

SDE NEXUS

COMPLEX CAPABILITY. DELIVERED AT PACE.

Overcoming the challenges of delivering UXV and hybrid capability at pace

POSITIV+
COHORT



Positiv Cohort

UK sovereign Defence SME delivering specialist engineering and integration resource in products and tools to help businesses deliver complex capability at pace.

Whether you are a start-up or SME seeking to scale / enter the UK, or a Ministry of Defence / Defence Prime looking to deliver that step change in agility now, we deliver that complex capability at pace, with all the governance and accountability you would expect on a critical programme.

"Positiv Cohort's team brought the secure agility and speed needed to innovate within a highly constrained environment. When one route was unavailable, they found another compliant way to keep the work moving."

Data & AI Engineer | Secure Defence Programme

"Positiv Cohort's team had the right experience to understand what the programme needed, ask informed questions and begin contributing within days. They also brought a broader perspective on how similar challenges had been approached elsewhere in defence."

Capability / System Engineer | Complex Weapons Programmes

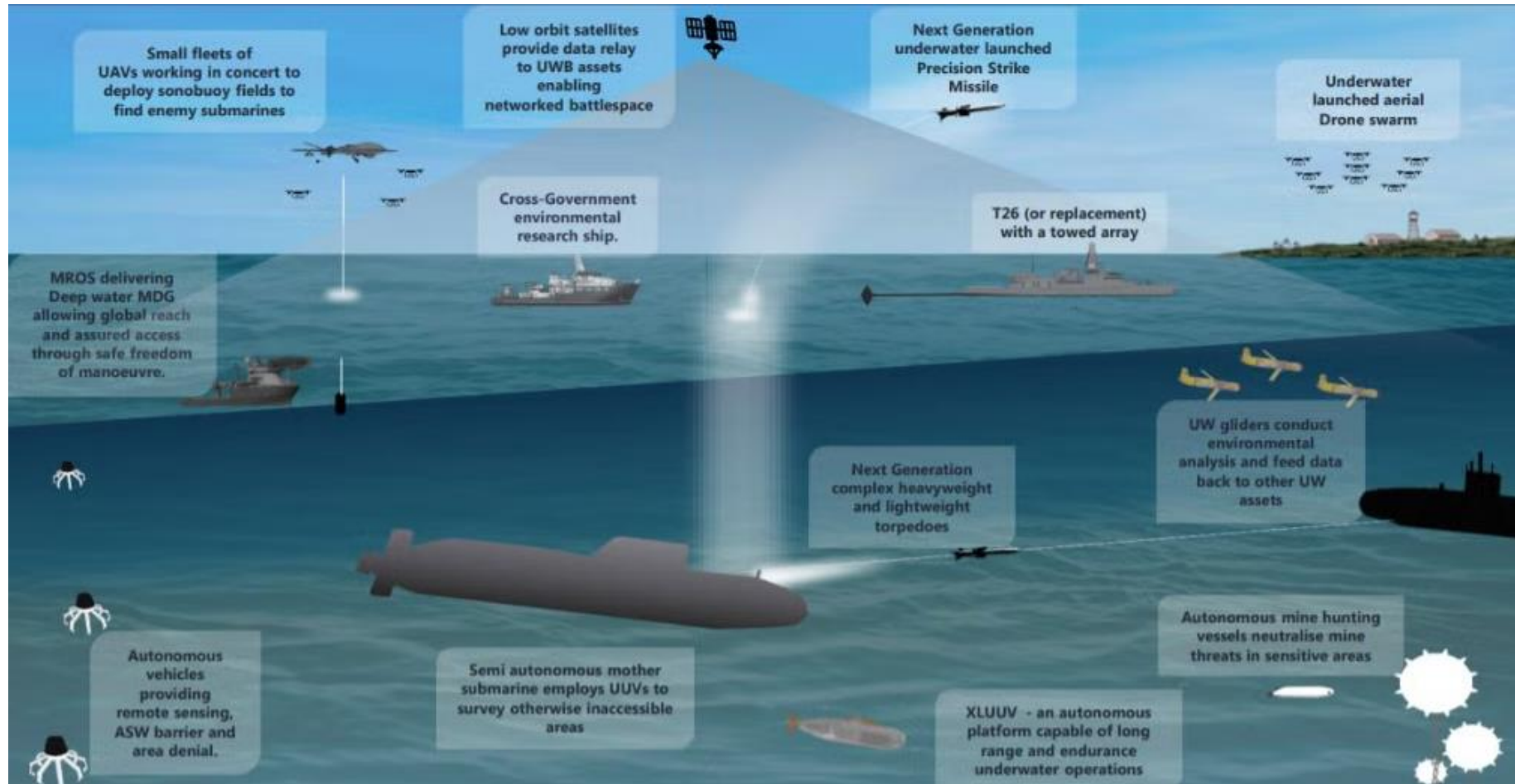
"Positiv Cohort's team brought the experience to see what the programme would need next, put stronger controls in place and help the leadership team maintain progress as priorities evolved."

Project Co-ordinator | FCAS Programme



So let's look at an example of what the Defence Investment Plan (DIP) envisions

UXV and Hybrid Capability – The Growth in the DIP



So let's look at the challenges this creates

“More, lower-cost, uncrewed and hybrid capability into operational use at pace”

One of the core challenges of the UKMOD's DIP.

At first glance, a straightforward ask, but dive a little deeper:

- Increased number of complex systems to be delivered in a shorter timeframe
- Demand increase putting SQEP under further pressure than they already are
- Increasing the pace of UKMOD, some primes, without changing culture or decision-making processes
- Transitioning from List X to FSC, lowering thresholds for S and TS classifications, increasing demand on infrastructure
- Much shorter acceptance trials, including system and component cyber security
- Many, new, complex systems being introduced at speed, and spiral developments, will increase training burden substantially
- Rapid evolution meaning systems become obsolete more quickly, shorter lifecycles
- At which point do complexity and availability intersect? e.g. When would minimally crewed be preferable?
- With most nodes becoming ISTAR assets, networks will see an order of magnitude increase in data flow
- SATCOMS are critical, but a potential point of failure with the growing threat in space
- Edge processing can help with network data flows, but what can be done on a UXV that is vulnerable to capture?
- Vulnerability of UXVs to capture and the Trojan Horse risk via CBRNE or cyber, “surprise payloads”



Let's consider how we can address these points

Increased Demand and Pace, SQEP shortages

Driven by:

- Increasing threats to UK
- Increased number of complex systems to be delivered in a shorter timeframe
- Demand increase putting SQEP under further pressure than they already are
- Increasing the pace of UKMOD, some primes, without changing culture or decision-making processes

Basically, we are going to be doing more, with less, in a shorter timeframe

How do we address this?:

- We need different processes to be able to move quicker – but culture takes time to change, which we don't have – so how?
- Firstly, We don't shorten the decision points, we shorten the admin tasks between those points using tools.
- Secondly, if there are too many decision layers (larger primes) we can offer them a thin prime position

What do we need in our toolbag as SME's?:

- The tools needed to deliver projects at pace - e.g. Mission+Assured project automation tool
- The specialist SQEP and solutions
- A close-knit ecosystem of SMEs, Primes etc. bringing insights and reach



Now let's look at some of the bottlenecks in security and testing

Bottlenecks in Security Infrastructure & Testing

Driven by:

- Transitioning from List X to FSC, with many List X facilities not compliant with FSC – work will be required
- Lowering thresholds for S and TS classifications, increasing demand for infrastructure/clearances – facilities and SQEP shortages
- Much shorter acceptance trials, including system and component cyber security

How do we address this?:

- Quicker routes to FSC facilities, whether getting ahead of the curve and/or acquiring temporary facilities.
- As mentioned on the previous slide, a clearance bottleneck will mean SQEP will be in short supply and need to be more productive
- System and component cyber security will need to be drawn down into the supply chain – no time for in depth review at acceptance

What do we need in our toolbag as SME's?:

- The tools needed to deliver compliant projects at pace – e.g. Mission+Procured component cyber security tool
- The specialist SQEP and solutions – e.g. Mission+Secured leased temporary secure facilities, SDE, etc.
- A close-knit ecosystem of SMEs, Primes etc. bringing insights and reach



What other changes will be needed to deliver UXV and hybrid capability into service at pace?

Need for a new training model

Driven by:

- Many, new, complex systems being introduced at speed, and spiral developments, increasing the training burden substantially
- Growing pressures on military personnel due to low numbers and increasing threats, reducing availability for training

How do we address this?:

- Firstly, moving away from waiting for numbers for face-to-face courses to begin
- Secondly, training delivered digitally with human oversight ref areas for improvement – a hybrid model?
- Finally, delivery where the individual is serving – even at the frontline

What do we need in our toolbag as SME's?:

- The tools needed to deliver training / training updates at pace - e.g. Mission+Qualified remote training systems
- The specialist SQEP and solutions – e.g. SDEs lifecycle support team
- A close-knit ecosystem of SMEs, Primes etc. bringing insights and reach



But how will we need to support this new capability in service?

Lifecycle Support & Availability

Driven by:

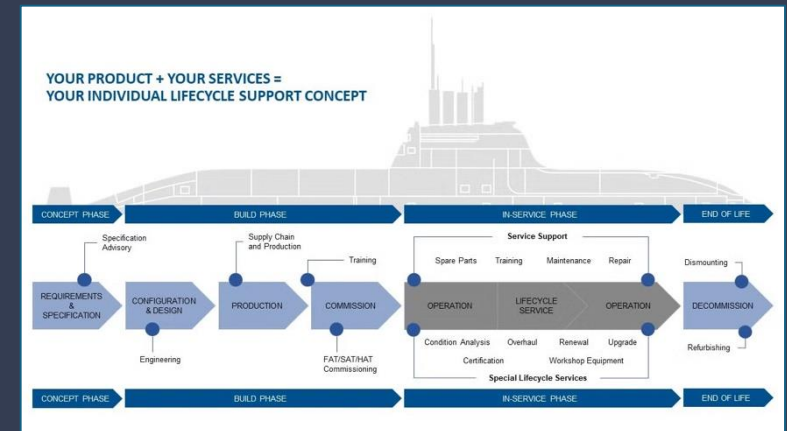
- Rapid evolution meaning systems become obsolete more quickly, shorter lifecycles
- At which point do complexity and availability intersect? As uncrewed systems become larger and more complex (e.g. arsenal ships) MTBFs risk at some point falling to a level lower than mission duration, necessitating minimal crewing.

How do we address this?:

- Start with established processes and tools (develop new tools?) to automate repetitive and non-value-add tasks - saving time
- Open architectures, LRUs, & common systems across multiple products – if you can't delay obsolescence, then minimise the impact
- New design philosophy for larger uncrewed systems. Don't design for maintenance, but for comprehensive condition monitoring and replacement (of asset on duty and/or of component in theatre)

What do we need in our toolbox as SME's?:

- The tools needed to deliver compliant projects at pace – e.g. Mission+Procured component cyber security tool, Pennant's (and others) suite of tools
- The specialist SQEP and solutions to bring new design thinking to UXVs to address the rapid obsolescence
- A close-knit ecosystem of SMEs, Primes etc. bringing insights and reach



These UXVs depend upon effective comms – how do we ensure this?

Network Data Flows & Edge Processing

Driven by:

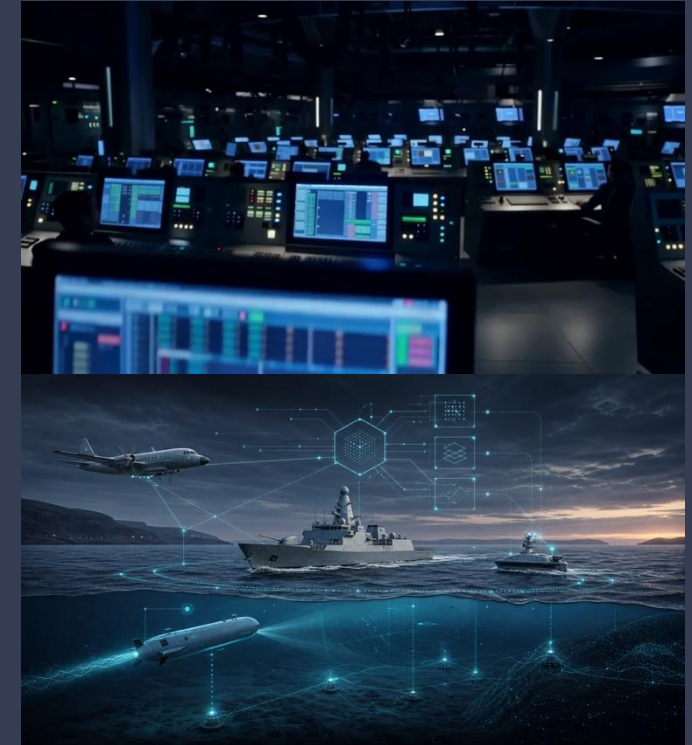
- With most nodes becoming ISTAR assets, networks will see an order of magnitude increase in data flow
- SATCOMS are critical, but a potential point of failure with the growing threat in space
- Edge processing can help with network data flows, but what can be done on a UXV that is vulnerable to capture?

How do we address this?:

- AI-driven communications management and data filtering to minimise traffic by focussing on the necessary only
- Owing to SATCOM vulnerability, and HF bandwidth limitations, are “deployed data centres / clouds” a potential solution / mitigation?
- A close-knit ecosystem of SMEs, Primes etc.

What do we need in our toolbox as SME's?:

- The specialist SQEP and solutions to bring new design thinking to UXVs to address comms vulnerabilities
- A close-knit ecosystem of SMEs, Primes etc. bringing insights and reach



Finally, an often overlooked subject, vulnerability to capture and interference

Physical Vulnerabilities of UXVs

Driven by:

- Vulnerability of UXVs to capture and the Trojan Horse risk via CBRNE or cyber, “surprise payloads”

How do we address this?:

- Vulnerabilities can be addressed through CBRNE sensing, intruder sensing (into HW and SW), weight / balance change sensing
- New design philosophy for uncrewed systems. Assume loss and interference and design systems and protocols for this

What do we need in our toolbag as SME's?:

- The tools needed to deliver compliant projects at pace – e.g. Mission+Assured etc.
- The specialist SQEP and solutions to bring new design thinking to UXVs to address security vulnerabilities
- A close-knit ecosystem of SMEs, Primes etc. bringing insights and reach



To summarise

Summary

We discussed:

- Increased Demand and Pace, SQEP shortages
- Bottlenecks in Security Infrastructure & Testing
- Need for a New Training Model
- Lifecycle Support and Availability
- Network Data Flows and Edge Processing
- Physical Vulnerabilities of UXVs

In conclusion:

- Specialist SQEP and solutions will be required
- The tools, processes, and ways of doing business will need to change to keep up with highly agile demand changes
- A close-knit ecosystem of SMEs, Primes etc. will therefore be core to successful delivery

If you would like to discuss any of the topics raised in this presentation, please don't hesitate to contact us.

Stephen Jefferies | Head of Business Development | stephen.jefferies@positivcohort.com

POSITIV COHORT

Complex capability. **Delivered at pace.**