NEPTUNES INSIGHT

WHITE PAPER

The Fight for Command

Command and control against a peer adversary in the age of autonomous systems

PREPARED BY	Hans Renssen · Neptunes Insight
DATE	July 2026
REFERENCE	NI-2026-01
VERSION	5.0

SUMMARY

Summary

Command is the art of authority: formulating intent, accepting risk, carrying responsibility. Control is the science behind it, the systems and procedures that keep execution on course. Technology can improve control a great deal. Command remains human work.

Uncrewed systems make command and control heavier. Every additional user of the battlespace means more deconfliction, more identification questions and a larger picture that someone has to interpret. Whoever develops or buys autonomy takes on a C2 problem along with it.

This paper maps four layers of autonomy to the levels of military operations. The core: the C2 integration burden stacks with every layer, while autonomy itself need not be built from the bottom up. Which level of autonomy is required follows from the mission profile. That insight should steer roadmaps, requirements and demonstrations.

01 · THE GAP

The gap between two worlds

At defence exhibitions, autonomy is a promise. In a planning room it is above all a question: who is in charge of that system, and what does it do when the link goes down? Both worlds talk about the same systems and rarely understand each other. Industry often does not know precisely what command and control entails or why an armed force weighs it so heavily. The military professional, in turn, often does not know what technically lies behind the word autonomy.

That confusion costs money and time. It produces systems that impress during a demonstration and then fit nowhere in a task group. It produces requirement sets for which no technical solution exists. And it sustains conversations in which both parties politely confirm each other without understanding each other. In the development of uncrewed systems, this has become one of the largest sources of delay.

This paper sets out to close that gap. It explains what command and control really is, why the subject forms a load-bearing chapter in every military plan, and why the rise of sensors, networks and uncrewed systems makes the commander's work heavier rather than lighter. It then presents a layered model that maps autonomy to the levels of military operations. The paper is written for the engineer and the operator at the same time; its value lies in the picture they will come to share.

02 · WHAT C2 IS

What command and control really is

US Army doctrine puts the distinction most sharply: command is the art, control is the science.[1] Command covers the authority formally vested in a commander, with everything human that comes with it. Formulating an intent. Accepting risk. Deciding while the information is incomplete. Control covers the systems and processes that make that authority effective, from procedures and reporting to information systems and the feedback between plan and reality.

Pigeau and McCann describe command as the creative expression of human will, and control as the structures that channel that will and contain the risk.[2] Alberts and Hayes condense forty years of C2 modernisation into a single warning: whoever treats C2 as a technology or an organisational chart misses the point. C2 is a function that has to be fulfilled. There is no system you can buy for it.[3] Van Creveld showed in 1985 how this plays out historically. Every technological leap, from the telegraph to the radio network, displaced the burden of command and usually increased it.[4]

For industry, this distinction has direct commercial meaning. Technology can improve control considerably, think of a faster picture or automated reporting. It cannot take over command, because authority and responsibility rest with humans, legally and morally. A product that promises autonomous command therefore promises something an armed force is not allowed to outsource. A product that demonstrably lightens the control burden of a crew solves a recognisable problem. Military customers hear that difference immediately.

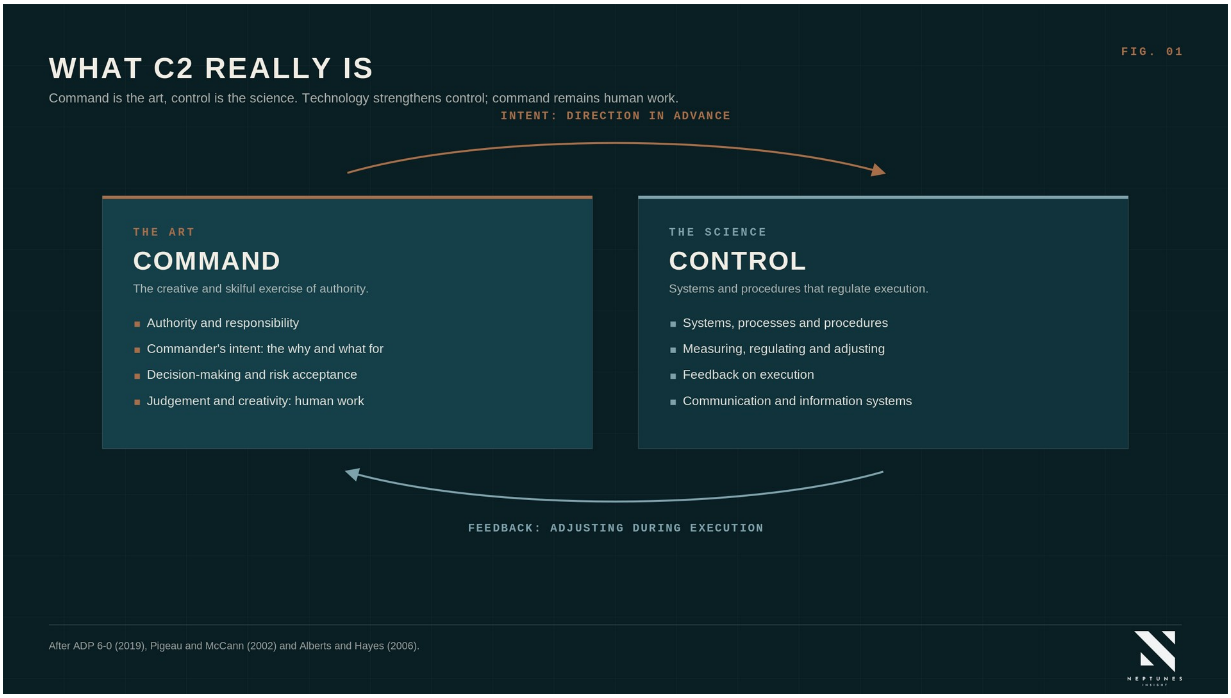

Figure 1. Command and control: two halves of one function.

C2 in planning

Military planning processes differ in name and detail. The Americans use the MDMP, NATO its Operational Planning Process, the Netherlands the SDMP. The same C2 questions run through all of them: who decides, who leads which unit, how is coherence maintained once the plan meets reality. The five-paragraph order makes this visible. After situation, mission, execution and sustainment comes paragraph 5, command and signal.[5] It states who is in command, who takes over if that commander is lost, where the commander is located and how units reach each other.

Every officer learns early why that paragraph exists. Plans rarely survive first contact unchanged. Whether a unit then adapts faster than its opponent depends almost entirely on command arrangements and communications. Paragraph 5 is the provision that keeps the rest of the order standing at the moment it comes under pressure.

Communications have their own planning discipline within this. For every operation, and sometimes per phase, a PACE plan is drawn up: primary, alternate, contingency, emergency, four tiers of communication means that may differ per mission.[31] The rapid development of radio equipment, from software-defined radios to jam-resistant waveforms and mesh networks, determines how solid each rung of that ladder is. For uncrewed systems this plan carries double weight. A crewed unit that loses all its links falls back on the intent and its own judgement. An uncrewed system has no such judgement; its fallback autonomy is in effect the last rung of the PACE ladder, and it has to be designed and tested before the operation starts.

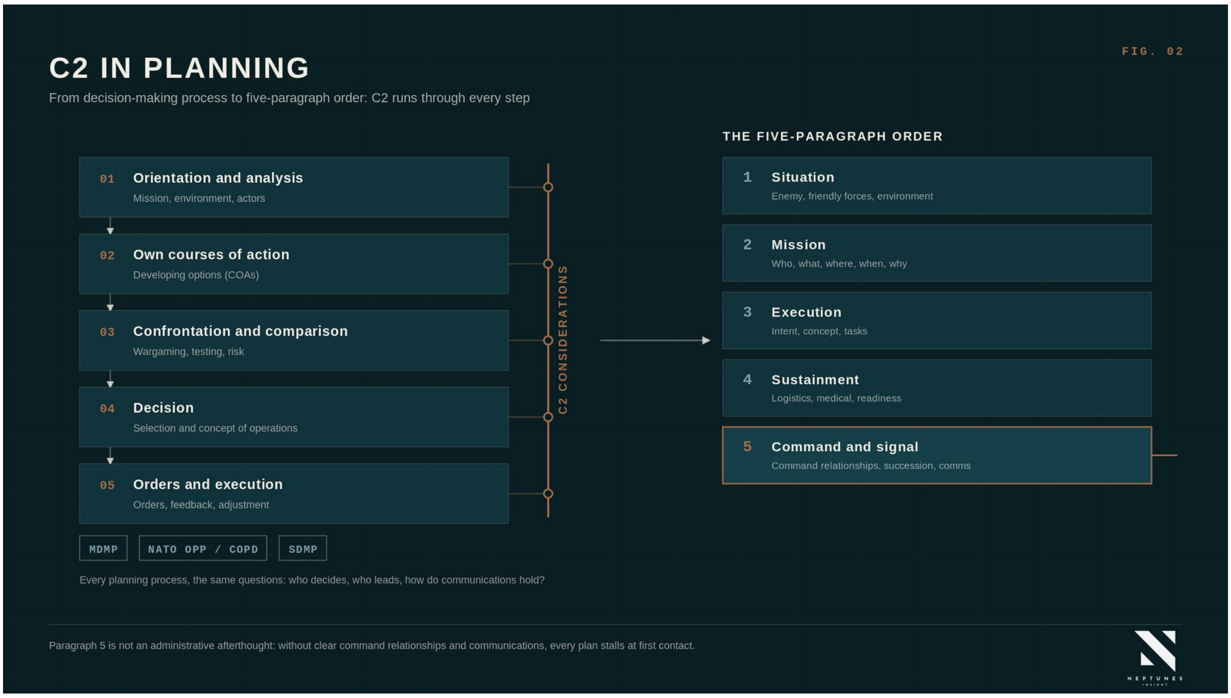

Figure 2. C2 runs through every planning step and culminates in paragraph 5 of the order.

03 · THE LEVELS

C2 across the levels of military operations

NATO doctrine and the Netherlands Defence Doctrine distinguish a strategic, an operational and a tactical level of military operations.[6,7] In practice, a technical level of execution sits beneath them: the platform, the weapon system, the sensor. Time horizon, geographic scope and information needs differ per level, and with them what command and control mean in concrete terms. One caveat for the maritime domain: a task group can be characterised as high-tactical or as operational, and both are defensible. For clarity of the layering, this paper uses the operational label.

Within and between those levels, Western armed forces apply mission command as their guiding principle.[8] The commander provides the what and the why; the executing unit determines the how within that intent. There is hard battlefield logic behind this. Whoever wants to take every decision centrally loses the tempo fight and turns their own headquarters into a single point of failure.[9] Once uncrewed systems join the formation, the principle carries even more weight. A system that loses its link can only continue if it was given an intent and boundaries in advance, just like a unit under mission command.

Autonomy also means something different at each level. Navigating independently at platform level is a different problem from executing a task independently at the tactical level, and different again from cooperating within a task group. Chapter 5 develops that layering.

Why technology makes C2 heavier

For over a century, new technology has promised to lift the fog of war. The opposite keeps happening. More sensors deliver more data, more systems demand more coordination, and greater reach creates more interfaces with others. Four developments currently drive the pressure on command and control.

Saturation and deconfliction

The battlespace is filling up. Where a task group once coordinated dozens of airspace users, crewed aircraft, helicopters, fires, loitering munitions and swarms of uncrewed systems now share the same space, above, on and below the water. Classic procedural deconfliction with corridors and time slots is reaching its limit. That DARPA and the American services are experimenting with automated deconfliction of the battlefield airspace says enough about the scale of the problem.[10] The risk of blue-on-blue grows at the same time. Friend, foe and neutral have to be told apart at ever higher speed, against targets that keep getting smaller and more numerous.[11] Deconfliction and combat identification are C2 functions. Autonomy does not remove them; they determine how much autonomy a commander can allow.

From picture to understanding

Endsley distinguishes three levels of situational awareness: perceiving what is there, comprehending what it means and projecting what it will do.[12] British doctrine extends that line to situational understanding, the insight that makes action possible.[13] Modern sensors and networks mainly strengthen the first level. The bottleneck therefore shifts from collecting to interpreting. A headquarters that sees more than it can process becomes slower. This too is ultimately a C2 question: who determines what is relevant, who filters, and on which picture is the decision taken?

Deep operations and effect at reach

Uncrewed systems bring effects within reach far beyond friendly lines, at costs that make mass achievable. Ukraine was the first to demonstrate this fully at sea. Without a fleet of any significance, it used uncrewed vessels and missiles to force the Russian Black Sea Fleet out of large parts of its operating area; the largest attacks involved more than twenty sea drones at once.[14,15] Less attention goes to where these operations were actually vulnerable: in the C2 chain. Relays, satellite links and their resilience under electronic warfare determined success, more than the platform itself.[16] Loss of link is loss of control. The drone war over land shows two movements at the same time. As long as cheap links were available, little autonomy was needed. Once jamming killed those links, terminal autonomy remained as the only substitute for the human in the loop.[17]

The temptation of centralisation

The reflex in response to all this complexity is predictable: connect everything to everything, centralise the picture and direct the fight from the network. The American JADC2 programme expresses that ambition.[18] Serious, well-founded criticism has followed. Such programmes are technology-driven, underestimate how vulnerable the network itself is and open the door to precisely the micromanagement that mission command is meant to prevent.[19,20] The doctrinal lesson stands. More data at the top does not replace delegated authority. Technology should strengthen control at the level where the decision belongs.

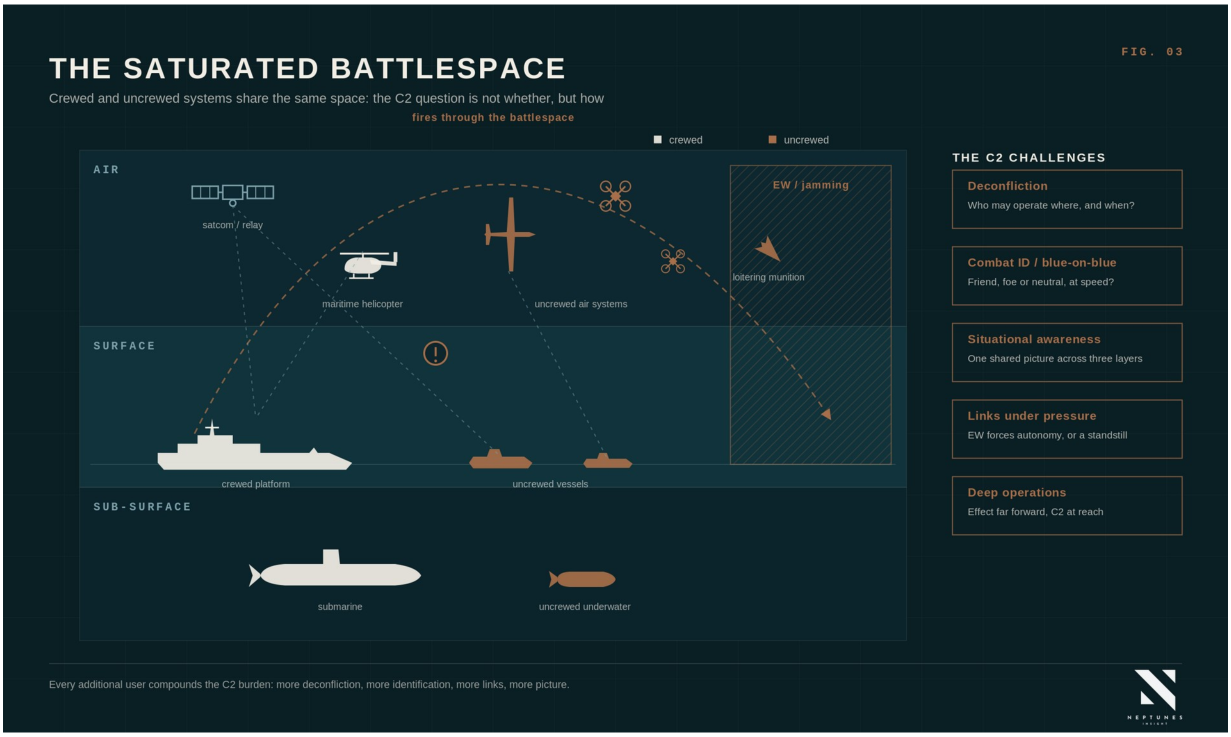

Figure 3. The saturated battlespace: crewed and uncrewed share the same space, and every additional user increases the C2 burden.

05 · THE LAYERS

The layers of autonomy

Anyone searching the literature for autonomy finds dozens of scales. Sheridan published his levels of automation in 1978, NIST built the three-axis ALFUS framework around the idea, and the IMO applies four degrees of autonomy to civilian shipping.[21,22,23] Nearly all of these scales describe the relationship between human and machine: who decides, how complex the mission, how difficult the environment. What is missing is the question of where in the military organisation the autonomous behaviour takes effect. The Defense Science Board concluded back in 2012 that thinking in linear levels of autonomy yields little, and proposed describing autonomy along, among other things, the echelon at which functions are allocated.[24] Bradshaw and colleagues dismantled the myth of full autonomy in the same period: every system operates within boundaries set by humans.[25]

Figure 4 builds on those insights and maps four layers of autonomy to the levels of military operations. The model says nothing about how autonomous a system is. It describes where the autonomous behaviour takes effect and what has to be arranged there.

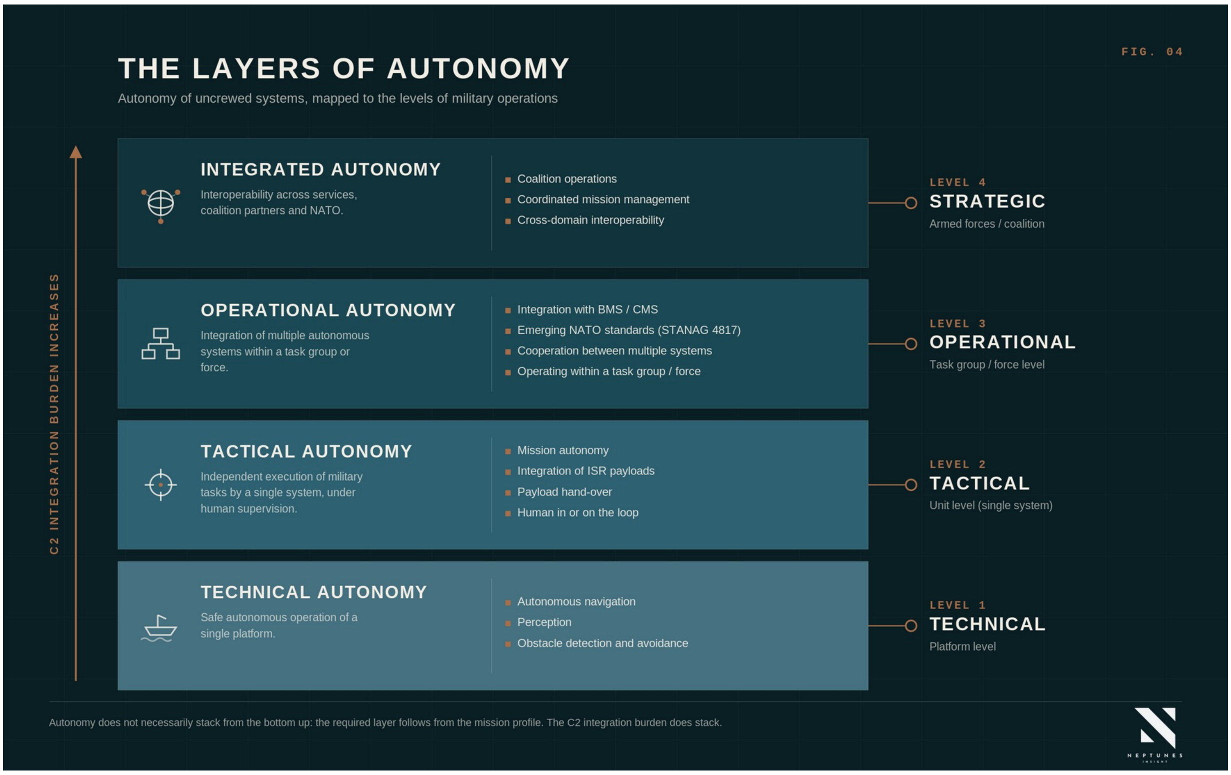

Figure 4. The layers of autonomy, mapped to the levels of military operations. The C2 integration burden stacks; autonomy itself does not necessarily.

Four layers

Technical autonomy operates at platform level: sailing safely on its own, perceiving, avoiding obstacles. This is the domain of certification and of civilian frameworks such as the IMO degrees. For peacetime operations, transit and operating near friendly or civilian shipping, this layer is indispensable. For some mission profiles it is emphatically not; more on that below.

Tactical autonomy operates at unit level: a single system executes a military task on its own, under human supervision. Think of mission autonomy, sensor employment and payload hand-over. As soon as effects enter the picture, meaningful human control enters with them. That human role runs through the entire targeting cycle and is not limited to the final press of the button.[26,27]

Operational autonomy operates in task group context: multiple autonomous systems cooperating within a task group or force. In concrete terms this means connection to battle and combat management systems (BMS/CMS), cooperation between systems and conformity with emerging NATO standards such as STANAG 4817, which is being tested in exercise series like REPMUS and Dynamic Messenger.[28,29,30] Most demonstrations founder at this layer. The platform works; the connection to the shared picture and the shared authority is missing.

Integrated autonomy operates in coalition context: interoperability across services, domains and allies, up to coordinated mission management in NATO operations. We deliberately avoid the term strategic autonomy here; in the European debate it carries a different, industrial-policy meaning.

No building sequence, but a stacking burden

The biggest misunderstanding around models like this is that they would describe a mandatory building sequence from the bottom up: first perfect the technical layer, only then deliver military value. Practice shows otherwise. The Ukrainian sea drones achieved effect at fleet level with limited technical autonomy. They were largely remotely operated, with the human in the loop during the terminal phase, without certified collision avoidance. The communications chain substituted for the autonomy.[14] Conversely, certifiable safe navigation is largely irrelevant for expendable systems, while for reusable platforms operating among crewed units it is a precondition. Which level of autonomy is required follows from the mission profile: expendable or reusable, peacetime or wartime, close to friendly units or far forward.

The C2 integration burden does stack. Every step up in the model means heavier demands on interfaces, standards, deconfliction and the shared picture. And at one moment the dependency on the lower layers returns with force: when the link goes down. Under electronic warfare, fallback autonomy at platform and mission level is the only substitute for the human in the loop, the last rung of the PACE plan. Whoever designs for combat designs for that moment.

For command, this means that autonomy moves command forward in time. The further the human moves out of the loop, the more has to be arranged in advance: intent, boundaries and behavioural constraints, and accountability afterwards.

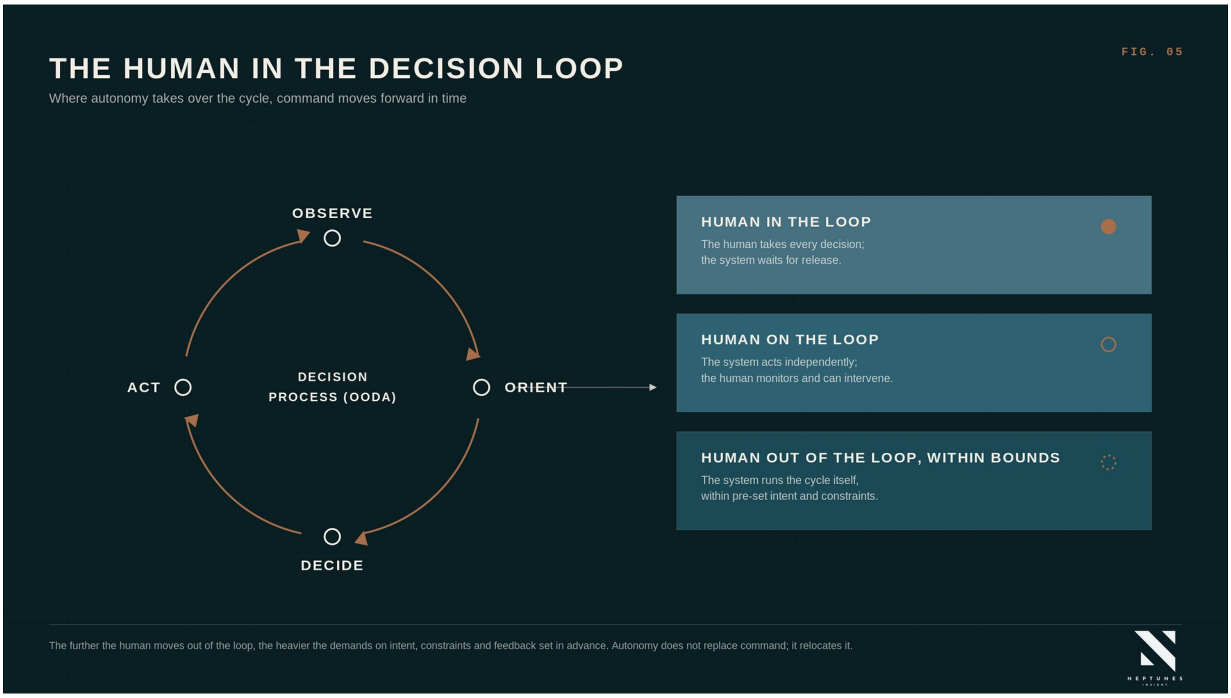

Figure 5. The human in the decision loop: the further the human moves out of the loop, the more command must be arranged in advance.

06 · THE BRIDGE

The bridge: what each layer demands of command and of control

The model becomes useful once each layer's demands on command and on control are spelled out. Table 1 provides that translation. A military customer implicitly reads every proposal along these lines. Defence organisations can use it the other way around, to specify requirements per mission profile instead of procuring autonomy as a single undivided concept.

Layer	Demands of command	Demands of control
Technical	Risk acceptance and employment rules: where may the system fail, and who carries that risk?	Safety monitoring, fail-safe behaviour, telemetry and logging for reconstruction
Tactical	Intent and tasking per system, authorisation of effects, safeguarding meaningful human control	Mission planning, boundaries and geofencing, payload management, feedback of mission results
Operational	Command relationships for uncrewed units within the task group, deconfliction authority, limits to delegation	Standard interfaces (incl. STANAG 4817/4586), integration into the shared picture, waterspace and airspace management
Integrated	Agreements on authority, rules of engagement and delegation in coalition context	Federated networks, data classification and releasability, interoperability testing in exercises

Two caveats. The command column cannot be outsourced to technology; whoever leaves it empty defers responsibility to the moment it is most expensive. The control column, on the other hand, can be engineered. That is where industry can make the difference, provided these requirements are taken into the design early and not left to the integration stage.

07 · IMPLICATIONS

Implications for capability development

For those who develop, acquire or integrate uncrewed systems, five working rules follow.

— **1.** Name the layer and the mission profile with every autonomy claim. Without a layer, autonomous is a marketing term; with one, it becomes a testable system property.

— **2.** Plan C2 from the first design sketch. The questions of paragraph 5 (who leads, who succeeds, how does the link hold) belong in the first design review, well before the acceptance test.

— **3.** Design for loss of link. Fallback autonomy within a given intent is a C2 requirement and a design requirement.

— **4.** Invest in the C2 provisions: interfaces, standards, the shared picture. Choose the autonomy level per mission profile.

— **5.** Keep the human in command. Automate control as far as is responsible. Command remains human work, including when it is laid down in advance in intent and boundaries.

The gap between the exhibition floor and the planning room is not a matter of unwillingness. These are two professional fields that still have to learn each other's grammar. This paper is a start. The organisations that master this language first, on both sides of the table, will notice it at every demonstration, every tender and every integration.

ABOUT NEPTUNES INSIGHT

About Neptunes Insight

Neptunes Insight is a defence consultancy at the intersection of end-user, industry and research institutes, specialised in maritime and uncrewed systems. Its foundation is nearly twenty years of experience as an officer in the Netherlands Marine Corps. From that background, Neptunes Insight translates operational needs into capability development and back, from operating concept and use case to market entry and integration. Strategic impact through operational insight.

The rise of artificial intelligence is shaping both technology development and the battlefield at high speed. Neptunes Insight factors that development into its analysis and advice every day, and deliberately tests AI in unorthodox ways by using it more and more in its own work. For this paper, AI was used to find and check sources and to draw connections between developments that rarely come together in a single piece.

Contact: info@neptunesinsight.com | www.neptunesinsight.com

SOURCES

Endnotes

1. US Army, ADP 6-0 Mission Command: Command and Control of Army Forces, Washington DC, 2019.
2. R. Pigeau and C. McCann, 'Re-Conceptualizing Command and Control', Canadian Military Journal 3(1), 2002, pp. 53-64.
3. D.S. Alberts and R.E. Hayes, Understanding Command and Control, CCRP, Washington DC, 2006.
4. M. van Creveld, Command in War, Harvard University Press, Cambridge MA, 1985.
5. US Marine Corps Training Command, The Five Paragraph Order (FMST-209). The format is used in variants across services and within NATO.
6. NATO, AJP-01 Allied Joint Doctrine, edition F version 1, Brussels, 2022.
7. Netherlands Ministry of Defence, Netherlands Defence Doctrine, The Hague, 2025 revision.
8. Netherlands Ministry of Defence, Joint Doctrine Publication 5: Command and Control, The Hague, 2012.
9. W. van Leussen, 'Opdrachtgerichte commandovoering' (Mission Command), Militaire Spectator 188(2), 2019.
10. DARPA, 'DARPA, Services Demonstrate Battlefield Airspace Deconfliction Software' (ASTARTE programme), 2023, www.darpa.mil.
11. Lieber Institute, West Point, 'Fighting at Machine Speed: AI and U.S. Army Counterfire Under the Law of War', lieber.westpoint.edu.
12. M.R. Endsley, 'Toward a Theory of Situation Awareness in Dynamic Systems', Human Factors 37(1), 1995, pp. 32-64.
13. UK Ministry of Defence, JDP 04 Understanding and Decision-making, 2nd edition, Shrivenham, 2016.
14. Center for Strategic and Budgetary Assessments (CSBA), A Navy of Necessity: Ukraine's Unmanned Surface Vessels at War, Washington DC, csbaonline.org.
15. RUSI, 'Uncrewed Platforms Have Been Critical to Ukraine's Success in the Black Sea', RUSI Commentary, London, rusi.org.
16. Center for Strategic and International Studies (CSIS), The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond, Washington DC, csis.org.
17. Modern War Institute, West Point, 'Networked for War: Lessons from Ukraine's Ground Robots', mwi.westpoint.edu.
18. US Department of Defense, Summary of the Joint All-Domain Command and Control (JADC2) Strategy, Washington DC, 2022.
19. Modern War Institute, West Point, 'A Solution Desperately Seeking Problems: The Many Assumptions of JADC2', mwi.westpoint.edu.
20. CSBA, Big Centralization, Small Bets, and the Warfighting Advantage (JADC2 policy brief), Washington DC, csbaonline.org.
21. T.B. Sheridan and W.L. Verplank, Human and Computer Control of Undersea Teleoperators, MIT, Cambridge MA, 1978. See also M.R. Endsley, 'Level of Automation Forms a Key Aspect of Autonomy Design', Journal of Cognitive Engineering and Decision Making, 2018.
22. H.-M. Huang et al., Autonomy Levels for Unmanned Systems (ALFUS) Framework, NIST Special Publication 1011, Gaithersburg MD.
23. IMO, Regulatory Scoping Exercise for Maritime Autonomous Surface Ships (MASS): four degrees of autonomy, London, www.imo.org.
24. Defense Science Board, The Role of Autonomy in DoD Systems, Washington DC, July 2012.
25. J.M. Bradshaw et al., 'The Seven Deadly Myths of Autonomous Systems', IEEE Intelligent Systems 28(3), 2013, pp. 54-61.
26. V. Boulanin et al., Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control, SIPRI and ICRC, Stockholm, 2020.
27. M. Ekelhof, 'Moving Beyond Semantics on Autonomous Weapons: Meaningful Human Control in Operation', Global Policy 10(3), 2019.
28. Janes, 'Is STANAG 4817 the final piece of the NATO MUS jigsaw puzzle?', 2024, janes.com.
29. UDT Europe 2026, 'Multi-domain maritime unmanned systems interoperability through NATO STANAG 4817', outcome of NATO REPMUS 2025, udt-global.com.

30. NATO Allied Maritime Command, 'Dynamic Messenger 2025: NATO drives maritime innovation through Allied experimentation', mc.nato.int, 2025.

31. US Army, FM 6-02 Signal Support to Operations, Washington DC, 2019. The PACE principle (primary, alternate, contingency, emergency) is common practice in communications planning across NATO.

Neptunes Insight B.V. · De Del 1, 3958 EH Amerongen · KvK 42042387 · BTW NL869442892B01 · info@neptunesinsight.com