Civilian-military asset handover: an unsolved challenge

Per Ödling[1], Tore Listou[2], Tomas Nordström[3], Freddy Jönsson Hanberg[4], Lizette Strandberg[5], Pia Kristiansson[6], Hanna Linderstål[7], Daniel Ekwall[8], Lauri Ojalla[9]

[1]Lund University, Sweden
[2]Norwegian Defence University College, Norway
[3]Umeå University, Sweden; RISE Research Institutes of Sweden
[4]Security of Supply Centre of Excellence (SOSCOE), Karlskoga, Sweden
[5]Bussgods i Norr AB, Umeå, Sweden
[6]Swedish National Road and Transport Research Institute (VTI), Skellefteå, Sweden
[7]Earhart AB, Sweden
[8]Swedish Defence University, Stockholm, Sweden
[9]University of Turku, Finland
[1]*per.odling@eit.lth.se*
[2]*tlistou@mil.no*
[4]*freddy.jonsson.hanberg@totalforsvar.org*
[6]*pia.kristiansson@vti.se*
[8]*Daniel.Ekwall@hb.se*

ORCID ID of Corresponding Author: Tore Listou https://orcid.org/ 0000-0002-8648-0302

Abstract

One of the challenges for civilian-military logistics systems is how to arrange the transfer of transport assets from the civilian operator to a military, and back. We are developing a dual-use, rural, drone transport system based on autonomous swarms that could also be used for frontline logistics. But how do we hand over the control of a drone in a cyber secure way? And then get it back to the civilian operator. All digital interfaces become potential attack surfaces enabling the entire system to be hijacked by an opponent, should the design fail.

This short paper presents no solution to this challenge. At best, we give a hint towards a solution. Our purpose is to describe the problem, put attention on this research topic, and broadcast a call for help. We plan a commercial deployment of the civilian system in 2027 and it would be useful to have a working hand-over solution by then. If not, we can instead offer the system as a prototyping platform for anybody interested in implementing and testing solutions. The intended civilian operator is Bussgods i Norr AB, a century old, publicly owned logistics company covering the northern half of Sweden with their transport services. Bussgods has 29 logistics centres in the form of bus stations that will be complemented with drone ports. The technical specifications of the civilian rural autonomous transport system are similar to what is needed for military frontline logistics in the sense that the drones operate over large distances, take reasonably heavy cargo (say in the order of 10 kgs), work in arctic winters, and are tolerant to bad connectivity. What needs to be added is resilience to electronically disturbed environments.

The presented work stems largely from NATO Exploratory Team SAS-ET-HFM-GD "UAV-logistics using a grid of autonomous charging stations".

Keywords: Frontline logistics, autonomous transport systems, UAV, UGV.

1. Introduction

With the rapidly changing geopolitical landscape it is necessary to pick up the speed with which we prepare for an armed conflict and any form of a hybrid war. Logistics is fundamental both for military operations and for a resilient society and will thus be a priority target in both an invasion-style war and in a hybrid war.

The way war is waged on the battlefield has changed dramatically where especially the use of drones has resulted in new tactics. On this new transparent battlefield, one must adapt to always being seen and thus often being targeted. Running logistic is very dangerous and often results in loss of both lives and cargo. While cargo is easily replaced, life is not. This mandates new methods for frontline logistics calling for an era of unmanned transportation systems. Autonomous frontline logistics is our field of work and what we will discuss hereinafter.

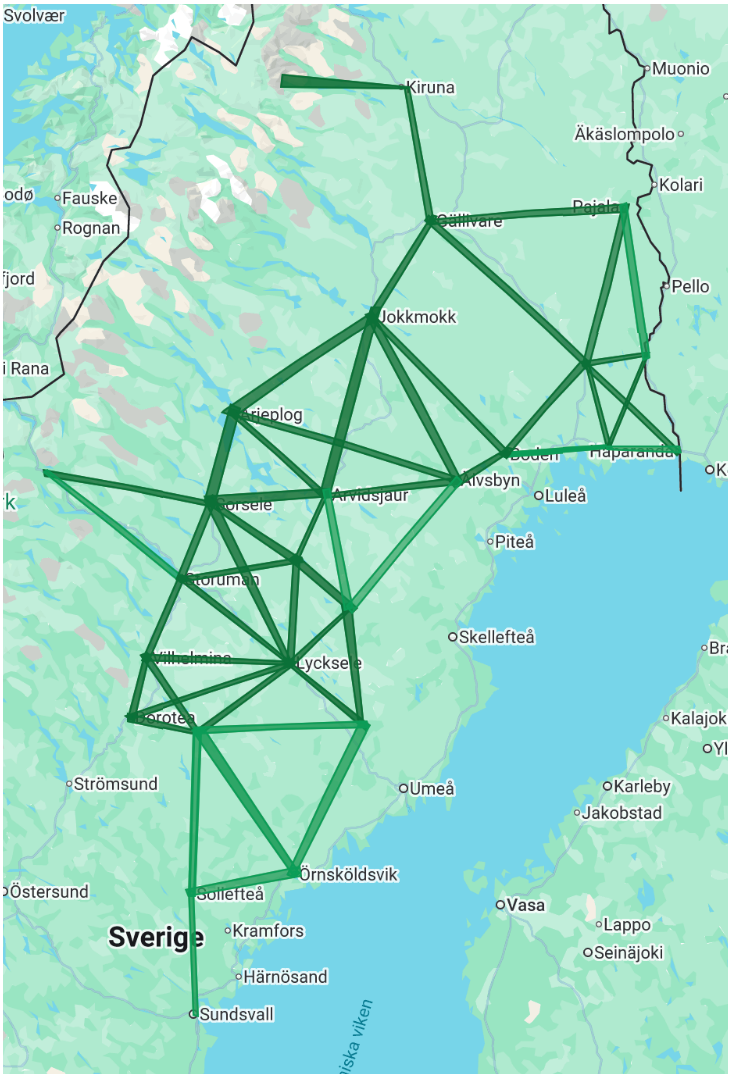
A scenario from NATO Exploratory Team SAS-ET-HFM-GD envisions an armed conflict in two areas, one being the in the Arctic north. Providing effective military logistics in this area is challenging as the availability and conditions of infra-structure such as roads, electricity, water supply, etc., are unfavorable.

The overarching goals of the project portfolio is twofold:

1: To demonstrate the strategic capability of military logistics in Arctic conditions.
2: To provide resilient rural civilian transport services in northern Sweden.

2. Current and emergent concerns

We work with civilian-military rural logistics using autonomous transport swarms, both UAVs and UGVs. Civilian-military, or dual use, means that we create civilian transportation systems that, if necessary, also can perform military logistics. Our civilian systems are designed for rural local delivery in arctic winters with the added capability of long-range hauls using autonomous charging stations. These qualities match well the frontline use case. While the front was a few hundreds of meters deep during WWI and a few kilometers deep in WWII, today's kill zone is several tens of kilometers deep. In the kill zone, logistics should be carried out with unmanned, small units to keep the cost of each committed resource as low as possible, given the mission at hand. The architecture of the frontline logistics system would then be a distribution of supply dumps far behind the frontline out of harm's way, from where UGVs and UAVs are loaded; and autonomous charging stations at the edge of the kill zone where UAVs can charge before moving in. Once at the front there are conflicting goals. It would be beneficial to spend as little time as possible there, but it is also necessary to make many fake cargo drops for every real one, in order to hide the location of friendly troops and predeployed supply. [Antai, I., & Hellberg, R. (2023). Identifying total defense logistics concepts: a comparative study of the Swedish pandemic response. Journal of Humanitarian Logistics and Supply Chain Management, 14(2), 208-222.] As opposed to UAVs, UGVs are likely to have enough battery capacity without recharging.



As the depth of the battlefield kill zone is several tens of kilometers, we need autonomous charging stations for UAVs to remove the range limitations. UAV doing frontline logistics need to be well charged when entering the kill zone to be able to make many fake deliveries for every real cargo drop. Our solution is placing autonomous charging stations just out of harm's way. In the civilian use case, the charging stations create a transport service that can cover very large areas, like the length of northern Sweden, more than 1000 km. The figure shows the planned drone transfer corridors between charging stations in Bussgods' upcoming network. The drones can then travel through this network without human intervention.

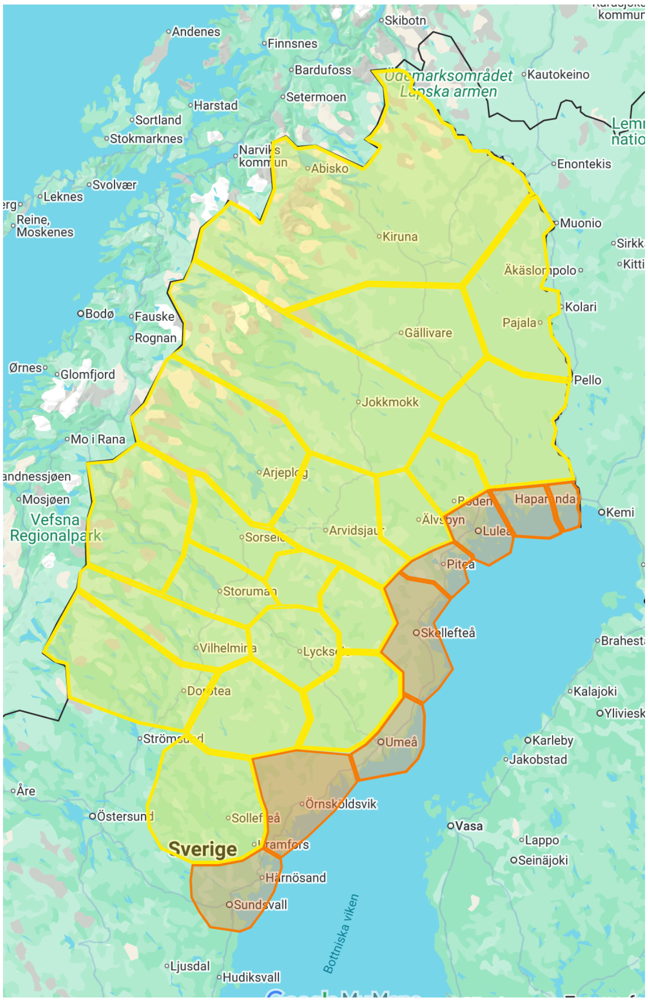
What is then the purpose of using civilian-military transport systems instead of just going for pure military systems? Using civilian-military systems saves money as costs are shared, and indeed mostly paid by the civilian part, but the main purpose is to avoid becoming stuck with an obsolete system. Military systems are traditionally designed, purchased, trained on, and fielded in cycles of years. The pace of innovation on the battlefield in Ukraine renders many systems obsolete in a few months, sometimes weeks. The main advantage with a civilian-military system is thus that it is kept up to date by the civilian operator as it is in constant use.

When choosing among civilian systems to achieve dual-use, the choice always falls on systems for rural use. There are a few delivery operations using autonomous vehicles, UAVs and UGVs, currently ongoing, but they are focused on delivery in cities, usually of warm food. In the cities the distances are short, roads even and tidy, cellular coverage excellent, and the weather often forgiving. These systems cannot easily become dual-use. The rural drone transportation system we are developing, and for which commercialization is planned in 2027, is intended for long distances, arctic weather, and spotty telecommunication coverage. We hope to add UGVs, i.e. transportation robots, during 2029. These will be able to handle rough roads, snow and ice, and some UGVs will even have extensive off-road capability. In their dual-use role, they will be able to handle military logistics, also for arctic warfare.

3. Study design

The intended architecture of the 2027 drone transport system is as follow:

- Two control rooms that monitor the transportation system and that can remotely control assets, for instance manually fly drones. One main control room and one back-up, preferably in a remote, secure location.
- 29 bus stations that already functions as logistics centers and will be equipped with drone ports and autonomous charging stations.
- Mobile drone charging stations for emergencies and for military use.
- A fleet of drones of various sizes, cost, and capabilities. Some intended for local distribution around a given bus station, some that can fly in between bus stations and thus migrate freely and autonomously over the entire network of charging stations.
- From 2029 and forward: an additional fleet of UGVs complementing the UAVs. The UGVs will also be of different sizes. The smallest in our current projects can carry a few bags of groceries, the largest is a self-driving BAE-Hägglunds Bv206 (a tracked, articulated, all-terrain carrier, the traditional Swedish “bandvagn”).
- From, say, 2028: complementary infrastructure that enable dual-use. This would typically be: one or more additional control centers for military logistics, additional mobile drone charging stations, additional drones, especially drones with sensors; and the digital infrastructure needed for handover, identification, etc. (This digital infrastructure is what we now ask for your help figuring out.)



The map illustrates the areas to be served by the planned autonomous transportation system. Bussgods aims for commercialization during 2027. Each marked area in the map is the reach of local drone-based transportation services from given bus stations. The yellow, inland, areas will be the first to get access when the system is established. The coastal areas marked in red already have good coverage by sustainable services and will then be included later.

The future military control room would have an overview of the civilian system plus hidden military assets like charging stations. From there, military operators would be able to request control over civilian assets, use them for various missions, and also be able to return them to civilian control. The theme of this paper is how these handovers should be orchestrated and implemented, a challenge yet unsolved.

Traditionally assets and resources are handed over from civilian to military control by an officer arriving at the scene to sign a paper and get some keys. [Alvinius, A., & Hedlund, E. (2024). A colossus on clay feet? Mechanisms of inertia in civil-military collaboration within the context of Swedish total defense. Defence Studies, 24(4), 601-623.] In our case all hardware in the rural autonomous transport swarm is monitored from a remote civilian control centre from which the pilots can take manual control over drones, the charging stations, and other assets in the transport system. For dual-use, these assets can then, at any time, be digitally “drafted” into military use and instead be controlled from the military command centre. The “drafting”, the handover of control will be done by means of a military computer talking to a civilian computer and then getting control over whatever asset or group of assets that was requested. Perhaps this will be preceded by somebody switching on the transfer functionality on a system level, and perhaps it is preceded by say a phone call for each transfer event where one or a group of assets are shifted over, but the actual transfer will be a computer-to-computer act.

4. Findings / Analysis

As we see them now, the challenges fall into two main categories, namely cybersecurity and orchestration. The cybersecurity challenges are mainly concerned with the risk of hacking where the control of assets is lost to an opponent; by denial-of-service attacks where we lose control over assets; and intrusions where an opponent can listen to communication and determine our intentions and the locations of assets and friendly forces. An example of the latter would be the message to a drone instructing it to make a set of fake cargo drops using a sequence of coordinates, a real drop, and another set of fake drops. If that message could be intercepted and understood, the location of the real drop could give an opponent information about the whereabouts of friendly forces or planned movements. There is a number of measures that could be taken to reduce the risks, for example using dedicated optical fibers for the communication between the computers, but every precaution comes at a cost and may depend on the architecture of the system. Say that if the military drone command center resides inside a truck and thus is mobile, one could not use fiber optical communication. In general, all communication chains consist of multiple hops where messages are passing through different technologies, and each link then has its own vulnerabilities. [Wen, K., et al. (2024). A Secure Authentication Protocol Supporting Efficient Handover for UAV. Mathematics, 12(5), 716.]

The orchestration challenges concern transferring control. This is a complicated issue with many aspects of which we will give only a few of the less obvious examples.

- Say that a drone upon being returned to civilian control is damaged, who pays? It would typically fall on the civilian insurance company, but they could be quite hesitant to provide insurance for drones when they work the frontline.
- The civilian drone systems will have a “give the right of way” functionality that makes them drop out of the passable airspace when and where, say, an ambulance helicopter needs to pass. But how do the priority list look when a drone flies a military mission, who yields to whom? The system needs to be programmed one way or another.
- How should the data models look for the entities in the system? The models may limit the intelligence of the system later on and this is an area where the devil really lies in the details.
- There is a risk that every UAV/UGV manufacturer has its own control interface which complicates handover and suggest the need for a common “meta interface” or some standardization of interfaces.
- When a drone lands to charge, the drone and the charging station will identify themselves to establish trust. When handed over, is there a new digital infrastructure for this identification with its own keys and methods or is the identification infrastructure somehow open to both the civilian and military operators, with the risks that this will bring? [Ma, J., et al. (2025). Dual-Chain-Based Dynamic Authentication and Handover Mechanism for Air Command Aircraft in Multi-UAV Clusters. Mathematics, 13(13), 2130.]

As we approach the implementation of the system, there is an alarmingly large number of practicalities that we realize needs to be solved before any commercial services are possible in a dual-use system, and many of these hurdles stem from the dual-use aspect.

5. Discussion

As far as solutions to the handover challenge comes the most suggested is to let the civilian operators also handle the military logistics. This solves a whole range of problems, not the least in the cybersecurity domain. But there are two main drawbacks. The civilian staff now become soldiers and a legal target in war. We have seen in Ukraine that this may make no practical difference during a war, the command center will be attacked anyway disregarding any laws of war, but it will still be consideration that may be uncomfortable for many civilian employees even during peace. It will also make the system centralized and inflexible. Ideally, we would want a frontline quartermaster to be in control of a set of assets with which he or she can meet the local needs. Preferably, the system should be so easy to use that a special forces commander should be able to step in and state: “I want this to be delivered there at that time”, and the system would arrange for everything, including a spread of fake drops. This type of flexibility would be difficult to achieve, even long-term, with a single command center staffed with people that have a very different background from the frontline quartermasters.

To keep innovating even in times of peace, there must be commercial cases for developing the new drone capabilities that also are relevant for the military. We need a substantial capacity to manufacture and innovate around future UAVs, even if there is no current military need to stock UAVs (as they quickly become obsolete and should be seen as consumables). We need public-private partnerships that are based on civilian business cases. Governmental support of civilian UAV deployments is needed to pay for the extra costs that occur when adding dual-use capability, and to establish and uphold mass-production capacity and know-how. The arms race of the cold war era has been replaced by a race for building knowledge and strategic capability, and falling behind in this new race would be unwise and dangerous.

6. Conclusions and practical implications

The step from a rural drone logistics system to a dual-use, civilian-military system is conceptually straightforward as the hardware should fit well but seems practically quite complex. When looking at the solution space, we have found one civilian application that may serve as a basis for our future civilian-military digitized handover. There is “systems of systems” research that look at e.g. construction sites where heavy vehicles appear, do some task, and leave. To keep a safe and efficient workplace, these assets need to be checked in and given attributes. Do they need to charge? Do they need extra staff to perform their task? Are there dependencies between their tasks and other tasks? The methodology and data models from this research area could possibly fit our civilian-military handover case. [Rylander, D., & Axelsson, J. (2025). Systems-of-Systems Engineering Challenges: Experiences from the Road Construction Domain. Proceedings of the 35th Annual INCOSE International Symposium.]

Acknowledgements

The presented work stems largely from NATO Exploratory Team SAS-ET-HFM-GD “UAV-logistics using a grid of autonomous charging stations”. Partial funding has been received from e.g. Vinnova (Sweden), the Swedish Energy Agency, and the Swedish Transport Administration.