Tactical Aerial Reconnaissance and NATO

Past, Present and Future

by Robert Egnell, Johan Jakobsson, Garfield Porter and Dag Åsvärn

Resumé

Natoinitiativet Joint ISR (JISR) ställer ökande krav på effektivisering av underrättelseprocessen i medlems- och partnerländer. Produkter ska snabbt kunna lagras, tas fram från ”arkiv”, bearbetas, exploateras och delas i ett CSD-nätverk (Coalition Shared Data). Försvarsmakten, FM, har dock ingen sådan JISR-/CSD-interoperabilitet, vilket är besvärande mot bakgrund av Försvarsmaktens utlovade medverkan med Gripen i Natos insatsstyrka NRF. FM kan JISR-interoperabelt varken lagra, ta fram eller dela data och kan heller inte delta i underrättelseplanering. Värdlandsavtalet med Nato, avsiktsförklaringen om försvarssamarbete med USA samt Finlands-samarbetet torde även de förutsätta JISR/CSD-interoperabilitet, vars krav på tempo och precision också bör gälla i Sverige. Gripen kan enkelt ges en grundläggande JISR/CSD-kapacitet genom en luftgapslösning, som senare kompletteras med en integrering av CSD-kapaciteten i själva Gripen-systemet. På sikt bör JISR/CSD-kapacitet införas i hela FM genom en robust, allomfattande JISR/CSD-lösning.

SWEDISH TACTICAL AERIAL RECONNAISSANCE (TAR) has, like other parts of Swedish Armed Forces' (SwAF) capability, followed shifts of emphasis in doctrine and practice. In particular, at the end of the Cold War, it moved from a posture focused on fending off a Warsaw Pact invasion towards greater emphasis on deployed interventions abroad. More recently, contemporary events have also impacted on Swedish thinking, resulting in a renewed focus on homeland defence whilst also recognising the need to act in concert with others. Consequently, interoperability issues will increasingly play a prominent role in Sweden's wider international approach.

Indeed, interoperability is high on the current agenda due to both the Host Nation Agreement (HNA) between Sweden and NATO and Sweden's on-going commitment to the NATO Response Force (NRF). Against this shifting backdrop, this article provides a broad outline of both past and present TAR capabilities before considering likely future development, with particular emphasis on interoperability, and offers some thoughts on how such increased interoperability might be incrementally realised.

History of Swedish TAR

From the '60s through to the '80s, SwAF intelligence requirements placed a strong emphasis on countering an invasion threat.[1] Accordingly, the need to follow regional developments, for example in and around the Baltic seaports, largely governed SwAF TAR[2] capability development. Sweden's main international effort during this period was in the Belgian Congo, where an air presence was deployed, using the reconnaissance version of the iconic SAAB 29 (The Flying Barrel).[3]

Gripen. Foto: Jörgen Nilsson.

Although the invasion threat remained the defining consideration, by the '90s there was also an increasing focus on international operations, mainly driven by events and subsequent SwAF deployments in the Balkans. Whilst no SwAF TAR units were deployed in this theatre, UK Remotely Piloted Aircraft (RPA) assets were used by Swedish troops, generating valuable tasking and user experience.[4] At that time, SwAF RPA capabilities were still under development, mainly within K3, an army regiment in southern Sweden.

The Balkans experience also reinforced the realisation that modern agile forces needed reliable ISR both at an organic and force level. Consequently, especially in response to the growing emphasis on deployed operations, the Swedish Air Force Rapid Reaction Unit (SWAFRAP) was formed in 2000. At first, SWAFRAP's tasks – mainly reconnaissance – were designated to the reconnaissance version of the SAAB AJSF 37 Viggen. The SWAFRAP was, however, never deployed.[5]

Over the next decade, SWAFRAP was re-equipped and replaced by a series of similar, small and agile units equipped for fighter and attack roles as well as for reconnaissance. This included assignments of the unit within the EU Nordic Battle Group Expeditionary Air Wing (NBG EAW). Based on a similar model to its assignment to the NBG EAW, since 2014, Sweden has also offered Gripen TAR assets in support of the NRF.[6]

The early part of this century offered few real-world opportunities to test the emerging aircraft- based TAR capability, but that changed in April 2011, when Sweden deployed a Gripen unit (equipped with eight aircraft) to participate in the NATO-led Operation Unified Protector (OUP) over Libya. Notwithstanding the organisational preparation that had taken place over the years, this was the first Swedish expedition-

ary experience with combat aircraft since the Congo deployment half a century earlier. In 2011, there were also advances in RPA capability when Swedish elements deployed to Afghanistan were equipped with the Shadow 200. During this deployment, it became increasingly apparent that organic tactical reconnaissance support was a modern day battlespace necessity. Somewhat later, smaller tactical RPA were also again tested and acquired.

Since 2011, the Gripen contingency commitment to the EU NBG EAW[7] has been sustained, although the unit has not deployed. Sweden, however, is currently contributing some 250 troops to the ISR Task Force (equipped with Shadow 200 and smaller tactical RPA) as well as to the Multinational All Sources Information Fusion Unit in Mali.[8]

Organisationally, SwAF TAR continued to revolve around three formations; F17, F21 (both Air Force wings) and K3 (an Army regiment). F17 and F21 each comprised two squadrons, all of which undertook TAR. However, in early 2016 the fixed wing TAR role was allocated solely to F17. At K3, TAR is organized within the regiment's Intelligence Battalion, which among other capabilities comprises two Shadow 200-equipped companies. Furthermore, each of the eight Swedish ground force battalions is equipped with organic RPA assets.[9]

SwAF TAR in OUP

The Swedish Libyan mission was divided into two rotations. First, from April to June 2011, the unit was tasked to provide Defensive Counter Air (DCA) and TAR in

Gripen. Foto: Jörgen Nilsson.

support of the No Fly Zone (NFZ). Notably, the ratio of pure DCA to mixed DCA/TAR was 1:11; however, most of the latter was purely reconnaissance.[10] The second rotation, from June to October 2011, expanded the mission to cover TAR across the full spectrum of UN-mandated tasks – going well beyond those related to the NFZ by including the enforcement of the arms embargo and, most importantly, the protection of civilians. In total, the Swedish operation contributed over 570 missions and about 1,770 flight hours; from a TAR perspective, around 2,770 reconnaissance exploitation reports (RECCEXREPs) were sent to higher command. In fact, during the second rotation, Gripens conducted a third of all OUP TAR assignments.

From these statistics, it is clear that Sweden's predominant contribution – beyond that of political support to the operation – was TAR. It is fair to say that initially Sweden's involvement was probably seen as politically useful, but it did not carry particularly high expectations of operational utility. Such scepticism quickly transformed into praise after the reconnaissance missions and imagery provided by the Swedish contingent consistently proved their worth. A RUSI report on the international intervention in Libya concluded: 'The Gripen aircraft and the Swedish pilots and support staff proved outstanding in [the reconnaissance] role and outstripped other combat assets with the quality of its tactical ISR (intelligence, surveillance and reconnaissance).'[11]

Key aspects in this timely turnaround of imagery into reports were highly trained analysts and the novel use of post-flight technology. Thus, Gripen's lack of a downlink capability was offset by, inter alia, the rapid Swedish imagery processing capability, Keystone.[12] Report preparation times were greatly reduced by not needing to download an entire mission's data before processing could commence, instead downloading initially data only from specific areas of interest.

OUP Lessons Learned on Interoperability

Whilst the Swedish contribution to OUP was in many ways a success, the operation also revealed a number of important challenges, which would need to be addressed to improve operational effectiveness in future coalitions. Upon deployment, it became clear that the Swedish communication systems, despite years of working on interoperability, could not be fully integrated into the NATO C2 systems. First, and most importantly, as a partnership country, Sweden had no access to the NATO Secret network from the outset, and obtaining a license initially proved difficult. Second, despite having made the Gripen's Link 16 compatible shortly before deploying, a crypto key had to be obtained, which also was a difficult and lengthy process.

Not providing early access to a substantial troop contributor was an unnecessary weakness, and the Alliance has been critical of its handling of this issue.[13] In short, these matters highlighted the importance of interoperability – both politically and technically, particularly when they impact on speed of information transfer and analysis – the key in TAR to operational effectiveness.

Interoperability with NATO Joint ISR today

The primary NATO initiative influencing Sweden's focus on TAR has been Joint Intelligence Surveillance and Reconnaissance (JISR).[14] Essentially, this initiative shifts the

focus from collecting intelligence to streamlining the collection process and ensuring subsequent products are stored and shared in a timely and efficient manner with minimal obstacles between the command chain and contributing/user forces. In many ways, it is dependent on building a network of Coalition Shared Data (CSD) servers which allows unhindered and timely transfer of products generated by those on the network, as well as the potential to transparently tap into the collection management process.

As this initiative gains traction (the underpinning doctrine, AJP 2.7 JISR, was published on 11 July 2016), nations will need to decide the measures necessary to ensure adequate interoperability both in terms of process and CSD capability. Given that this process will most likely form the basis of any coalition activities, potential partners, like Sweden, will also need to make suitable contingency arrangements to avoid interoperability speed bumps on contributing elements.

The Swedish government has explicitly directed its military to maintain interoperability with NATO and actively transform towards NATO compliance. Although Sweden has no formal STANAG ratification process, many relevant standards (both procedural and technical) have been implemented. In particular, with regard to TAR capabilities, the Swedish Armed Forces will continue to comply with the requirements of STANAGs 3377 and 3596[15] for reporting methodology and RECCEXREP. However, when it comes to other JISR standards, Sweden, having not been part of the Multi-Intelligence All-source Joint ISR Interoperability Coalition (MAJIIC) community,[16] and with some of the MAJIIC technology work patterns not yet published as STANAGs, is understandably lacking some JISR-specific solutions. Nevertheless, Sweden is following the current NATO JISR initiatives closely, and has decided to become a NATO FMN (Federated Mission Networking) participant.

The Coalition Shared Data Challenge for Swedish TAR

Sweden bases its interoperability requirements on NATO's Partnership for Peace Planning & Review Process goals and the Allied Command Operation Directive 80-096 on the NATO NRF. Neither document currently includes any specific JISR technology guidance, for example on CSD servers. Consequently, CSD interoperability has no formal priority on the current SwAF agenda. However, the need to share and collaborate in this manner is well understood and accepted, leading to increased discussion regarding CSD issues. Nevertheless, the lack of formal guidance has to date stymied any CSD initiatives by the Swedish Defence Materiel Administration on behalf of the SwAF.

In recent years, there have only been minor changes to equipment. Consequently, Gripen's reconnaissance pod lacks a downlink capability, meaning data is only available to interpreters for exploitation post-landing. Fortunately, as previously mentioned, a solution is in place allowing the image interpreter to almost immediately start producing the RECCEXREP, while the entire mission data set is still being downloaded. Nevertheless, a CSD solution for sharing raw or exploited data is currently neither available aboard Swedish reconnaissance aircraft nor at the respective ground stations.

In the same manner, demands for video archiving, cataloguing and retrieval with CSD interoperability are beginning to be felt within the SwAF Tactical RPA community. The latest development of NATO JISR doctrine and procedures clearly point to the need for common methods and messages in regards to JISR operations; moreover, the

requirement to make RPA video available to partners is a distinct challenge. However, there are at present no plans to CSD-ify SwAF Tactical RPA.

Ironically, the very challenges revealed by sharing information at coalition level are very similar to those facing Sweden in homeland terms. To get real synergy from the data/imagery that is collected, there is a requirement to permit routine access to information at both force[17] and joint levels, as well as potentially other government departments and agencies. In some ways, it could be compared to a national banking system where money (information) is routinely moved between bank branches (CSDs) at a national level and through international banking rules and regulations (STANAGs) plugged into a wider system whenever required (NATO JISR), thus making CSD and a secure communication system the building blocks for future development.

Improving Interoperability – A Way Forward

As stated above, Sweden has committed, and is likely to continue to offer, Gripen aircraft to the NRF. As an example, during Trident Juncture 18, Gripen aircraft are planned to take part, possibly in a recce role – albeit Sweden has not barred any of the three possible roles[18] from NRF use. Also, as Sweden has an HNA with NATO, explicitly aiming at facilitating NATO support in the event of a homeland crisis, it is reasonable to assess that some sort of intelligence interoperability is also implied. Furthermore, it is difficult to see how interaction with both US and Finnish forces, very high on the current Swedish political agenda, could be facilitated other than using NATO interoperability solutions.

Given these Swedish commitments and aspirations, along with the increasing NATO impetus towards JISR interoperability amongst both member and partner states, it could be argued that Sweden would do well to start thinking about JISR, even if we have seen that no formal obligations to do so exist as of now. Moreover, it is increasingly apparent that whether based on NATO JISR protocols or not (but why reinvent the wheel?), Sweden will need to reinvigorate its internal sharing of information to meet the pace and precision of modern operations. Indeed, such a thought process has started. Following a SwAF HQ directive, a working group has been formed, chaired by the SwAF Intelligence and Security Directorate (Must). This group is tasked to draft the following items:

- A SwAF definition of JISR
- A discussion paper regarding JISR, explaining in more detail what JISR is, again from a SwAF perspective, how it could be used within the SwAF, and the principles of the use of JISR within the SwAF.
- A plan for the implementation of JISR concepts and practices within the SwAF, including repercussions for existing systems, workflows and training.

The working group has already delivered the first two items, the SwAF definition of JISR and the discussion paper, to its steering group. The third deliverable, the plan for implementation of JISR concepts and practices within the SwAF, will be initiated only after these two items have been accepted by the steering group.

Increments Towards Full CSD Compatibility

The formation of the SwAF JISR working group constitutes a clear signal that CSD

is now on the SwAF agenda, and that the thought process towards CSD interoperability has begun. Given the increasing pressure from the Swedish political level for improved interoperability, it is anticipated that, in due course, this process will lead to a Swedish CSD capability. Notably, in early 2017, the SwAF reportedly reinforced its decision to become a FMN participant by placing an order with the Swedish military procurement agency FMV for five FMN systems. Also, the SwAF has applied to participate in the NATO Trial United Vision 18 in June 2018, and current plans include fielding a JISR capacity, including RPA assets. As a natural follow on from these ambitions, there is now an on-going discussion between the SwAF and FMV as to what the FMN order should entail in terms of CSD capability.

Without in any way wishing to prejudge the unfolding process, three distinct steps in the build-up of a SwAF CSD capability could perhaps be discerned. These steps are described below.

A first step, supplying the Gripen aircraft system with basic CSD capability, would entail deploying a CSD server alongside the Gripen unit. The Gripen unit could then publish data to the CSD server via an air gap, from whence publishing data to a Mission Network via Swedish BICES.[19] With supporting advice from the NATO Communication and Information Agency (NCIA), such short-term plans to integrate Gripen with CSD have been under discussion within the SwAF for some time; amongst potential solutions, it is noteworthy that a CSD module has already been developed which could be retrofitted to current Gripen workstations.[20] One advantage with this approach is that it minimises the work required for authorisation and accreditation, as it would not entail any tampering with the Gripen system itself, but still enable Sweden to live up to its NRF commitments. Two other advantages are that the cost would be relatively low and that the solution could be in place within months. A distinct disadvantage, however, is that the current air gap would persist, meaning delays, typically in the range of minutes.

A second step would be to integrate CSD capability into the Gripen system itself. As the work would entail changing the system, this is a more far-reaching effort, probably taking more than a year to accomplish. However, such a measure would lead to the SwAF more fully living up to the expectations associated with its Gripen NRF commitments.

A third step would be to introduce CSD capabilities throughout the SwAF, for example adding a CSD module to the RPA workstations, through a robust, all-embracing CSD solution. Such a solution would probably need to include most, or all, of the items described below.

- A national Secret network. At the time of writing, there is no Swedish nationwide Secret network appropriate for JISR use, let alone any means of seamlessly exchanging Secret material with partners. However, current SwAF plans include the setting up of such a Swedish national Secret network, appropriate for JISR use, already in early 2019. This network would need to be interoperable with FMN.
- An interoperable tool to handle intelligence requirements, planning and tasking, i.e. Intelligence Requirements Management and Collection Management. Such systems could be had from several sources.
- A number of CSD servers, both centrally and at collection entities contributing large data volumes. There is a growing

The UAV Shadow 200 in flight – in Sweden referred to as UAV 03. Photo: AAI Corporation All Rights Reserved.

market supplying such CSD solutions, among them Swedish firms.

- Formalised, interoperable report formats compatible with those found in e.g. the NATO Message Catalogue (App-11).[21] Such formats are readily available to the SwAF through its co-operation agreements with NATO.
- Formalised, interoperable methodology. Such methodology is also readily available to the SwAF through agreements with NATO.
- Training and exercises in the JISR domain. Here, as the SwAF has a long-standing tradition of actively participating in NATO exercises, it can safely be assessed that the SwAF will continue to try to benefit from such JISR-related exercises and trials, e.g. Trident Juncture, Bold Quest and Unified Vision.

Whilst all the above measures would also contribute to information sharing at a national level, there might also be merit in seeking to move such an initiative forward in liaison with Finland to ensure optimal flexibility downstream.

Conclusion

Operationally, interoperability issues could be quite significant going forward. Could SwAF TAR today offer the same utility as it did in OUP? The current inability to provide a CSD-driven approach would most

certainly impact on its utility in time-sensitive terms. In today's more sensor-rich environment, the chief effect of this would be that Swedish intelligence products, not being available via CSD, would take longer to access than products available from CSD-capable nations. Consequently, it is assessed that, should something akin to OUP happen today, Swedish assets would be used less, and would be given lower priority tasks with less important time constraints. Notably, the lack of CSD architecture also means that SwAF units cannot access the vast archives of imagery that would most likely be generated, or receive time-sensitive data from other coalition assets, to the detriment of their own effectiveness.

TAR will inevitably play a prominent part in Swedish defence planning, which perhaps is natural for a small, non-aligned nation with limited resources and a strong focus on homeland defence. This TAR emphasis has been strengthened by the recent good use made of such capabilities in international missions such as Libya and Mali. It would therefore be surprising if SwAF TAR resources were to be further diminished, despite current economic strains.

That said, just like the rapid rise of RPA at the turn of the century became a necessity, interoperability and sharing will likely make similar demands on any nation, in or out of NATO, wishing to contribute to collective missions downstream as well as to ensure that, internally, the right information is rapidly disseminated to those that need it. So, given that the NATO JISR initiative, particularly its sharing philosophy based on exploiting CSD, could well become the operational norm, the timely codifying of what an alliance/coalition contributor needs to achieve in terms of interoperability would be a significant step forward, if not an essential precursor, to successful operations. With or without such codifying efforts, a number of avenues are already open to the SwAF on its journey towards JISR interoperability.

Robert Egnell is professor and head of the department of Security, Strategy, and Leadership at the Swedish Defence University. Major Johan Jakobsson, Swedish Air Force, is currently stationed at the Intelligence and Security Centre in Uppsala. Garfield Porter is Air Commodore (Retd) in the Royal Air Force, whilst Dag Åsvärn is a biologist, remote sensing specialist and Swedish Commando Reserve Major currently working as Operations Manager at Spacemetric, the Swedish company providing image handling capacity to both Gripen and the Swedish tactical RPA currently deployed in Mali.

Notes

1. Grahn, Jan-Olof: *Om Svensk underrättelsetjänst*, Medströms bokförlag, Falun 2016, p. 232 ff.
2. For the purpose of this article, unless otherwise stated, tactical RPA are included in the concept of Tactical Aerial Reconnaissance
3. *https://sv.wikipedia.org/wiki/Svenska_flygvapnet*.
4. Personal experience of Dag Åsvärn as Head Intel Section (S2) at the Swedish Second Kosovo Battalion (KS02) in 2000.
5. *Flygvapennytt*, No. 4 2003, p. 24 ff.
6. The NRF comprises four elements: Command & Control element based on a deployable Joint Task Force HQ; Very High Readiness Joint Task Force (VJTF); Initial Follow On Forces Group (IFFG) and, a Response Forces Pool (RFP). The Swedish contribution would be to this latter category.
7. *http://www.forsvarsmakten.se/sv/aktuellt/2014/11/peter-basar-over-ett-miniatyrflygvapen-i-nordic-battlegroup/*.
8. *http://www.forsvarsmakten.se/sv/var-verksamhet/internationella-insatser/pagaende-internationella-insatser/mali-minusma/*.
9. These are AeroVironment Puma and AeroVironment Wasp III, in Sweden together referred to as UAV 05.
10. The section on the Libyan campaign builds on Egnell, Robert: "The Swedish Experience: Overcoming the Non–NATO-Member Conundrum" in Mueller, Karl (ed.): *Precision and Purpose: Airpower in the Libyan Civil War*, RAND Corporation, Santa Monica, Calif. 2015, p. 309-338.
11. Quintana, Elizabeth: "The War in the Air" in Johnson, Adrian and Mueen, Saqeb (eds.): *Short War, Long Shadow: The Political and Military Legacies of the 2011 Libya Campaign*, RUSI, Whitehall Report 1-12, London 2012, *http://www.rusi.org/publications/whitehallreports/ref:O4F631FBA20DF9/*, pp. 31-38.
12. Keystone is an imagery processing capability produced by the Swedish company Spacemetric which, in addition to the Gripen, also provides imagery processing for SwAF RPA.
13. Hill, Matthew P.: "Operation Unified Protector", Unclassified EUCOM briefing, 2nd November 2011.
14. NATO JISR background can be found in Murray, Robert: "How NATO makes the Unknown Known" *JAPCC Journal,* Ed. 22, pp. 12-16.
15. Reconnaissance and Intelligence Report Form / Air Reconnaissance Requesting and Targeting Reporting Guide.
16. MAJIIC was a NATO-led, 9-nation programme to provide procedures, a service-orientated architecture and the understanding to allow compliant systems to interoperate thereby allowing collaboration on a broader and timelier scale. It also supported the development of Coalition Shared Data (CSD) platform.
17. Land, maritime and air.
18. TAR, Air Defence and Attack.
19. Battlefield Information Collection and Exploitation systems. Joint US/NATO project to integrate current and future intelligence networks. BICES coordinates and exploits battlefield intelligence gathering among all NATO commands and participating nations.
20. The Gripen Keystone can be retrofitted with a Keystone CSD module. Spacemetric has already built such a module, having been party to the MAJIIC process and follow-on JISR workstreams through its Dutch development office, contracted by the Netherlands MoD.
21. APP-11 provides users with a ready reference of messages and supporting tables commonly used in Joint, Land, Maritime and Air Operations.