cegeka

CEGEKA SPECIAL OPERATIONS · WHITE PAPER

The AI CASTLE Framework

A strategic blueprint for mission-ready AI in Defence, Law Enforcement & Intelligence

Why we wrote this paper

Introduction

Across defense organisations, police forces, customs authorities and intelligence services, we keep having the same conversation. Everyone agrees that AI matters, but almost no one can say, in one sentence, what their organization is buying it for.

Procurement is often governed in an AI-tool-by-AI-tool way. One team pilots computer vision, another buys an analytics platform, and a third experiments with a language model. Each project can be defended on its own terms. Together, they don’t always add up to a capability, and in many cases, they can’t be explained to a minister, a court or a parliamentary committee.

The missing piece is not technology. It is a shared way of talking about outcomes. This paper offers one.

What this paper gives you

A thought map for determining where you already have AI capability and where you have none.

A common vocabulary shared by operators, technologists and oversight bodies.

A publicly defensible way to sequence the next three budget cycles.

cegeka

A world that no longer waits

The strategic context

Mission-critical organizations are being squeezed from several directions at once. Geopolitical fragmentation, hybrid and cyber threats, constrained budgets and a steady drain of specialist talent no longer arrive one at a time. They meet, they reinforce each other, and they accelerate. Waiting for the pressure to pass has stopped being a strategy.

At the same time, the technology meant to carry the mission keeps falling short of what the moment asks. Legacy systems, fragmented data and uneven security maturity pull in different directions, leaving little clear sight of the whole. Meanwhile the data arriving from satellites, sensors, body cameras, customs scanners and open sources has passed the point where skilled teams can keep pace unaided.

NATO's revised AI Strategy is blunt about the consequence: it is vital to adopt these technologies, responsibly, as soon as possible.

6

NATO Principles of Responsible Use now govern AI in defence and security

70%

fewer unplanned equipment breakdowns from AI-driven predictive maintenance

3 hrs

to reconstruct by AI a cyber attack on critical infrastructure, down from weeks

cegeka

Sources: NATO (2024); McKinsey & Company, AI decision advantage for defense; PNNL with Anthropic, for US DOE / CISA (2026).

Why most AI programs stall

The problem

The pattern we see

Data fragmentation & disconnect

AI enters mission-critical organizations through the side door. A unit runs a promising pilot. A vendor demonstrates a capability. A budget line opens and something gets bought.

Within two years the organization holds a dozen disconnected systems, each trained on its own data, each with its own interface, none of them talking to the others. Analysts switch between screens rather than working faster. Commanders cannot tell which system to trust when two disagree.

What it costs you

Uncertain funding

The bill arrives in four forms. Capability gaps stay hidden, because nobody has mapped what the organization can and cannot do. Duplication goes unnoticed, because two directorates buy the same thing under different names.

Oversight becomes fragile, because explaining a patchwork to an oversight authority is far harder than explaining a design. And momentum drains away, because leaders who cannot demonstrate outcomes lose the argument for the next tranche of funding.

None of this stems from the technology itself. Each outcome is the predictable result of structuring AI around product categories rather than mission outcomes.

The Cegeka AI CASTLE framework

Six outcomes, one shared language

The framework does one thing: it classifies every AI capability by the operational outcome it produces, rather than by the technology inside it. Six outcomes cover the full mission cycle, from first detection to long-term adaptation. A commander, a chief information officer and an oversight body can all use the same six words — which is precisely what makes an AI portfolio governable.

C

1. Capture

Perceive — sense & detect the operational environment across every domain.

A

2. Analyse

Understand — turn multi-source data into assessed insight.

S

3. Select

Decide — evaluate the options and choose the course of action.

T

4. Take Action

Act — execute the decision rapidly, precisely and within the rules.

L

5. Last

Sustain — keep people, platforms and networks ready for the long haul.

E

6. Evolve

Learn — train, retrain and adapt faster than the adversary can.

cegeka

The Cegeka AI CASTLE Framework. Original concepts: Perceive, Understand, Decide, Act, Sustain, Learn.

C — Capture

Detect and perceive the operational environment

Everything downstream depends on what you can sense. Capture is where AI extends reach and endurance beyond what human observers can sustain: more sensors, watched continuously, fused into one picture rather than a wall of separate screens. The measure of success is coverage without a proportional increase in headcount.

Defence

- **Sensor fusion** across optical, radar, infrared and hyperspectral feeds builds a single real-time threat picture spanning land, air, sea and space.
- **Edge-deployed object detection** reads UAS and satellite imagery at machine speed, including in poor weather and low light.
- **Autonomous ISR platforms** hold persistent watch over contested areas without putting additional crews at risk.

Law Enforcement

- CCTV, automatic number-plate recognition and acoustic gunshot **detection** converge into one command-centre picture instead of separate consoles.
- **Computer vision** flags crowd density, traffic and perimeter anomalies at a scale no watch room could monitor manually.
- At the border, **AI-assisted cargo and container imaging** helps customs officers spot concealment patterns that manual screening misses.

Intelligence

- **Persistent open-source monitoring** covers thousands of sources continuously, surfacing signals before they reach a formal reporting channel.
- **Multimodal models** fuse imagery, intercepted material and field reporting into one queryable operational picture.
- **Sensor-fused monitoring** of critical sites detects aerial, underwater and cyber-physical intrusion early enough to matter.

cegeka

Sources: ORM_AI technology roadmap; Army University Press, Military Review (2024); NATO (2024).

A — Analyse

Transform data into understanding

The bottleneck was never collecting data; it was making sense of it before the moment passed. Analyse is where volume becomes assessment — where pattern, anomaly and relationship are extracted at machine speed and handed to a human who still owns the judgement.

Defence

- **Multi-domain fusion** turns land, air, sea, space and cyber feeds into one coherent assessed picture, cutting analyst overload rather than adding to it.
- **Pattern recognition** separates genuine threats from decoys and clutter under ambiguous, actively contested conditions.
- **Predictive models** sketch likely adversary courses of action early enough for planners to shape events rather than react to them.

Law Enforcement

- **Link analysis** cross-references case files, financial records and communications to surface organised networks a single investigator would miss.
- **Pattern-of-life analytics** turn years of historical incident data into forward-looking risk maps for patrol and resource planning.
- **Automated triage** ranks the highest-value leads inside tip volumes that would otherwise be worked in order of arrival.

Intelligence

- **All-source fusion** merges signals, imagery and human reporting into a single assessed picture with confidence levels made explicit.
- Generative models let analysts **interrogate captured documents** and foreign-language material in the field, not weeks later.
- **Large-scale text analysis** helps surface coordinated disinformation and influence operations while they are still forming.

cegeka

Sources: Strategy&, The global AI race and defense's new frontier (2025); TAID working group; NATO (2024).

S — Select

Evaluate and select courses of action

Select is the outcome most often misunderstood. AI does not make the decision. It widens the set of options a commander can realistically consider and shortens the time needed to weigh them. The authority — and the accountability — stay exactly where they were.

Defence

- **Decision-support systems** rank feasible courses of action against risk, cost and readiness, with the commander firmly in the loop.
- **Simulation and AI-assisted wargaming** let planners pressure-test options against a thinking opponent before committing forces.
- **Machine-speed threat evaluation** compresses the observe-orient-decide-act cycle where reaction time is the scarce resource.

Law Enforcement

- **Risk-based triage** helps commanders decide where finite patrol and investigative capacity produces the most public-safety benefit.
- **Scenario simulation** pressure-tests public-order and major-incident plans in advance rather than during the incident itself.
- **Decision support** surfaces evidentiary strength and legal thresholds, while charging decisions remain with authorised officers.

Intelligence

- **Structured analytic techniques, supported by AI**, help weigh competing hypotheses honestly under incomplete and contested information.
- **Option generation** widens the range of collection approaches a chief can consider within the time actually available.
- Every **recommendation** is designed to be explainable and auditable, so a decision can be defended long after it was taken.

cegeka

Sources: Trustworthy AI in Defence (TAID) working group; Strategy& (2025); NATO Principles of Responsible Use (2024).

T — Take Action

Execute rapidly and precisely

Take action is where a decision becomes an effect, and AI shortens the distance between the two. Precision is the point: fewer errors, less collateral harm, and a clear human signature on every consequential act. Automation here is bounded by design, not by good intentions.

Defence

- **Precision-guided and robotic systems** absorb the dull, dirty, dangerous and expensive tasks that would otherwise consume crews.
- Once a course of action is approved, **tasking, transport and resourcing** execute across the logistics chain without manual re-entry.
- **Human-machine teaming** keeps a named person accountable for every use-of-force decision, in line with international humanitarian law.

Law Enforcement

- **Automated dispatch** routes the nearest suitably equipped unit the moment an incident is confirmed, rather than after manual triage.
- **Alert-to-response pipelines** compress the gap between detection and intervention, which is where most outcomes are decided.
- **Automated evidence handling and report drafting** return officer hours to the street instead of the keyboard.

Intelligence

- **Time-critical indicators route** directly to the analyst or operator with the authority and the means to act on them.
- **Pre-approved workflows** execute collection tasking the moment a defined threshold is crossed, under standing authorisation.
- Every **automated action** remains inside explicit rules of engagement, with a **full audit trail** of what was done and why.

cegeka

Sources: Artificial Intelligence in Military Application, Land Forces Academy Review; Strategy& (2025); NATO (2024).

L — Last

Maintain readiness and operational endurance

Endurance is a capability, not a by-product. Last is the least glamorous of the six outcomes and often the highest-returning: it is where AI keeps platforms serviceable, supply chains honest and networks defended, so that the other five outcomes are still available next month.

Defence

- **Predictive maintenance** has cut breakdowns by around 70%, lifted productivity 25% and reduced maintenance costs 25% in US Army use.
- **AI-driven logistics** reallocates fuel, parts and personnel dynamically as demand shifts, rather than on a fixed replenishment cycle.
- **Digital twins** of the supply chain let planners close readiness gaps by simulation before they appear in the field.

Law Enforcement

- **Condition monitoring** keeps vehicle, radio and sensor fleets serviceable, so availability stops depending on the last inspection.
- **AI-assisted rostering** keeps specialist roles and unpopular shifts consistently covered without burning goodwill.
- **Continuous monitoring** defends the case-management and communications systems that every operation now depends on.

Intelligence

- **AI-accelerated adversary emulation** reconstructed an attack on a simulated water-treatment plant in three hours instead of weeks.
- **Automated threat hunting** sustains round-the-clock defence of sensitive networks at a tempo human teams cannot hold alone.
- **Lifecycle governance** keeps models reliable years after deployment, when drift rather than launch quality is the real risk.

cegeka

Sources: McKinsey & Company, AI decision advantage for defense (US Army); PNNL with Anthropic, for US DOE / CISA (2026).

E — Evolve

Learn, train and adapt continuously

Adversaries adapt, so a framework that only describes today decays quickly. Evolve is the loop that feeds real outcomes back into training, models and doctrine. Organizations that close this loop fastest hold their advantage longest — and it is the outcome most often left unfunded.

Defence

- **AI-driven simulation**, VR and digital twins tailor training to each individual's measured skill gaps rather than a fixed syllabus.
- **Synthetic data generation** fills training gaps where real operational data is too scarce, too sensitive or too highly classified.
- **After-action analysis** retrains forecasting and recognition models on what actually happened, not on what was expected.

Law Enforcement

- **Case-outcome feedback** continuously retunes triage models, which is also the practical mechanism for detecting and reducing bias.
- **Immersive simulation** rehearses high-stakes, low-frequency scenarios without exposing officers or the public to risk.
- **Structured lessons-learned loops** move hard-won practice between units and jurisdictions instead of leaving it local.

Intelligence

- **Generative-AI tutoring** shortens the time an analyst needs to become productive on a complex collection platform.
- **Continuous and transfer learning** let models absorb new mission data quickly as the operating picture shifts.
- **Standing review boards** convert lessons into standards, so improvement survives the departure of the people who found it.

cegeka

Sources: ORM_AI technology roadmap (simulation and synthetic data); NATO (2024) on retraining and allied test facilities.

Trust is the binding constraint

The keystone that holds the framework together

Why capability alone is not enough

An AI capability that cannot be explained, audited or controlled is not an asset in this market. It is a liability waiting for a commission and/or court date.

Defence, law enforcement and intelligence organizations act under legal authority, and that authority is only ever as strong as the evidence trail behind it. Three constraints therefore sit across all six CASTLE outcomes rather than beside them. Systems must be lawful and accountable. Their reasoning must be explainable after the fact. And the data they run on must stay under national control — not subject to foreign jurisdiction because of where a cloud region happens to sit.

NATO's six Principles of Responsible Use

- Lawfulness — used within national and international law
- Responsibility and accountability — a human answers for the outcome
- Explainability and traceability — decisions can be reconstructed
- Reliability — capability is tested against its stated purpose
- Governability — systems can be overridden or deactivated
- Bias mitigation — active steps against unintended bias

cegeka

Source: NATO, Summary of NATO's revised AI strategy (2024), reaffirming the six Principles of Responsible Use endorsed in 2021.

Cegeka Special Operations

A division built for organizations where failure is not an option

Cegeka Special Operations is the division we built for defence, law enforcement, intelligence, critical infrastructure and space — the organizations society depends on when things go wrong. It draws on a family-owned Belgian company that has delivered for government and critical sectors since 1992, and on the full Cegeka stack: infrastructure, cloud, security and data engineering under one accountable roof.

What makes it different is not a product. It is European ownership with no exposure to foreign data law, the ability to build, test and deliver on the high side, and a habit of working shoulder to shoulder rather than at contractual arm's length.

What we bring

- Data engineering and platforms
- Predictive analytics and ML
- AI on Microsoft Fabric & Databricks
- Modern SOC and cyber resilience
- Sovereign EU datacenter hosting

9,000+
people group-wide

400+
data & AI experts

230+
cleared security specialists

€1.3bn
group revenue

10
EU datacenters

1992
family-owned since

cegeka

Source: Cegeka corporate figures (2026) and cegeka.com/en/solutions/data-ai.

Organize first, then buy

Conclusion

The organizations that hold an advantage over the next decade will not be the ones that bought AI earliest. They will be the ones that knew what they were buying it for.

The CASTLE framework is deliberately modest in what it claims. It does not tell you which model to train or which supplier to select. It gives you six words to hang every decision on, so a portfolio can be mapped, a gap can be named, an investment can be sequenced, and an outcome can be defended in front of the people entitled to ask.

Start by auditing what you already hold against the six outcomes. Most organizations find they are strong in Capture, thin in Select, and have funded almost nothing in Evolve. That single picture is usually worth more than the next procurement.

Three first moves

1. Map your current AI portfolio against the six CASTLE outcomes and mark the gaps honestly.

2. Pick one outcome where a visible win is achievable inside two budget cycles, and resource it properly.

3. Fix the trust layer first — data, governance and sovereignty — because everything else rests on it.

Let's build it together.

Cegeka Special Operations — the cornerstone that gives you mission-ready technology.

cegeka.com/specops

cegeka