The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.04

On the importance of continuous development in the military domain

Jonas Nordlöf
Licentiate of Engineering
Head of Department, Communications Electronic Warfare Systems
The Swedish Defence Research Agency
SE-164 90 Stockholm, Sweden
e-mail: jonas.nordlof@foi.se

Kristofer Bengtsson
Master of Political Science
Head of Department, Electronic Warfare Assessment
The Swedish Defence Research Agency
SE-164 90 Stockholm, Sweden
e-mail: kristofer.bengtsson@foi.se

Abstract. A significant percentage of modern products and systems purchased from the defense industry are difficult for the buyer to adapt or develop for new needs after lessons learned on the battlefield. This results in the procured systems having unnecessarily short lifespans. This paper contains a literature survey of the implementation and adaptation of military systems, combined with the authors' own observations from real cases of procurement in the military domain. Furthermore, this paper presents concepts for continuous development in the military domain, addressing several of the issues observed with modern systems. The term "continuous development" is here defined as the continuous modification, improvement and enhancement of military equipment or a military technical system over the course of its life cycle. The paper outlines how compatibility, flexibility and interoperability relate to unmanned aerial vehicles, counter unmanned aerial systems operations and electronic warfare operations, their role in continuous development and why these concepts are important on the modern battlefield. We contend that the ability to modify equipment increases adaptability, and therefore survivability, in conflict scenarios where new threats continuously appear. The paper concludes with recommendations of practical value for the defense industry on how equipment can be adapted to facilitate continuous development.

Keywords: continuous development, electronic warfare, EW, procurement, interface accessibility.

Introduction

As demonstrated during the Russian full-scale invasion of Ukraine it is hard to overrate the importance of versatile and potent military materiel as well as the flexibility in accepting and making use of said materiel. Many lessons can be drawn from this war, not only from a strictly military point of view but also from an industrial and government perspective with regard to how military materiel is produced and used. *Compatibility*, *flexibility*, and *interoperability* are key factors emphasized in this regard. Ukraine has received foreign military materiel and has, after a short training period, been able to put the materiel into good use on the battlefield. The creativity and innovativeness of Ukraine's use and integration of these systems (Jones et al, 2023) has at times even surprised the donating nations. This is indeed not only worthy of admiration but also clearly worthy of studies in the years to come: how did Ukraine achieve this effective implementation and what lessons can be drawn from it?

The authors suggest that one valuable lesson is the importance of continuous development in the military domain. The term "continuous development" is defined in this paper as the continuous *modification, improvement* and *enhancement* of military equipment or a military technical system over its life cycle.

Blakcori et al. (2024) note that procuring commercial unmanned aerial vehicles (UAVs) is often beneficial in the long-term provided that these systems employ open-architecture and modular systems, which are highly suitable for continuous development. For instance, the Ukraine-made Wild Hornet unmanned aerial system (UAS) can be customized to operate at different signal frequencies making it harder to jam by Russian electronic warfare (EW) systems (Roslin, 2023).

Experience from Ukraine also shows that almost all autonomous systems become obsolete over a six-week cycle due to enemy EW-tactics (Kaushal et al., 2023). Such systems then need to be modified or replaced. However, slow procurement processes can delay the acquisition for an extended period of time, well above the required six-week cycle, making these reacquisitions inadmissible at times. For such cases, development and modifications of available systems is the only viable option. For instance, procurement of counter UAS (C-UAS) systems by NATO and individual allies has been hindered for up to two years between the definition of requirements and contract execution (Borsari and Davis, 2023). Thus, the ability to conduct continuous development with military equipment and systems at hand is important because

(1) the systems will be adaptable to new threats and strategies,
(2) it enables the integration of lessons-learned from the front lines,
(3) it ensures that the equipment is relevant for a longer period of time, and
(4) it ensures soldiers' trust in their equipment, with regard to the before mentioned factors, thus increasing morale and overall combat efficiency.

As noted by Kaushal et al (2023), less focus should be put on designing a perfect system and more on continually adapting the software, frequencies and other aspects to keep ahead of the adversary.

Methodological Framework

This paper presents results and conclusions based on a literature survey of the implementation and adaptation of military systems, combined with the authors' observations and experiences from real cases of procurement in the military domain. The focus is specifically to investigate and evaluate the concept of continuous development for military applications with the purpose of identifying possible benefits and challenges.

Results

Military systems can be procured in several different ways. In recent years, there has been a transition from having a large set of technical specifications to instead defining a set of operational goals, or abilities, which need to be fulfilled. For the purpose of this paper, the authors suggest that procurements can be generalized into the following three broad categories:

- Category I: Buying off-the-shelf with limited ability to make changes in the equipment
- Category II: Buying off-the-shelf with access to modification capabilities
- Category III: Designing to specification

In order to integrate enhanced abilities in Category I equipment, it is often necessary to make new procurements. This can be acceptable for equipment with low cost and low survivability on the battlefield. However, this is seldom acceptable for other types of equipment, such as more advanced vehicles, *e.g.*, fighter jets, larger naval vessels or main battle tanks, due to the acquisition cost and logistical and infrastructural factors following in the wake of such enterprises.

There are several examples of Category I procurements where the equipment, not seldom highly advanced and therefore expensive, has become ineffective due to new threats. Since the buyers cannot

adapt Category I equipment to address these new threats by themselves, they must rely on the supplier to make the necessary changes. This is somewhat troublesome as specific threats, or other factors, might not necessarily be prioritized by the supplier. This could degrade the user´s trust and reliance in the equipment.

As new procurements are often needed in order to enhance the functionality of the original equipment, Category I procurements are not necessarily the best course of action. Therefore, national in-house development is often considered the only admissible approach in order to ascertain overall combat efficiency. However, this kind of materiel development is expensive and conducted at severe financial risk for the developing organization, especially if the equipment becomes too specialized due to national geographical and/or operational requirements.

Category III procurements have historically been common, especially in Sweden, with systems such as JAS 39 Gripen, CV90, Visby-class corvettes, submarines and the Archer artillery system. However, these tend to be quite complex projects with a high degree of risk for the developing nation and is therefore less prevalent today. Category II procurements therefore seem to be a viable cost-efficient solution. However, this requires that the supplier can provide potential buyers with a complete accessible interface, which enables national adaptations and enhancements for national specific demands and needs as they develop over time.

The authors argue that, to a greater extent, the concepts of Category II need to be integrated into equipment provided by the industry as these are not presently available in most equipment on the market today. This would enable national development of integrity critical systems. Furthermore, by making such equipment available, the suppliers will gain a commercial competitive benefit and the prospect of collaborations between military forces and the producing industry partner is improved.

UAV, C-UAS and EW-operations

This section emphasizes how compatibility, flexibility and interoperability relates to UAVs, C-UAS and EW-operations, their role in continuous development and how these are enabled by Category II equipment.

Compatibility: Experiences from modern military conflicts show that the effectiveness of UAVs depends on their integration into a wider military ecosystem centered on mutually supporting and enabling capabilities, such as EW, cyber, and intelligence gathering (Borsari and Davis, 2023). By providing the modification capabilities in Category II equipment to the user, this integration can be facilitated, through continuous development, even though the overall ecosystem is radically changed.

Flexibility: It has also been shown that, due to anti-radiation loitering munitions (Kasapoglu, 2020), the survivability of electromagnetic-radiating systems on the modern battlefield is low. Thus, reducing the time EW-systems spends emitting signals is crucial for the survivability of the system. Products bought off-the-shelf tend to have very general forms of jamming waveforms, the most common ways of jamming found in these products are barrage jamming. By using information of specific adversarial systems, gathered from different types of intelligence operations, more sophisticated jamming techniques can be utilized. As an example, utilizing knowledge about the 5G communication protocol, a denial-of-service (DoS) attack can be achieved on the 5G-system, which is designed for robustness and reliability (Rinaldi et al., 2021), by only jamming 0.1% of the OFDM subcarrier symbols (Lichtman et al., 2018). Similar results are expected to be obtainable for military systems.

In C-UAS and EW operations, classified information gathered through intelligence operations cannot always be shared with the industry. This often makes Category II procurement the only option, as modifications need to be performed by the military forces themselves in order to keep confidentiality, and as Category I often does not meet current and future needs. Furthermore, with highly flexible systems, approaches to handle new threats can be incorporated into current equipment.

The importance of this is underlined by lessons-learned from Ukraine, where critical systems need updates and modifications on a regular basis to keep ahead of enemy EW-tactics (Kaushal et al., 2023).

Interoperability: Even though new technology and new operations can be found on the modern battlefield, effective data management and interoperability across domains remain critical for the success of any military force (Blakcori et al., 2024). Whether unmanned systems are used to increase the precision of artillery (Kunertova, 2023) or to strike naval vessels (Sadler, 2023), they need to be coordinated with other domains in the battlespace.

In order for the industry to support these key factors in their products, increased focus and effort should be put on, (1) the use of highly compatible standards (compatibility) and (2) the ability for a user nation to modify threat and countermeasure libraries and mission data (flexibility). This technical compatibility enables interoperability (Moon et al, 2008), which in collective defense is of the utmost importance in order to, in turn, enable multilateral multi domain operations (MDO) within the realms of an overarching doctrinal strategy.

Interoperability and technical compatibility in an ever-changing world with ever-increasing geopolitical frictions have a great importance in the conduct of successful military operations. This is especially true in the defense of democratic and humanistic values against opponents with a total disregard for said values and who strive to achieve their agenda by any means necessary. Technological and operational adaptability together with allies is what enables success, this can be achieved in cooperation between government, academia and industry. This cooperation is also what needs to drive military innovation.

Alignment

In a larger perspective, military systems have developed from being hardware-defined, and thereby not easily altered without significant hardware modifications, to being software-defined, where, *e.g.*, the operating frequencies can be changed by a single line of code. This trend of software-defined military systems (Soare et al, 2023) makes the concept of *continuous development* even more appealing, as the modification of software can significantly increase the efficiency of military systems. Previously, the change might have included severe alterations due to the need for exchanging hardware components, which in turn could feed a need for redesigning the whole system to fit the new hardware. Software dependency is not all good, *e.g.*, increased need for experts at lower echelons to properly maintain and service the equipment, but the fact that certain changes to software can enhance a system's capabilities without changing the overall design is definitely one of the real benefits.

Continuous development of a software-based system is not necessarily without challenges between different actors and especially between nations with regard to the EW domain, which often is highly secretive in its nature. Although manageable, the exchange of data and information often needs to be accepted on the highest national decision level. To utilize the benefits of software-defined systems (and to some extent mitigate the challenges set out above), the key factors of compatibility, flexibility and interoperability need to be incorporated in the industrial product development, design and production. This can be achieved by implementing common industry standards.

The modification capabilities needed to enable continuous development range over several functions in a C-UAS or EW-system. In this paper we propose the following list of configuration or modification access needed for different purposes and capabilities:

- threat libraries for classification of emitters
- countermeasure libraries for dispenser systems and ECM waveforms
- modification of signal detection and signal estimation algorithms
- improving localization capabilities of surveillance systems

- sensor fusion and integration with command and control systems
- low-level access to data streams for detailed analysis

There are widely used standards that enable the above capabilities. Software standards such as SAPIENT (Sensing for Asset Protection with Integrated Electronic Networked Technology) (DSTL, 2021) and CESMO (Combined ESM Operations, NATO STANAG 4658) can be used to integrate systems and improve commander situation awareness. Data standards such as SigMF (Signal Metadata Format) (Hilburn et al, 2018) can be used for analysis and artificial intelligence. Data stream standards like the VITA 49 Analog RF-Digital Interface (Cooklev et al, 2012) are widely used for real-time signal processing and can be used to extend detection and other capabilities. Hardware standards like SOSA (Sensor Open Systems Architecture) enable modularity in hardware and extensive changes over the lifetime of a system (Collier et al, 2016).

Discussion

This paper is foremost aimed at addressing matters regarding procurement of military materiel and more specifically, materiel for UAV, C-UAS and EW operations. Interoperability is key and needs to be taken into consideration already at the design phase; will the system be compatible with systems from other, friendly, nations/actors?

Technical compatibility and flexibility not only enables continuous development in collaboration with others, but foremost it enables interoperability, which is deemed as essential for the efficient conduct of military operations in the (near) future (Weissmann and Nilsson, 2023). This, in turn, is driven by the overall worsening geopolitical environment, foremost in terms of the Russian war of aggression against Ukraine but also with regard to more increasing tensions between Western countries and Iran and China (Holmquist and Englund, 2020).

One way to enable continuous development is based on the adherence to standards and that partner countries and industry actors to a greater extent can engage in standardization processes and also agree on common standards. The adherence to common standards together with accessible interfaces would to a large extent enable partners to commit to continuous development. This could also feed the industry with new interesting business portfolios at the same time as the equipment stays relevant for a longer time. The overall combat effectiveness is also enhanced with less time spent training personnel on new, highly specialized equipment.

The immediate gains with using Category II equipment are assessed to provide a positive cost-benefit for governments and major industry partners. It also opens up the possibility for allies and partners to enhance already proven and potent military materiel to a lower cost. Lastly, Category II equipment would allow more experience to be pooled together to make equipment stay relevant in the face of time and emerging threats. This, in addition, is deemed by the authors to be cost reducing, as new materiel does not have to be procured to the same extent.

Conclusion

Given the geopolitical layout, interoperability is of the essence. One way to accomplish this is through technical compatibility. Technical compatibility, in turn, comes as a result of standardization, but can also be achieved through continuous development by partners and allies.

The industry embracing these factors is of the utmost importance. Applying a continuous development approach enables actors to conduct efficient procurement of military equipment that is capable of defeating the enemy today, tomorrow and beyond, without having to reinvest in new system designs.

The benefits for the industry also lies in the fact that if one user of a particular kind of military system has come up with a novel enhancement, this can benefit the original industry partner as well and might open up for new business collaborations.

This paper concludes that utilizing Category II equipment is considered the most beneficial

means of producing and procuring military equipment. This approach has several advantages over Category I and Category III, partly from an economic perspective but also from the perspective of compatibility, flexibility, interoperability and efficient conduct of military operations together with allies and partners.

Recommendations

The authors recommend all industry partners to increase the buyers' access to modification capabilities in military systems, thereby providing means for a continuous development of systems and to achieving a better outcome on the battlefield.

Acknowledgments

The authors would like to acknowledge the technical assistance of Per Brännström, Dr. Leif Festin and Simon Ahlberg.

References

1. Blakcori, N., Stathakis, L. I., Koutsoukos, L. D., Kirilov, L. K. (2024). The Evolving UAS Threat: Lessons from the Russian-Ukrainian War Since 2022 on Future Air Defence Challenges and Requirements. NATO, Integrated Air and Missile Defence Center of Excellence
2. Borsari, F., Davis, G. B. (2023). An Urgent Matter of Drones, CEPA. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/,Accessed March 10, 2024.
3. Collier, C. P., Lipkin, I., Davidson, S. A., Dirner, J. (2016). Sensor Open System Architecture (SOSA). In Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation. SPIE.
4. Cooklev, T., Normoyle, R., Clendenen, D. (2012). The VITA 49 analog RF-digital interface. IEEE Circuits and Systems Magazine, 12(4), 21-32.
5. Defence Science and Technology Laboratory, DSTL (2021). SAPIENT autonomous sensor system, https://www.gov.uk/guidance/sapient-autonomous-sensor-system,GOV.UK, Accessed March 10, 2024.
6. Hilburn, B., West, N., O'Shea, T., Roy, T. (2018). Sigmf: the signal metadata format. In Proceedings of the GNU Radio Conference (Vol. 3, No. 1).
7. Holmquist, E., Englund, J. (2020). China and Iran - an unequal friendship. The Swedish Defence Research Agency (FOI).
8. Jones, S., McCabe, R., Palmer, A. (2023). Ukrainian Innovation in a War of Attrition. Center of Strategic and International Studies (CSIS).
9. Kasapoglu, C. (2020). ANALYSIS - Five key military takeaways from Azerbaijani-Armenian war. https://www.aa.com.tr/en/analysis/analysis-five-key-military-takeaways-from-azerbaijani-armenian-war/2024430#, Accessed March 10, 2024.
10. Kaushal, S., Bronk, J., Watling, J. (2023). Pathways Towards Multi-Domain Integration for UK Robotic and Autonomous Systems, RUSI, Occasional Papers.
11. Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine, Contemporary Security Policy, 44:4, 576-591, DOI: 10.1080/13523260.2023.2262792
12. Lichtman, M., Rao, R., Marojevic, V., Reed, J., Jover, R. P. (2018). 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation. In 2018 IEEE international conference on communications workshops (ICC Workshops). 1-6. IEEE.
13. Moon, T., Fewell, S., Reynolds, H. (2008). The what, why, when and how of interoperability. Defence & Security Analysis, 24(1), 5-17.

14. Rinaldi, F., Raschellà, A., Pizzi, S. (2021). 5G NR system design: a concise survey of key features and capabilities. Wireless Networks 27, 5173–5188. https://doi.org/10.1007/s11276-021-02811-y
15. Roslin, A. (2023). Wild Hornets: Ukraine's Tiny Armor-Busting, Trench-Clearing Secret Weapon, Kyiv Post, July 8, 2023, https://www.kyivpost.com/post/19227, Accessed March 10, 2024.
16. Sadler, B. D. (2023). Applying Lessons of the Naval War in Ukraine for a Potential War with China. Backgrounder 3743, 1-13.
17. Soare, S. R., Singh, P., Nouwens, M. (2023). Software-defined Defence: Algorithms at War. The International Institute for Strategic Studies.