundancies. As such, the strive for digital and technological autonomy becomes imperative.

Sovereignty over digital and technical capabilities

Autonomy in the digital space in the defence sector is a multi-layer, multi construct phenomenon. Autonomy needs to be present at different layers within the system, from operations, swarming technology, communication and connectivity – and availability of 5G or 6 G network, up to the practical stages of decision making and target selection. Different investments are needed for each of these phases and layers, and thus priorities must be set in terms of country profile specialisation and investments, depending on the state of the art status of the respective segment and envisioned medium to long term strategy. While interdependency has long been hailed as a means of preserving peace and balance of power, and has proven economically advantageous, the recent observed threat levels and potential system vulnerabilities due to vendor lock-ins and backdoors have called for consolidating and striving for reaching digital and technological autonomy. Reliance on proprietary or open source solutions still gives rise to discussions in terms of risks and advantages for both, such as the risk of vendor lock in for the former category and speed of update and fast system patches for the latter with risks of backdoor unwanted access due to known vulnerabilities. Examples of incorporated mitigation measures include he use by Palantir (much debated in technology developers and policy makers circles) of an open standard allowing for users to analyse the code serve as reassurance measures.

Because digital and technological autonomy is a comprehensive, multilayered construct, that is time and resource intensive, sudden break away from existing suppliers and solutions can be costly, technically challenging to say the least, and have wider geopolitical consequences, in a series of tit for tat moves. It becomes thus more sound that parallel processes are undertaken,

for consolidating comprehensive 360° autonomy while having the lead in a sector according to country specialization profile. Reaching sovereignty is an agency driven continuous exercise of practicing free will and making hard choices. Sovereignty is thus a constructed result, requiring manifestation at different levels in order to reach realisation. These levels and corresponding choices are reflected in cloud policy, IT acquisitions, continuous investments in knowledge and capacity training. Aiming to have better technology than that of the enemy is not enough, one must as well have the operational experience on how to best operate that technology on the battlefield, thus deployment in operational settings is needed for skills development.

The question of sovereignty in the digital and technological space has been high on the Dutch Governments agenda in the first month of 2026, in continuation to discussions taking place in the previous year on the dossiers of Nexperia, the technology and weapons deliveries to Israel (Popa, 2025) and older discussions in defence, political and technology circles on the need for departing from the dependency risk and vulnerabilities of using digital solutions that fall under the US Cloud Act, especially for critical systems and sensitive data. The risks that would be incurred by the potential inclusion of the DigiD system under this act is a particular urgent topic, as it is used as centralized login to most public services by the Dutch population. This trend in focus presents more than a time consistency in terms or positioning, observing an exponential growth in volume, urgency of discussions and acute character of implementation of proposed measures. Reflecting this trend, in the new Dutch cabinet formed in the first months of 2026, digital autonomy is a distinctive element of the ministerial portfolio.

France shows faster adaptation and implementation of sovereign digital and technological systems in response to warnings given by her intelligence services (Giraud, G, in Schaduwoorlog, 2026). This can come as result of observations made over the changing nature of conflict and threats posed to one's own society and national interests. Resistance or pushback from past of current technology suppliers is well anticipated but should not serve as a factors of influencing strategic choices. Often, large technology and cloud providers have the backing of their governments, bringing the technology issue in the geopolitical arena. Acknowledging domino effects and their costs, and the difficult and costly process of exiting existing lock-ins, governments need to engage in multilayered strategies for reaching the 360° level of digital and technological autonomy, while finding the resources needed for temporarily sustaining parallel streams of solutions until autonomy is reached or sustaining the costs and potential system effects of a sudden break from existing solutions.

Drone warfare and consolidation of air defence lines

Developing different types of counter-drone capacities is one of the main focuses for NATO countries and Ukraine alike, yet with different types of urgency, size and intensity of faced

attacks. In Europe, the Netherlands has own national drone and counter-drone capacity and development programmes, with one of the highest investment proposal values in the sector - 1 milliard euros (Wennink, 2025). Despite these investment, Europe is still behind the US and China in terms of operational capacity and investments in the counter-drone and space sectors (Wennink, 2025). These present challenges can be systematically addressed through strengthening the Dutch daring capital ecosystem by means of high risk investments (Wennink, 2025). The national drone programme is not developed in its singularity, but rather is integrated in a comprehensive 360° defence strategy. This drone ecosystem is embedded within a larger ecosystem of sensors and data processing capacity, addressing air, land and see defence. It is not unreasonable to say that accent on drone capacity development was transferred from observing the potential and effects of the technology in theatres such as Ukraine, where deployment drives development.

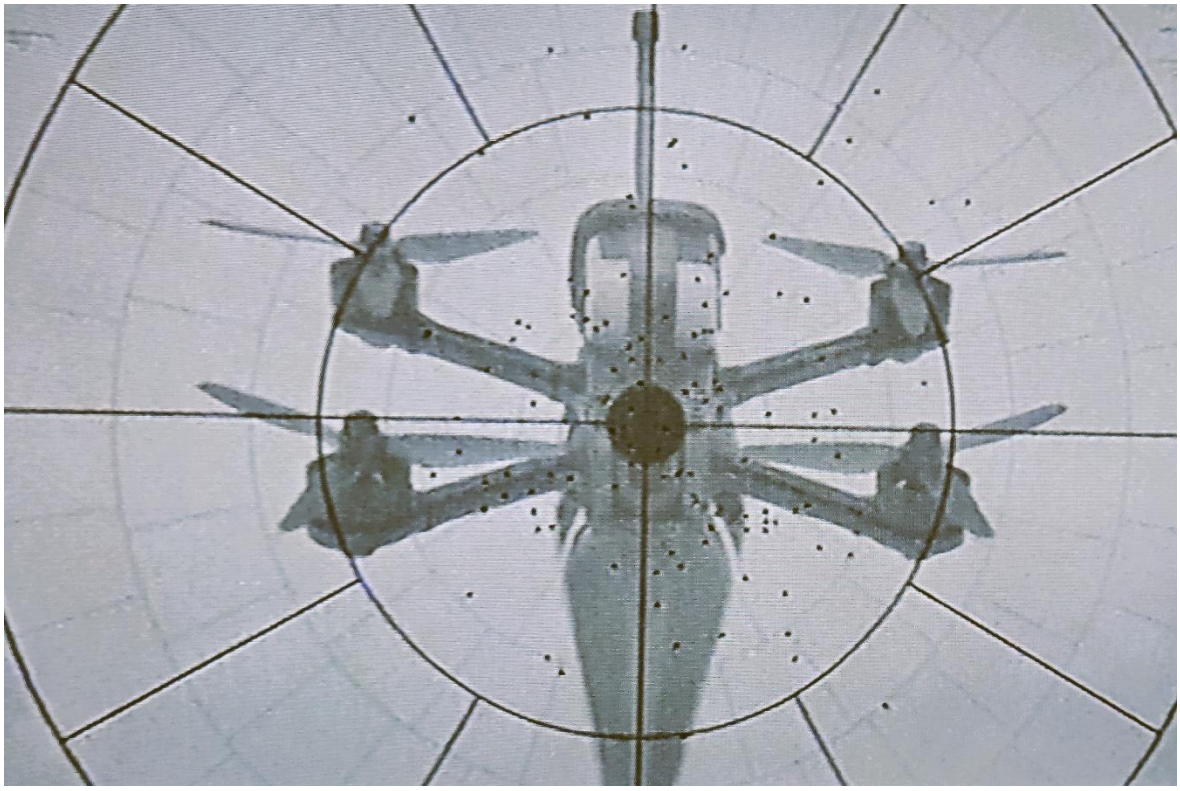
Worries have been expressed about Western deliveries of drone technology and other military goods to Ukraine being a way to circumvent Western regulation on export control, given the laxer legislation on the subject in the case of Ukraine. In the same time, due to differences in legislation, it is precisely why technology is being tested and developed on the battlefields in Ukraine, with general interest in extracting the knowledge and knowhow from the field and afterwards testing it in terms compatibility and potential for integration in own systems. What is of interest here is not only the potential for transfer of knowledge and know how, that could be limited by existing constraints in one's own system under normal conditions, but knowing what the potential of the technology really is and how it *could* be deployed if and when wanted and the effects of multilateral interaction.

Counter-drone measures rely heavily on deployment of electronic warfare. Kinetic counter-drone measures include the dynamic deployment of netting to stop drone advancement and, on the front lines - ultimately releasing live fire at the advancing drone when it comes in shooting range. Fixed anti-drone protection measures of large objectives include instalments of anti-drone netting, either hard or soft, for example in the case of vehicles on the front line, or soft over entrance to blindages or check points or over road infrastructure.

2025 has seen several drone incidents across the European space, not only in the vicinity of the Russian and Ukrainian borders. Counter-drone technology is being developed and marketed for specific protection of the homeland, meaning protection against attacks or threats to critical infrastructure and high value targets such as airports. Reportedly the drone incidents in Europe have lead to the manifestation of panic reactions in the public found in the vicinity of the incident.

The perception of drones is however heavily influenced by the nature and volume of interactions between user or impacted individual and the technology or representative unit of the technology itself. As a technology deployed in peace time and on territory not affected by general scale conflict, drone technology is deployed and embraced as instrument for solving or optimizing a certain problem or recreative purposes and its development is largely driven by scientific drive. A different stance altogether is observed in relation to drone technology in a

territory affected by a war heavily reliant on the attack capabilities enabled by drones, as is the case in Ukraine. Not denying non-kinetic use such as reconnaissance, the very concept of "drone" is associated with the potential of attack with different sizes of payloads and corresponding impact or damage. While special shotguns such as the Safari are incorporated in counter-drone arsenal in Ukraine, on the front lines, given spread and number of deployed units on the contact lines, taking down a drone with live ammunition from the weapon in the standard individual combat equipment becomes a necessary skill. In a 1x1 interaction, in close contact, when hiding is not possible, firing at the drone becomes the last line of defence.



Drones as shooting targets.
Source: The Author

Video footage from the battlefield of drone strikes often show instinctual "ducking" behaviour of the target, indicating awareness of low chances of efficient countermeasure once in close range of the drone and in open space. This internalised behaviour is individually developed through previous observation and experimentation. Being present for long periods of time in an environment constantly occupied by drones develops instinctual reactions towards sound stimulants associated with drones. Observing the effect of drone attacks first hand and having so called *close calls* further internalized and automatizes reactions to visual and sound indicators of drone presence. This 1x1 interaction between on the ground combatant and drone introduces an uneven balance, in terms of speed, reaction speed and size of damage in relation

to size and chances of survival. Experiences accumulating in time and volume transform in generalised perceptions towards the deployment of drones, depending on which side of the drone deployment process one was. Opposite reactions have been observed: virtual immersion via technology has been reported to have an effect of detachment on combatants deploying the technology on the battlefield. In the same time development of PTSD syndrome in drone pilots that operate away from the battlefield has been reported, indicating pilots are still subjected to psychological and moral consequences of combat. From a different perspective, this delocalisation of combatants, as is the case of drone pilots, raises questions regarding the definition of veteran and its associated (legal) implications .

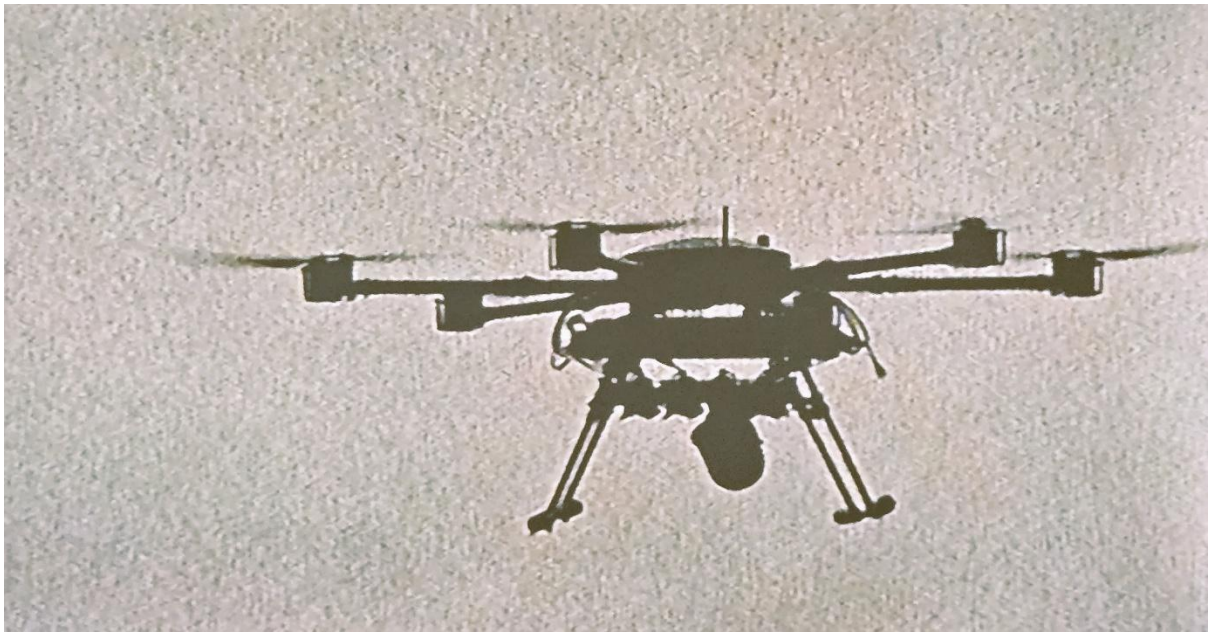
Drones have the potential to trigger strong emotional reactions following immersions in the virtual environment used for controlling them or in the physical environment they impact. While defence specialists observing the potential of the technology deployed on the ground in Ukraine want to integrate the benefits of drone technology in their own strategies for protecting the lives of their own troops and maximizing enemy damage, the need to address the inescapable negative effects of combatants being (repeatedly) confronted with such direct encounters is stringent. While size of army and overall defence investments and capabilities can influence the number of one's own fighters coming under direct drone threat, the challenge of preventing the effects of repeated exposure remains the same.

In terms of permanentizing of anti-drone measures, developments are observed. Land defence structures by means of systems of multiple lines comprising of dragon's teeth, bob wire and trench systems are installed in anticipation of kinetic action and as a means of demarketing permanentizing of contact lines. The Eastern front in Ukraine observes consolidation of both land and air lines of defence, with the novel character of seeing permanentizing of anti drone systems. As recent as the beginning of 2026, anti-drone nettings are being installed in the Kharkiv region above the main roads in large sections (Mezha, 2025; Terajima, 2026) indicating the need for long term defence against attacks from the air of critical roads and suggesting expectancy of continuation of threats from above. Reports on enemy enhancing its targeting range by installing Starlink terminals on drones and using "mother ship" type of drones to penetrate territory and launch smaller attack drones are examples of developing tactics that present new challenges in terms of countering capabilities.

Degrees of technological complexity and responsibility

The more complex the technology, the more complex discussions on accountability borders become. It has been the case with autonomous systems – exemplified by the 2018 voting of the European Parliament on the ban of using "killer robots" on European soil.

Responsibility for using current day military technologies is complex and often diffused within the system in terms of steps taken before the technology is deployed in a real life combat situation. Often this comes in the form of the double pair of eyes principle, where multiple checks are infused in the system or process itself for safety reasons. This principle also diffuses responsibility among different actors. The overarching legal and ethical implications of using drones in the modern warfare are still being explored due to unanticipated cumulative and long term effects and field adjustments. Drone deployment on the battlefield more often than not requires more than one person. Segmenting the process of preparing the drone for flight with explosive payload, targeting and dropping into distinct steps, conducted by different persons, is such a way of diffusing attribution, although done for much more practical reasons. As is the case with larger system, the setting of the explosive charge on the drone is often conducted by someone else than the pilot who eventually decides the moment of the drop, thus diffusing the attribution process. While in the case of larger systems or exquisites this might be a necessity, in the case of offensive drones with one discharge this can be an assumed choice.



Vampire type drone.
Source: The Author.

AI on the battlefield

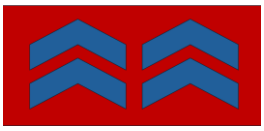
It has been previously noted that there are few available reports on the deployment of Artificial Intelligence (AI) in active conflict areas (Klonowska; Kwik, 2026). This should not come as a surprise, since in conflict, indication of capabilities gives away strategic advantages with

immediate impact on the battlefield. In active and contested conflicts, deployment of disruptive or emerging technology is tested in terms of technical limits and impact on the enemy, in terms of inflicted damage. Due to overlapping layers of complexity, from the technology itself – the often mentioned "black box effects", the environment of deployment and unanticipated cumulative effects from interacting variables, testing the extent of compatibility with existing international principles is most pertinently done post factum. Most available studies on AI in the military realm rely on OSINT for their inferences and analysis. It is mostly this etic or outsider approach that has the additional focus of testing the extent of the compatibility of development and deployment with existing international or deployment specific principles, and vice versa: testing the comprehensive or obsolete character of existing principles and frameworks. One also notes that legality is context bound and international exercises for affirming exercised legality during conflict has never been without contestation. Opaqueness of AI solutions developed and deployed during martial law or in conflict areas are a reflection of the concrete objective for which they are deployed and the time needed to test and adapt the technology in a multidirectional way (technical, operational, conceptual and in terms of governing frameworks), while reflecting the focus of saving own (human) resources and inflicting damage on the enemy directly in the case of AI enabled attack drones or indirectly, in the case of reconnaissance drones.

Artificial Intelligence is reportedly being used on the battlefield by both Ukrainian and Russian armies in the end phase of munition directing in order to circumvent electronic jamming. This trend has the potential to further develop into different forms of automatization, including target selection automatization and decision making on the battlefield. Observing developments form the battlefield, European developers warn that swarming capability is only a few months away from becoming reality (Commission for Defence, Dutch House of Representatives, 2026). This is again an example of war conditions and necessity enabling innovation at greater speed and surpassing limitations imposed by peace time agreements on technology development and deployment.

While international agreements are in place regarding the responsible use of AI in the military domain (REAIM), there is no bounding international legislation covering AI deployment in the military domain. Due to multiple layers of black box effects of the technology streaming from its intrinsic characteristics and its unanticipated results when interacting with and deployed in new contexts, there are no catch–all governing frameworks. Development of technology during martial law favours battle testing the technology in terms of capabilities and limits. Against this, prioritization of the requirements of review and verification seems antagonistic if being a matter of quantifying impact and scale of gains. In practical terms, spiral development or development while in service is now being implemented in different areas of defence by Ministries of Defence, especially in the case of technology with a short span before becoming obsolete such as is the case of smart drones.

National procurement programms for Ukraine and public-private R&D programms feed input from different national and international streams into the front line battlefield testing. This is a



cascading approach, with technology from different or stringed systems being pushed to the front end for testing on the battlefield, feedback being incorporated in short innovation cycles on the battlefield and streaming back to the corresponding development path. In this, the battlefield benefits from multiple innovation streams while it can also suffer overload of alternative solutions, needing resources to test alternative solutions. If integrated, these parallel and overlapping streams of solutions can also present the risk of system pollution via the weakest link.

Developers of AI enabled technology (drones included) in the defence sector need and want to test their technologies against real war conditions for testing robustness of technology. These grounds are scarce and access is negotiated within geopolitical alliances. Entering this space thus becomes a competition for developers. While the receiving country benefits from consolidated materiel flowing in, it also needs to adjust own policies for integrating and accommodating the deployment of the technology. Battleground testing needs to consider impact on operational efficiency. While it is in the interest of the developer to test the technology, the interest of the deployer (such as the unit commander) is the success of the operation. It leads then to a fine balancing exercise in accommodating these two elements simultaneously, while engaging with enemy forces.

Technology deliveries are therefore not a one step process. They require feedback integration in order to keep the innovation loop and resources allocation for testing, integration, maintenance or user training. The frontline thus projects backwards into a wider technology integrated battlefield, while the integrated technological battlefield sees a multi stream push to the front end where technology is tested against that of the enemy as well as laterally.

Through contact with the enemy, technology develops and adapts. Contact with the enemy is therefore essential for developing both capabilities and countering measures. This is a reciprocal process: by consecutive contact, the enemy also comes to understand capabilities and techniques and strategies and adapts its systems accordingly. Both interaction with the enemy's technology and lateral interaction and integration of solutions lead to achieving technological superiority faster. Specificities of regional frontlines or segments in the frontline observing different needs and deployment of troops and materiel allow for distribution of solutions and can aid to de-clutter a certain region of interest. This requires again streamlining of logistics, procurement and allocation processes and resources of existing and incoming solutions.

This forward projecting procurement and innovation cycle leads to increased speed of technology development, which, when considering its main purpose of deployment on the battlefield, increases and spreads levels of lethality, turning regional capabilities to global capabilities.

While positioning of developers close to the deployment level enables shorter innovation cycles for a wide range of technologies, the same is valid in the case of fielding of AI. It's important to have public – private developers who work close to the ground deployment level

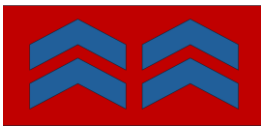
in order to develop the technology in line with user and mission requirements. Companies who have access to the operators deploying the technology have a better insight into the needs of the user, the existing limitations and state of the art of the fielded technology and thus can better and faster develop their product. If technology from producers outside of Europe is fielded in Ukraine, those developers will also benefit from the advancements on the battlefield, thus further increasing the gap in knowledge and knowhow between European and non-European tech developers. Maintaining self-imposed restrictions at European level in terms of governing frameworks over technological development can prove to be not on the interest of the state if it allows for knowledge and capacity gap enlargement.

Foresight scenarios

Paradoxically, a ceasefire in Ukraine can lead to Russia's shift in focus and capabilities towards Europe as a main target for disruption while stocking up on hard military capabilities. Experts anticipate that a ceasefire could see the disengagement from the formal combatant status of large numbers of combat hardened individuals who will represent a challenge for the government in terms of re-integration. Western experts thus anticipate that a large part of these individuals could be sent into Europe as elements of disruption, changing the intensity of the grey zone war activities on European soil. This will observe an overlap of the malign activities conducted in the cyber space with the ground presence of elements of destabilisation or infiltration increasing in intensity.

The integrated battlefield is thus not only expanded due to interconnectivity and digitalisation and made transparent due to technology with eyes in the sky, on land and water, it also widens by means of dilution, penetrating the very fabric of society. An increase of number and intensity of conflicts is already being observed worldwide, with strong elements of political disruption and social unrest. With conflict becoming more insidious, the security challenges will continue for European agencies tasked with the security of territory, population and national interests. Population resilience towards both active and passive forms of conflict is increasingly needed. Exponential increase of *comprehensive* defence capabilities is sine qua non for maintaining European security, autonomy, preserving values and way of life.

Recently the European public was faced with the question of fighting now and contributing toward the defence of Ukraine or having their children fight and potentially die tomorrow. Such questions and the new dilemmas that technological capabilities on the battlefield bring, force for a reopening of evaluations of principles that we have long considered to be set or clarified, given conditions of peace and prosperity. For the general public, awareness about increasing threat levels and need for upscaling overall defence capabilities must be raised gradually, an element that is crucially at this stage. In the same time, politicians are faced with hard choices on foreign policy issues, have to bare political costs and face public inquiry when uncomfortable choices have to be made. What can negatively affect overall defence capacity



and long term contracting in the defence sector is the weighing in of political interests against military interests. This is why, despite the fact that technology trade and diplomacy are more and more often intertwined, separation of power and decision flows is needed. Given the time lag between needed political choices and public assimilation of changing circumstances or setting of public sentiment, in the defence domain, waiting for overall general support undermines own interest. Public sentiment changes unevenly and even when changes occur, it might only ephemerally be so. A final example of shifting public opinion in relation to defence is the position of public universities engaging in R&D projects with or for the defence sector, as entities that have the pulse of socially sanctioned attitude towards science (and thus civilian participation) for defence purposes. In the Netherlands, the position of universities engaging in R&D activities with and for the military sector has also seen permutations, with support growing steadfast.

References

Howe, B. (2026). *Ukraine's Brave1 Market allows for suppliers to track kit performanc*e. DSEI gateway News.

Klonowska, K.; Kwik, J. (2026) *Artificial intelligence in contemporary conflicts and the future of military law* in Ducheine, P. Gill, T.; Pijpers P.; Zannenburg M. (Eds). *A research agenda for militray law.* Elgaronline.

Ministry of Defence (2025). *Inkoopen voor Oekraine*. Magazine.defensie.nl/materieelgezien/2025/07/inkopen-voor-oekraine

Minister of Defence and State Secretary of Defence (2026). *BRIEF VAN DE MINISTER EN STAATSSECRETARIS VAN DEFENSIE* Aan de Voorzitter van de Tweede Kamer der Staten-Generaal, 26 643.

Mezha (2025). *Anti-drone nets installation* Expands in Kharkiv Region.

Popa, D. (2025, a). *Strategic relevance through technological & digital sovereignty in times of geopolitical instability*. Red Sky 4.

Popa, D. M. (2025, b). *Mapping defence, security and resilience trends and perceptions*. Red Sky 4.

SAAB (2025, a). *Delivering sustained growth. Q3. Interim Report 2025*. Available at: https://www.saab.com/globalassets/cision/documents/2025/20251024-saab-q3-2025-results-delivering-sustained-growth-en-0-5239456.pdf

SAAB (2025, b). *Saab Q3 2025* Presentation. Available at: https://www.saab.com/investors/webcast/q3-2025

Schaduwoorlog (2026). *Zo neemt Frankrijk de positive van Amerikaanse dinsten over*. January 2026.

Terajima, A. (2026). *War notes.* The Kyiv Independent. January 30th '26.

Commission for Defence, Dutch House of Representatives (Vaste commissie voor Defensive, Tweede Kammer), (2026). *Cyberstrategie voor Defensie*.

Wennink, P. (2025). *De route naar toekomstige welvaart. Een sterk Nederland in een relevant Europa.*

Popa, Diana (2026). The integrated battlefield.
Red Sky 4.
© Red Sky 4, 2026

About the author.

Diana Popa has over 17 years of experience in research and academia and has authored numerous reports and scientific articles. Recent research and analysis focus on resilience as part of defence programmes, emerging disruptive technologies, in particular Artificial Intelligence in high risk areas, including defence.

Red Sky 4
The Netherlands
www.redsky4.nl
Redsky4@ziggo.nl