RHEA GROUP

Improving agility in defence capability innovation and acquisition of disruptive technologies in the space and cyber domains through process improvement and concurrent design

June 2021

Table of Contents

Authors

BGen (Ret'd) Robert Mazzolin
Chief Cybersecurity Strategist, RHEA Group

Sam Gerené
SEMT Business Unit Manager, RHEA Group

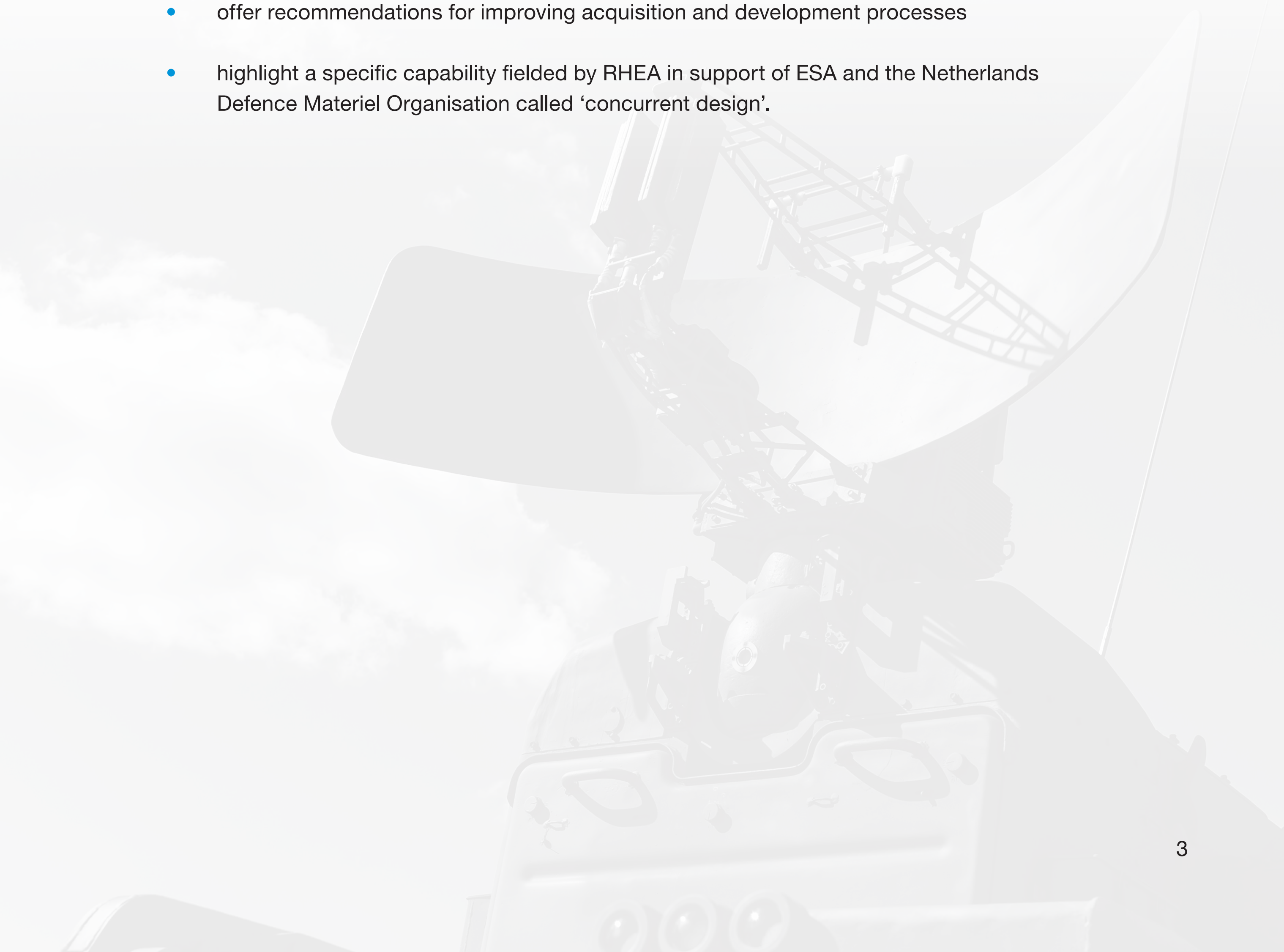
Introduction

Two core challenges impact military capability acquisition across environments that involve disruptive technologies, particularly in the emerging operational domains of space and cyber. Traditional acquisition approaches are too slow and rigid to keep pace with innovation and obsolescence cycles, and most procurement projects are too large and complex, introducing unnecessary risks for business and government.

Potential solutions to these issues fall within two areas. The first involves the revision of traditional acquisition models and processes supporting acquisition. The second involves the employment of technology in the form of concurrent design, currently employed within the European Space Agency (ESA) and the Netherlands Defence Materiel Organisation to support revised system engineering and design methodologies to address complex 'system of systems' technologies that comprise increasingly disruptive technologies.

This paper will:

- highlight some key challenges facing defence regarding the acquisition of cyber and space capabilities impacted by disruptive technologies
- offer recommendations for improving acquisition and development processes
- highlight a specific capability fielded by RHEA in support of ESA and the Netherlands Defence Materiel Organisation called 'concurrent design'.



The relationship between technological innovation and military advantage, and the disruptive technology challenge

The rapid evolution of, and military dependency upon, technologies over the past 30 years has radically altered the symmetry of military power between competitors. This poses new disruptive technology challenges for military institutions and the associated defence industry that challenge traditional development and acquisition approaches. They have rendered outdated many current policies, doctrines and organizations of respective actors, thereby requiring wholesale reinvention of current tactics, doctrine and capability development, acquisition and fielding approaches.

The relationship between disruptive technologies and their application to the defence industry may be characterized as either ‘sustaining’ or ‘disruptive’. Sustaining involves the gradual development of existing technology. Disruptive technology, on the other hand, invokes a revolutionary impact, with implicit risks associated with new, untested, scope-limited considerations, thereby creating challenges for innovators.

In the defence and security domain, disruptive technology environments arise from the expanding use of robotics, advanced sensors, augmented reality, wearable tech, the ongoing information revolution, artificial intelligence (AI) and the Internet of Things (IoT) etc. These combine to rapidly impact traditional C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) systems by becoming the Internet of Battlefield Things, ubiquitous robots, bot swarms/mixed teams, augmented human soldiers, automated decision-making, cyber warfare, disruptive technology weapons and increasing emphasis on space-based assets and capabilities. It is anticipated that all of these will be fielded by 2050 because the various components required to enable such developments already exist and are undergoing rapid evolution.

Clearly, future warfighting will be dominated by information technology. As the speed of technological development accelerates, it will revolutionise warfare and competitive edge will dominate the state-level arms race. As the military is traditionally the deliverer of kinetic effects, rather than technological innovation, this increased competition will force it into greater co-operation with commercial civilian industry to seize and maintain a tactical advantage.

New geo-political strategic risk

A new risk category has been introduced in national policy considerations related to technology development; specifically, the economic and financial (E&F) technology hybrid operations of non-democratic governments. These are defined as activities in the international trading and financial systems often conducted for strategic, rather than purely commercial, purposes.

Currently, China and Russia are the primary actors in such activities, particularly in the areas of space and cyber hybrid operations on a global scale, which are free of democratic debate, processes and election cycles. State-owned or controlled enterprises of these state actors often serve as forward deployed assets, executing

space- and cyber-related partnerships and thereby managing to steal innovative Western technologies and implement them through much quicker and less risk averse processes. They forge international defence and security industry partnerships that involve the purposeful building of vertically integrated dependencies, often on a sole-source supplier basis. This opens the targeted countries to partial or complete sector capture, which is ultimately designed to limit the freedom of action and independence of the recipient state's space sector.

The authoritarian nature of these governments enables them to pursue strategic objectives in relation to space partnerships, free of time-consuming constraints faced by democratic governments. In some cases, control over space and cyber sectors also has downstream strategic value as it delivers influence over other sectors that depend on, or benefit from, cyber and space capabilities, such as agriculture. This influence can, in turn, translate into wider political influence over the country.

Acquisition challenges in association with traditional processes applied to space and cyber capabilities

Since the fall of the iron curtain, defence funding in many nations has varied significantly in response to an evolving political climate that has deprioritized defence spending, resulting in declining budgets. Responses to international crises and recent conflicts in Afghanistan and Iraq, along with the increased threat posed by hybrid warfare techniques, have required rapid investment and the re-initiation of acquisition activities. This has placed pressure on organizations that have lost the necessary competencies in this realm. Consequently, an expedited design and requirements elicitation process supported by revised techniques, such as concurrent design, offers significant benefits.

The challenges around acquisition have a number of aspects. One key element relates to the competencies of procurement professionals, given the requirement for new skills and training to keep pace with cyber and space innovations and modern procurement practices better suited to cyber and space. Government and industry have been slow to align on solutions to these challenges and closer industry–government dialogue and collaboration are essential.

NATO allies are currently involved in ongoing cyber conflict that affects the public and private sectors, democratic institutions, the military, security agencies and citizens. Every day national security authorities are blocking malicious actions aimed at federal systems, databases and websites, and attempts to access and infiltrate government networks. Networks related to research and development, science, engineering and acquisition have been attacked and compromised on many occasions since the early 2000s.

In response, a number of nations have built strong cyber capabilities to counter threats associated with this emerging landscape, recognizing the intrinsic nature of collaboration between government and industry, extending to critical infrastructure and the defence and security communities.

The private sector plays a different and enhanced role in provision of cyber- and space-related capabilities for defence compared with its role in traditional defence.

Today's industrial base enables a speed of innovation and attack that is faster than that found in the delivery of traditional defence capabilities. Industry plays a greater role in fundamental technical innovation and an increasingly greater role in delivery of capability and support to operations. Further, industry is the owner and operator of the majority of the cyber and space environments, including the underlying networks and enabling technologies. Consequently, the delivery of operational military and related national strategic effects represents an accentuated combined effort that is unique to the cyber and space technology environments.

This industry–government dynamic in the field of cyber and related technologies highlights the need to counter threats collaboratively because the cyber environment presents a unique risk profile and calculus that challenges current procurement approaches. Adversaries can field new capabilities from initial concept in 10 months or less, so the perceived benefits of taking time to thoroughly de-risk and compete procurements may be outweighed by the potential damage caused by an undefended attack. This highlights a core challenge of cyber procurement, which is that rigid requirements prematurely cemented in technology become obsolete well before an operational solution is delivered many years later.

To that end, the development of cyber capabilities is best achieved by decomposing large problems into smaller, more discrete elements, which further aids in de-risking delivery.

As the pace of expansion of new cyber knowledge, technologies and practices accelerates, so do cyber technology innovation cycles and the development cycles of adversaries, leaving established government acquisition protocols inadequate to match them. Western governments must develop new approaches to aggregating the various areas of expertise, technical competencies and knowledge and more progressive and expeditious ways to develop and acquire capabilities. The pace of cyber technology innovation places a premium on continuous reskilling and training, and constant knowledge exchange between government, industry and academia.

Acquisition and its relationship to sustained collaboration

An effective procurement ecosystem for cyber capabilities requires a combination of a clear regulatory environment, adaptable norms and revised culture in order to support a productive and collaborative relationship between government and industry.

There is always a risk that if procurement processes cannot improve, selected sectors of industry may decide to retain their best products and services exclusively for other countries and customers who demonstrate an interest and ability to acquire them in a timely manner. This is of particular concern when considering a strategically competitive environment where the effectiveness of a capability is degraded with use (for example a unique/proprietary vulnerability or the exploit of an adversary's system). The failure to improve cyber acquisition potentially undermines the NATO Alliance's security and limit its access to the most advanced cyber innovations and technologies.

Increase the pace of innovation by streamlining the acquisition process and the adoption of agile development methodologies

Most military cyber procurement faces significant challenges. Three consistent factors contribute to sub-optimal outcomes. The first is that the cyber procurement process is too slow and rigid to keep pace with cyber innovation and obsolescence cycles. Secondly, most cyber projects are too large and complex, introducing unnecessary risks for business and government. Finally, procurement professionals need new skills and training to keep pace with cyber innovations and new procurement practices that are better suited to today's requirements.

A number of fundamental principles apply to ensure cyber capability acquisition is successful. Firstly, it is imperative that operational and technical authorities are engaged early, remain committed to the initiative and enforce the delivery of incremental results within short cycles (10 months). To that end, operational requirements need to be rapidly pre-validated – and periodically re-validated – by end-user clients. Industry may then be trusted with significant leeway to propose creative, innovative solutions. With this approach, the business case and scope of work will remain manageable as the project evolves.

In addition, administrative and procedural overheads need to be consolidated and simplified, and communication between public and private stakeholders must be direct and consistent. One key challenge here is that the turnover of core team members in public sector programme management organizations needs to be minimized over the lifetime of a project so that key public servants fully understand the operational systems and requirements. Finally, strong executive support is needed to ensure funding remains available. These success characteristics are vital for military cyber and space procurements but also applicable elsewhere.

The application of industrial-era acquisition processes to digital era requirements remains prevalent in defence. The challenges apply most significantly in the 'options analysis' and 'implementation' stages. Although locking requirements at the options analysis stage makes sense for traditional procurements, it introduces unacceptable costs, risks and delays for rapidly evolving cyber technologies.

Procurement strategies and related documentation need to be updated to reflect a more iterative approach to procurement, one that prioritizes smaller and steadier progressions of deliverables and eliminates the current approach that one entity 'wins' the delivery of an entire programme of capabilities. Such an approach would break down complex projects into manageable subsets of tasks to address requirements. These would embrace increasing levels of sophistication and scale over time, and result in a series of deliverables, with multiple options to replace non-performant technologies or suppliers, or to incorporate emerging innovations.

It is important to differentiate within programme environments to identify mission-critical capabilities and key technology areas that have sufficient specificity to merit development of prototypes. This needs to be accompanied by detailed, aggressive development and implementation plans that move technology from concept through to deployment for specific platforms and applications.

A modified approach involves increasing emphasis on demonstrations, prototypes and minimum viable products in support of bid submissions (as opposed to highly detailed and rigorously specified requirements) in order to demonstrate bidder compliance with requirements and the ability to deliver viable solutions before moving to full-scale delivery. An emphasis on experimentation leads to greater competition, which further de-risks procurement processes for both industry and governments. Such staged progression from proof of concept, through prototype, to scaled testing provides opportunities to re-evaluate technologies and companies, and remove and/or engage new ones as required. Meanwhile, financial compensation is regulated through a progression of increasingly complex, meaningful deliverables over time that reduce the financial risks of failure to government and industry. A programme such as this, which is focused on outcomes and considers a diverse range of potential approaches, increases the range of solution options for governments and would result in the fielding of technology in much shorter timelines.

A complementary approach involves maintaining the flexibility to upgrade cyber capabilities over the programme's lifecycle by establishing umbrella projects for ongoing capability improvements, where funding may be reallocated among sub-projects by programme sponsors. These early-phase projects comprise discretely sized requests for demonstration or proof of concept. Later phases increase in technological sophistication and scale of deployment. Such prototypes and technology demonstrations should be prioritized over paper-based submissions and testing and validation phases backed operationally and financially by military sponsors.

Approval processes for programmes typically involve the engagement of different functional authorities over various standard gated project phases: identification, options analysis, definition, implementation and close out. The simple scheduling of meetings associated with the required reviews at each stage, often across months or as long as 1 year, lead to timelines in the order of 7 to 10 years, which is far from the desirable 10-month deployment cycle.

Finally, there needs to be increased emphasis on educating and training programme managers in emerging streamlined acquisition processes, as these may not be widely known or understood. Acquisition professionals and project managers supporting cyber-related capabilities require new skills in order to accomplish their responsibilities. Such soft skills involve the development and management of collaborative arrangements between industry and government to ensure strong mutual understanding of the operational and associated technical aspects of the target environments and to manage innovative approaches to showcase developing capabilities and engage with start-ups.

It is also increasingly important to understand the nature of evolving and converging technologies and their impact on the target operational environments. Further, increasingly strong technical skills are required in order to engage with operators involved with real problems, in either live or simulated environments, in order to better appreciate implementation and interoperability considerations.

Concurrent design – Technology in support of acquisition and system design in the space and defence sectors

One capability that has been successfully developed and applied by RHEA to highly complex space and defence systems is concurrent design, which is a technique derived from model-based systems engineering. This is an approach developed at ESA to improve the efficiency and rigor of a system design in the early design phases. It improves efficiency, provides more transparency in design choices and improves the communication of engineering information between the different stakeholders.

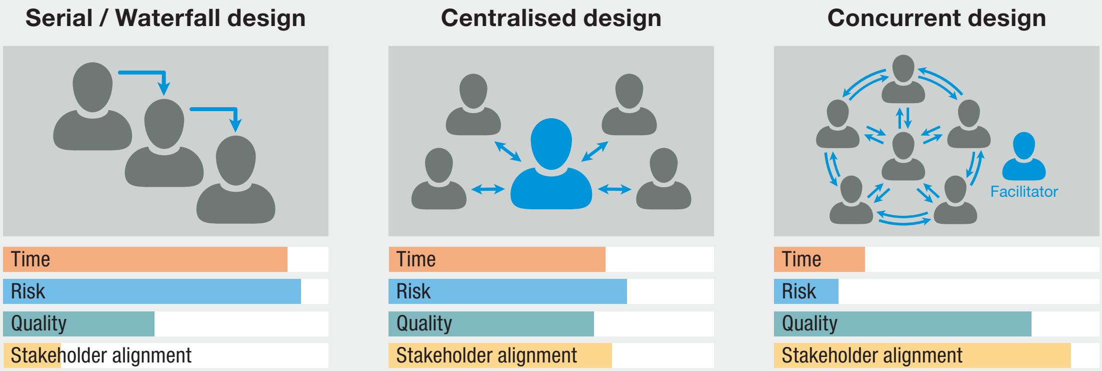
After demonstrations of the method and visits to facilities at ESA and a commercial yacht builder in the Netherlands, the Netherlands Defence Materiel Organisation (DMO) acquired this capability in September 2019. Early estimations show an efficiency improvement of over 200%. More importantly, an improvement in quality and rigor was noticed by the leading engineers, despite the fact that due to the COVID-19 lockdown, work sessions had to continue online.

When complex programmes involving multiple space and non-space missions cooperate to deliver better overall capabilities – forming a system of systems (SoS) – additional challenges present themselves. These include differential evolution of infrastructure and instruments, emerging needs and system behaviour, interface and governance issues. The resolution of such challenges may be achieved through the use of progressive design methodologies such as ‘generative design’ (GD). This is also referred to as ‘computational design synthesis’ (CDS), a solution for autonomously generating design alternatives. In CDS, the user first expresses the potential designs in terms of goals and constraints and a computer then generates design options; the user then explores the evaluated options to select the optimal solutions.

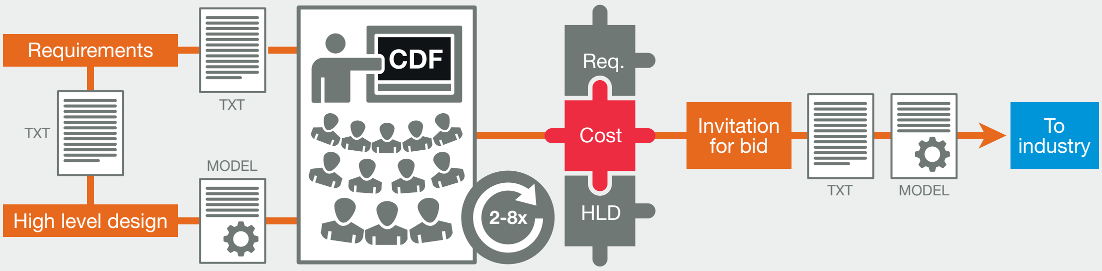
For much of the 20th century, the defence sector played a leading role with respect to technology innovation. This is no longer the case and in many areas defence lags industry. Defence must adapt and find alternatives that will help to close the widening technology development gap between defence and commercial industry.

An important part of this process is for defence to look beyond its own borders for

Defence
Public sector
Multinational
High-risk environment
Complex projects
Technology intensive
Space



▲ *This diagram shows the evolution that ESA took from the 'classic' waterfall approach through centralized design and then ultimately to concurrent design. ESA has been successfully using concurrent design since 1999.*



▲ *The concurrent design process is quite different from the waterfall process. Requirements, design and cost estimates are all 'locked down' at the same time. This allows the requirements to be adapted so that they meet the user requirements and also results in an optimal design.*

non-traditional solutions provided by non-traditional actors. One obvious choice is the space sector and, more specifically, ESA. The overall success rate of complex space missions executed by ESA is significantly higher than that of complex defence projects. Furthermore, ESA is public sector, multinational, deals with complex projects that have to work in a harsh environment and has a mandate to outsource much of its work to industry.

To that end, concurrent design is a 'best practice' already embedded in the culture of the space sector that is now gaining a foothold in defence, and could transform defence capability delivery in the same way that it has benefitted space organizations since the early 2000s.

Currently, most defence establishments use a documentation-heavy, serial process throughout the project lifecycle that imposes excessive costs and results in long project lifecycles, negatively impacting the quality of the final product and particularly the procurement of IT systems that have a limited lifespan and benefit from rapid delivery.

The most serious problem is that written documents are subject to interpretation and complex user requirements are extremely difficult to capture. Further, lengthy requirements documentation often includes incomplete, ambiguous and conflicting requirements. Project managers frequently work under considerable time pressure. They therefore face challenges when they need to seek clarification from the authors of the original requirements as they fear such consultation will introduce delays. Consequently, project teams make assumptions that can seriously undermine the quality of the final product. Once requirements are 'locked' prior to the design process, trade-offs are no longer possible, resulting in designers having less latitude to consider more suitable alternatives that would be more cost effective or quicker to implement.

ESA has addressed many of these challenges through the concurrent design (CD) process, resulting in a reduction in the time required to complete a high-level design by a factor of four and the cost of such activity by a factor of two. Further, in a longitudinal study that reviewed 30 projects before and 30 projects after ESA started using CD, ESA determined that the number of engineering change proposals (ECPs) during project execution was reduced by more than 30%. This is significant as it means projects are executed more quickly and inexpensively. Also, it enables ESA to provide industry with better specifications, which in turn enables industry to provide more accurate bids against higher-quality specifications.

One benefit for defence is that CD is consistent with current defence protocols, with high-level requirements being the starting point for all projects, which are then given to teams who translate the requirements into a high-level design. One difference from typical defence projects, however, is that the requirements are not ‘locked down’, thereby providing opportunities to adjust the requirements later during concurrent design sessions.

Once the initial high-level design has been completed, all of the stakeholders are physically gathered at a concurrent design facility (CDF). During such CDF sessions, there is direct engagement between the designers and engineers and the end-users of the capability being developed. This provides invaluable opportunities for designers to ‘get into the heads’ of the end-users and for designers and end-users to discuss potential trade-offs to achieve an optimal design.

Such sessions enable conflicts to be quickly resolved through discussion; where certain issues require further consideration, they may be ‘parked’ for later consideration. It should be noted that when any conflict arises in a CDF session, a similar conflict would have presented itself in the serial process used by defence. However, in a serial process staff are not working concurrently and therefore any conflict would potentially not be identified. This would result in it going unresolved and, in turn, lead to a weaker specification, with the resultant added project time delays and cost.

CD sessions give all stakeholders the opportunity to present their specific domain areas with active engagement by the customer, facilitating the parallel evolutionary tailoring of requirements alongside the optimization of a design. The stakeholders at these sessions may at times include representatives from industry, who contribute the ‘design capability’. Multiple domains of expertise are taken into account, with cost, risk and planning typically part of all CD activities. The resolution of conflicts between requirements and design at the earliest stages in CD projects has enabled ESA to achieve a reduction in downstream engineering change proposals by more than 30%.

Models are an essential part of any successful CDF activity as they evolve over time to capture key elements of each of the domain areas covered. Explicit models enable design teams to achieve a level of consistency and quality from project to project that is impossible to achieve with projects that are designed in isolation, as is the case with many defence projects. In most cases, the models are contained within Microsoft® Excel® spreadsheets. Although helpful, it only provides a partial solution. Consequently, RHEA Group’s COMET™ software suite plays a vital role as it is a unique open source software product that

▲ *RHEA Group's COMET™ software platform comes in both a freely available open source version and a commercially supported Enterprise Edition, giving organizations the choice of saving money or optimizing their use of the software through professional support.*

allows the models to be both configuration managed and synchronized.

COMET enables complex system interdependencies to be modelled and permits changes in one part of a mission element to be cascaded in near real-time to reflect its global impact on the rest of the mission. Such near real-time updating of models saves an incredible amount of time and ultimately results in much higher quality design. In the context of the Netherlands DMO, multiple models have been created to support the integrated logistics support (ILS) domain for maritime and land-based platforms. These models are reusable for future projects and therefore will, over time, further increase the speed of the decision-making process.

There are many common elements between space and defence environments. This commonality is being accentuated by the identification of space and cyber as operational domains within the NATO defence community. However, it is important to carefully consider the characteristics and constraints that differentiate the defence environment from traditional space missions.

One such area is models, where the unique characteristics of military-specific disciplines – intelligence, situational awareness, operational planning, logistics, command and control, air, land and maritime, special operations and cyber as a military discipline – must be accounted for. Further areas include more generic aspects of any defence IT project such as interoperability and federation, cybersecurity, information security, data modelling, network environment, human machine interface, training, testing, computational and storage infrastructure, adaptive operations and maintenance.

Consequently, a defence CDF (D-CDF) would support a broader range of activities, including capability development, complex defence project troubleshooting and military exercise planning. An additional activity would be multinational defence requirements arbitration, a process whereby nations come together to develop commonly agreed high level requirements to meet specific operational challenges. Here, a D-CDF would offer a particular benefit, given the complex interplay associated with respective national sovereign defence interests and the need to achieve economies of scale.

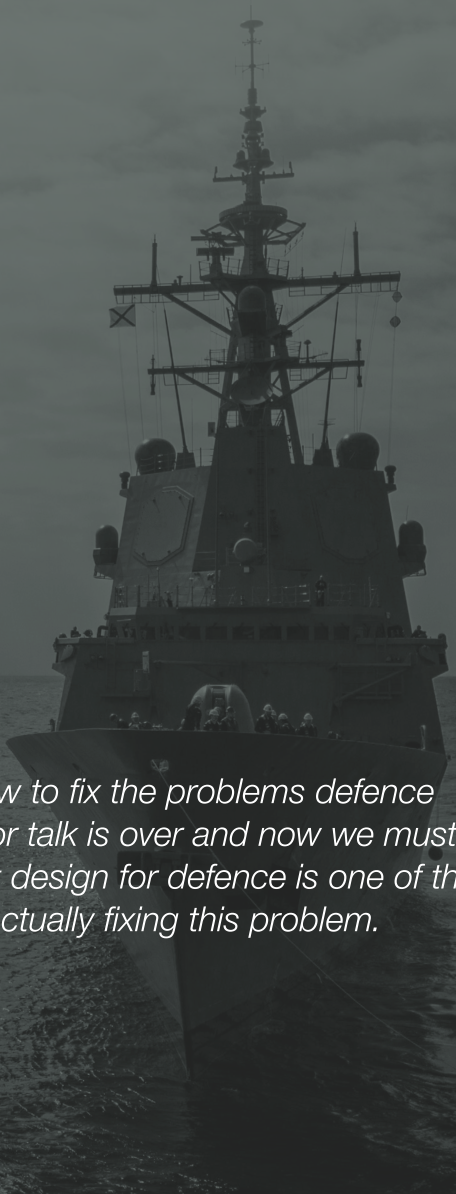
To that end, the Netherlands DMO has contracted RHEA to roll out the concurrent design process and a dedicated concurrent design facility in a 3-year programme. The RHEA concurrent design process is now in place, adapted where required for the specific needs of the defence industry. The DMO workforce is being trained both 'on the job' and through a dedicated training programme, as are its industrial partners. The aim is that they will become self-sufficient in applying concurrent design. In addition, the intent is that a potentially larger effort may be developed that will bring in other nations and potentially support broader NATO activities by creating an expanded D-CDF capability.

Conclusion

Defence faces unprecedented challenges in the rapid acquisition, development and fielding of cyber- and space-related capabilities, which are increasingly impacted by, and dependent upon, disruptive technologies. These challenges are further complicated by a confluence of the increased reliance on the private sector and industry for the provision of dual use technology supporting critical military capabilities and hybrid operations by hostile foreign actors.

Traditional approaches in this domain must be replaced by more flexible acquisition processes based on new contracting models to expedite technology system development that better meshes with software design methodologies such as Agile development. Such enhancements would enable agencies to rapidly modify a project or a design well before its final stages, saving time and money, and ensure solutions meets end-user needs. The use of alternative acquisition models, combined with new software tools and capabilities such as concurrent design, currently in use within the European Space Agency and the Netherlands Defence Materiel Organisation to help manage technology-based programmes, can ensure organizations meet their operational needs in a faster and more agile way.

Such amendments to existing approaches, and the employment of alternative processes, are dependent on a change in acquisition culture, which involves significant institutional transformation and development within the programme management and acquisition communities. Such protocols align very closely with iterative, Agile development in software environments, enabling organizations to incrementally work through a development process until it achieves the desired end state. The key focus must be on ensuring that allied forces' capabilities are superior, stronger, faster and more lethal than those of potential adversaries.



> *There have been countless studies on how to fix the problems defence has in acquiring new systems. The time for talk is over and now we must act. The project to implement concurrent design for defence is one of the most promising steps I've seen towards actually fixing this problem.*
>
> **Vice Admiral AJ. de Waard**

References:

- “The Innovator’s Dilemma”, Clayton M. Christensen; Harvard Business School, 1997

- Report for the Center for a New American Security (CNAS), Ben FitzGerald and Shawn Brimley

- State Actor Strategies in Attracting Space Sector Partnerships: Chinese and Russian Economic and Financial Footprints, March 31, 2019, Prague Security Studies Institute

- www.nato.int/docu/review/2013/cyber/timeline/en/index.htm

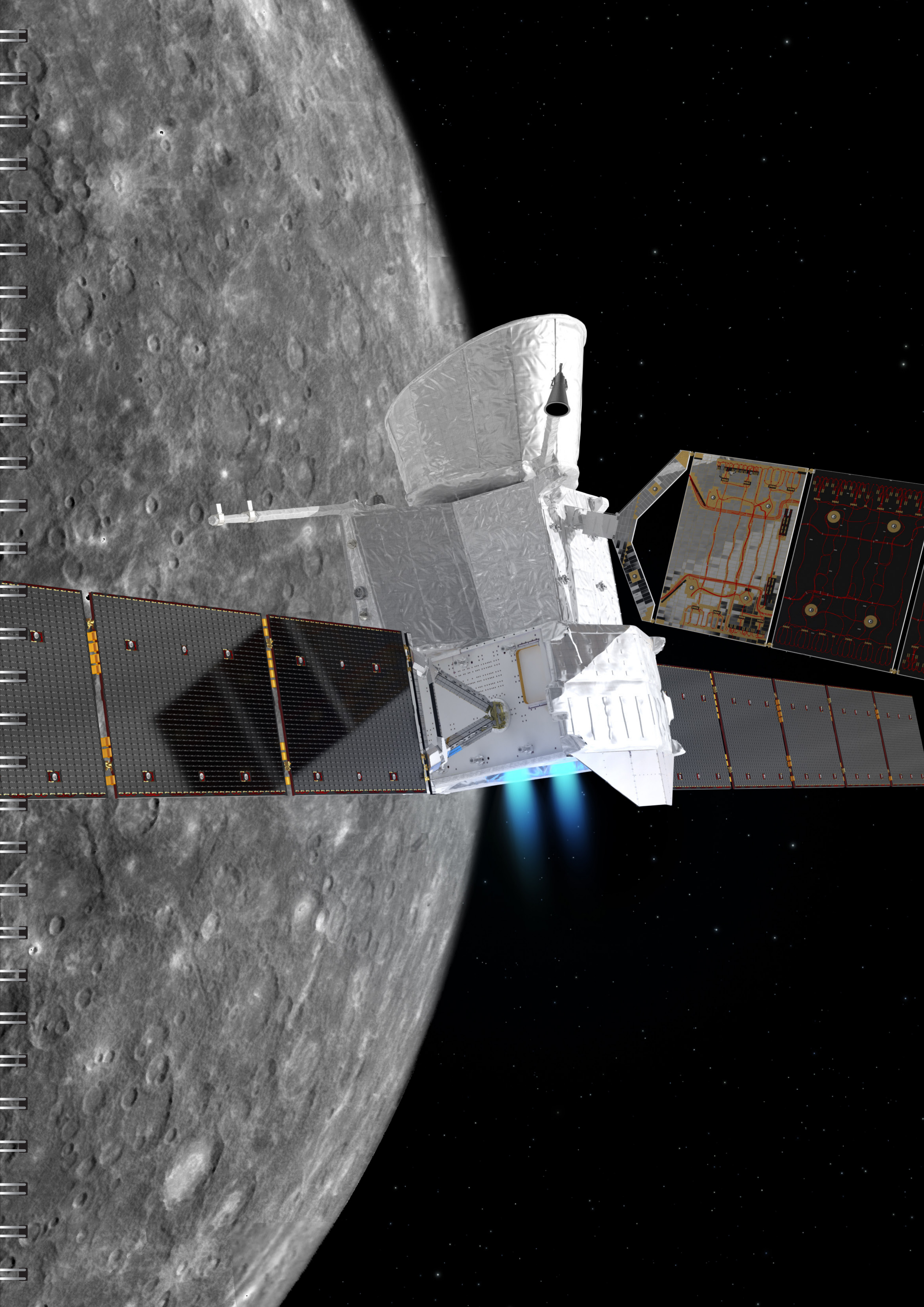
- Army Modernization Strategy, US Army, 2019

- Small Business Strategy, Department of Defence, 2019

- Small Businesses Behind Defence’s Biggest Projects Recognized, Ministry of Defence, 2018

- D-CDF: Adapting ESA’s Concurrent Design Facility for use in the Defence Sector; J. White, S. Gerené; SECESA 2018

- “Procurement at Cyber Speed”, CADSI 2021 Report.



RHEA
GROUP

About Us

RHEA Group is a privately-owned professional engineering and solutions company, providing tailored engineering solutions, system development and security services for space, military, government and other critical infrastructure organisations. Since its creation in 1992, RHEA has built a reputation as a trusted partner, developing tailored solutions that help drive organisational and cultural initiatives, leading to sustainable added value for its customers.

Headquartered in Belgium for its European operations and in Montreal for its North American operations, RHEA Group employs over 600 people and has offices in Belgium, Luxembourg, UK, Czech Republic, Italy, France, Germany, Spain, Switzerland, the Netherlands and Canada and works at clients' premises throughout Europe and North America. RHEA is ISO 9001 and ISO 27001 certified.

✉ info@rheagroup.com

🌐 www.rheagroup.com