Maritime Autonomous Swarm Systems

OPPORTUNITES AND CHALLENGES TO REALISATION

REPORTS OF A WORKSHOP HELD ON THE 22ND MARCH 2018

DISCLAIMER

The reports contained within this document have been written using published information already in the public domain as well as that provided by equipment suppliers. In presenting this information, the contributors have applied engineering judgment. While every effort has been taken to ensure the accuracy of the information provided in this report, no liability can be accepted for any errors, omissions, or results obtained from the use of the information herein, by the Ministry of Defence, the Royal Navy, the authors or the publishers. The information contained within should not be considered as representing the official view of the Ministry of Defence, UK Government or the Royal Navy.

Contents

Introduction

The UK Ministry of Defence (MoD) Defence Nuclear Organisation (DNO) is responsible for the UK Defence Nuclear Enterprise. Part of its remit is to understand and prepare the UK for the future underwater capabilities needed to fulfil the Defence Tasks set out in the Strategic Defence and Security Review 2015 alongside other strategic objectives.

Within the DNO, the Maritime Underwater Future Capability (MUFC) Programme has been established to investigate and research the future requirements, capabilities and possibilities of the underwater environment. As part of this work, DNO has partnered with UK Naval Engineering Science and Technology (UKNEST) in holding workshops with early career graduates who can bring in innovative thinking and fresh perspectives. These workshops enable the UK MoD to challenge assumptions and explore questions whilst enabling industry graduates to understand and explore the challenges faced by the DNO and the UK MoD.

On Thursday 22nd March 2018, the DNO hosted UKNEST graduates at MoD Main Building for a workshop. The theme for the day was Maritime Autonomous Swarm Systems and what capabilities could be provided now and in the future by these systems. The mixture of industry and government graduates engaged in rigorous debate about the drivers behind the development of swarm systems, the present and future scenarios these drivers could lead to and what capabilities Maritime Autonomous Swarm Systems could deliver within these possible scenarios. The graduates came up with a range of innovative ideas and solutions that Maritime Autonomous Swarm Systems could deliver and the challenges and obstacles need to be overcome before possible implementation. In groups, the graduates presented their thinking and ideas to a panel of Senior Industry and Government personnel, concluding their presentations by giving the panel their recommendations for the future of Maritime Autonomous Swarm Systems.

The panel was chaired by Rear Admiral Tim Hodgson, DNO Director of Submarine Capability and comprised; David Sherburn, Deputy Head of Portfolio Commissioning at Defence Science and Technology (DST); Jay Hart, Chief Combat Systems Engineer at BMT Defence Services Ltd; Neil Skelland, Head of Submarine Systems Division at Atlas Elektronik UK and Colonel Chris Holmes, Information Warfare Officer at Navy Command Headquarters (NCHQ).

Each group produced a follow up report on their presentations which have been compiled into this report document.

The DNO would like to express its thanks to everyone who got involved in making the workshop a success and looks forward to working with UKNEST again in the future.

Group Poseidon Report

Group Members: Eve Tymon, Gemma Jefferies, Matthew Cox, Daniel Chippendale

1. Scenario 1 (Short Term)

1.1. Overview

Scenario 1 looks at 'a low trust in AI' coupled with 'nonlethal use of swarm systems', and has been chosen because it best represents the short term possibilities which could utilise our current level of technology.

In the short term, or in a situation where trust in AI remains low, swarm systems will remain a tool for humans to utilise with final decisions and interpretation being carried out by human operators. Non-lethal engagement is a driver which may either result as a short term symptom of a lack of trust, or in fact an active decision made by governments and regulatory bodies. If these two drivers were to combine, it is likely that the swarm system would fulfil a purely data gathering capability within the military. This scenario assumes that maritime laws are not introduced in the near future which restrict the use of autonomous systems, particularly in the underwater environment.

The Royal Navy can look to harness current Autonomous Underwater Vehicle (AUV) Technology, such as SeaFox (Unmanned Mine Disposal) or Remus (Surveillance, mapping and sensing), and incorporate current military and commercial swarm technology. This concept removes the financial, ethical and legal implications associated with autonomous swarm technology whilst still making a meaningful step towards their application within the Royal Navy.

This approach would have the swarm as a payload on a surface or sub-surface vessel, and this swarm would consist of a small number of units. The swarm would be co-ordinated and controlled by a single operator located on board the vessel, who delivers basic commands to a single AUV. Any AUV in the swarm would be able to receive the operational instructions, decentralising the swarm and making it more adaptable, while also making it less vulnerable to attack. The communication would then be transferred around the entire swarm for the AUV's to collectively perform the detailed task. Such system would require minimal investment in R&D and could be realised within a relatively short timescale to provide the Navy with several key capabilities.

1.2. Capabilities

Surveillance: The swarm could work together locate and track targets and once located only one member of the swarm would be responsible for communicating the message back to the operator. This would give the capability greater range and improved scope, removing the need to introduce large vessels or humans into high risk environments, and making the surveillance capability more covert.

Data harvest: The swarm would have a greater capacity to harvest data from sources at a greater range. Again, large vessels and humans would be removed from high risk environments and data could be collected more covertly. Each AUV could be developed with different harvesting tools increasing the ability to collect a greater range of data. This capability could be developed so that the data collected by an individual in the swarm would be unusable without information from other swarm members, making the swarm less vulnerable to cyber-attack and corruption.

Route planning/ Mine Sweeping: The swarm could work together to navigate vessels or fleets through the underwater environment. With numerous members the swarm would be able to more

quickly sense across a wider area, using a variety of sensing techniques and building a more comprehensive map of the battlefield environment. This would allow the swarm to combine their information to better identify potential threats.

1.3. Challenges

The fact that this scenario is looking at the short term development and implementation of swarm system capabilities means that there will almost certainly not have been a new purpose built platform which can house the units. This means that the systems will have to be integrated into existing surface ship and/or submarine platforms. The integration challenges associated with this are already beginning to be explored, such as the possibility that the units could be deployed from a submarine missile tube, but if the current potential of swarm systems is to be realised then more work is needed. Once developed, these methods will also need to be trialled.

Within the swarm, short range communications would be feasibly delivered via current acoustic communication technology, however communications between the human operator and the swarm are likely to require the development of longer range, potentially non-acoustic, sub-surface communications e.g. LED/Laser Communications or Electric Fields. Depending on what platform will be co-ordinating the swarm and receiving the recorded information, there may be above to below communication required. This form of communication between mediums is problematic as different transfer methods are used for each. One option is for swarm members to surface or communicate to a surface buoy that would then allow high speed communication to be transmitted back to the operator. Another option would be to give one unit a higher data transfer capability (hub), with all other units sending collected data via the hub, but this would create a single unit loss failure which would prevent data from being transmitted during an operation. However, more novel methods of communication should be explored.

Equipment availability is a key consideration when looking at swarm systems; if only a small portion of the system is available for deployment then this will have an impact on the effectiveness and capability. This is particularly important in the short term scenario where it is expected that units will be larger and form part of a smaller swarm compared to what might be expected in the longer term. There would need to be dedicated workshops for repairing and maintaining swarm systems and a through life maintenance plan would need to be developed.

1.4. Recommendations

The key recommendations to allow the above application of swarm technology to have a significant beneficial impact in the Royal navy are:

- Focus R&D funding for autonomous technology to develop the communication capability of existing AUV's to allow them to operate at a greater range from the controller. This should include research into non-acoustic communications and to find solutions to the water/air boundary issue.
- Initiate a study into current commercial and military swarm technology and how it can be applied in the subsea environment.

2. **Scenario** 2 (Long Term)

2.1. Overview

Scenario 2 looks at a ‘high level of computing power’ and ‘an advanced level of technology miniaturisation’. This has been chosen because it looks at what future capabilities might look like in

the longer term; through large improvements in technology. This is considered more blue sky thinking but with some clear pathways for realisation. This concept assumes that there are no restrictions introduced to R&D due to ethical practices in the foreseeable future. It has also been assumed that investment in research and development remains substantial and growing/index linked, to enable such technology to be developed.

In terms of deployment, this concept has assumed that it can be achieved but does not specify how. Compatibility with existing vessels or deployment mechanisms is not crucial due to the long term approach which could see platforms being developed with this capability in mind. Future mechanisms for swarm release could simply be over the side of a surface ship or dropping from the air. A more creative option for deployment could be a dormant swarm that is left underwater and activated remotely or through a few agents remaining alert.

2.2. Capabilities

Defence or protection: The swarm system could create a gate to a channel of water, scanning vessels to determine if they should be allowed to enter. The swarm could also be used to surround and protect a specific vessel from attack.

Decoy: The swarm system could replicate the shape and signatures of a vessel in order to trick an oncoming enemy warhead and divert it from its original target. The swarm could also act as a more permanent decoy by altering the signature of the vessel it is protecting.

Route planning: Suitable for choosing a safe route for divers or for a much larger vessel. Ant colonies lay down pheromones to help 'weight' the shortest path, in a similar sense a swarm system could be used for route planning or route optimisation in the underwater battlespace.

Neutralise or destroy: The swarm system could attach to an enemy or foreign vessels similar to how barnacles attach to surfaces. Given the right technological capability the swarm system could either be rigged with explosives to destroy the vessel or emit certain signal types and frequencies to incapacitate (neutralise) the other vessel.

2.3. Challenges

There is a skills gap in specialist science, technology, engineering and mathematical (STEM) job roles throughout the UK. Although the increased media attention has provided a small increase in uptake, more is required to meet the demand. Younger generations will need to be targeted to pursue STEM, and talented individuals from other industries will need to be attracted to the Naval Engineering sector.

Retention in existing STEM roles could be greatly increased through the training of new technologies. To reduce the skills shortage existing employees could be trained in different methods and therefore encourage them to stay longer before retirement. Schemes to pass this knowledge down to new starters are being implemented, however for this sort of concept to progress the rate of the transfer of skills must be addressed.

For this concept to work, industry would have to collaborate and develop an open sourced environment. An example of this is the current trends with Apple/Samsung mobile phones, the increase in CPU processing power is inversely proportional to the size of the CPU. If Apple/Samsung, for example, published their developments and test results it is not unfeasible to assume that a niche company would be able to provide a different approach and solution. Thus advancing technology far quicker than a standalone company could.

Maintaining the development of this technology is a big challenge, particularly with the potential for tighter budgets in the future. Algorithms will have to be developed, specifically with underwater capabilities in mind. With a swarm that has 100s-1000s of individual agents, a learning algorithm would be required. There are existing algorithms that have shown basic swarm capability such as forming an overall shape from a random arrangement of individual agents, but this must be translated to an underwater context. Swarm units must be able to act quickly without the delayed process of human decision making, which is not just a challenge technically but also in terms of perceptions and trust.

When looking at the miniaturisation of the swarm units, power & propulsion (P&P) become key challenges, and must be developed in tandem in order to remain compatible. Miniaturisation of technology means that swarm systems could replicate those found in biology. Bio-inspired ideas could similarly be investigated for P&P development, e.g. organic based energy stores (using sub surface minerals or filtering water for correct components), or organic based actuators.

2.4. Recommendations

The capabilities which have been outlined for this scenario currently rely on an assumption that R&D is maintained in this area. If these capabilities are to be realised then there needs to be continued research into the following areas:

- Miniaturisation and piezo-electric materials to dissipate heat;
- Learning algorithms specifically for the underwater battlespace;
- Bio-inspired ideas for P&P development;
- Relationship between power source and propulsion system and how both of these can be reduced in size;
- Methods of deployment of large swarm systems;

Finally, initiatives should be set up which look to encourage young people, who tend not to be confined by the 'laws of physics' and technicalities of a project, to think about these challenges. The Royal Navy should allow students to pursue a small project related to swarm technology, which would increase intake into STEM roles and push boundaries in R&D.

Group Dreadnought Report

Group Members: James Connolly, Charlotte Cox, Dan Pateman and Chloe Woodger-Smith

1 What capabilities 'Autonomous Swarm Systems' could give the Royal Navy?

When thinking of Autonomous Swarm Systems and the capabilities that they could give the Royal Navy, the possibilities are truly open ended. The mind can begin to run into the realms of fantasy and fiction, with the laws of physics being completely forgotten and the art of the possible not being the focus, and the art of the impossible coming to the fore.

Initially there are a few options that the RN could pursue to make use of the Autonomous systems that may be available to them and also to invest in certain areas of technology that may help and inform them for future developments in the autonomous sectors. These may include:

1. Battery Technology
2. Communications Technology
3. Materials Technology
4. Harbour protection
5. Attack Swarms

There will also be many other areas that may be of interest and warrant investment, but in the view of this report we have decided to focus in on the way that the RN improves it capabilities to recruit the correct people to facilitate the future shape of the enterprise. In order to allow the RN to have the future capability, it must begin to look at the way it trains and recruits its future work force, and focus on the type of individuals that will help it deliver its future missions.

In our opinion, there is a real need to look at how the RN wishes to structure the autonomous strategy to ensure that the people that are recruited or trained to facilitate the missions understand the impact that Autonomous warfare could potentially have on future war space and how they must be of the correct mind-set to perform these missions.

If the strategy is to use autonomous swarms to be programmed and then allow them to independently complete missions, there will be a level of complex programming that will be required; are the RN prepared for this challenge?

Will autonomous swarms be controlled from a base point, where the kind of individual required will be different to ensure that they are prepared for mental challenges that this kind of platform will deliver? There may also be the option that swarm systems may only be used as information and sensory systems to inform command decisions that need to made by the RN as to how they will use other capabilities at their disposal. This could allow for the release of precious personnel that are involved in the more mundane and monotonous daily tasks that need to be performed, to ensure that our national and international duties can be performed with more traditional platforms in the future.

2 What future scenario do you think would make 'Autonomous Swarm System' usage feasible?

The scope of Autonomous Swarm Systems is vast and presents huge potential for future capabilities of the RN. However, the future of the technology is dependent on two factors. Firstly, the decision from the RN on the requirements of the system (e.g. primarily defensive, offensive, reconnaissance etc. or a combination) and secondly, overcoming key technological barriers to provide those capabilities. Both will significantly influence the direction in which the technology is taken, and the future scenario in which swarm systems are used. Therefore, with such a broad scope, our team opted to focus on two distinct future scenarios:

A. Low Capability Harbour Defence Swarm System

This scenario envisaged a cheap to produce, low level technology swarm system operating in a harbour defence environment. The primary function would be to monitor traffic through the harbour and detect unknown vessels, with the added capability of tracking and following a target. This would remove the necessity for RN personnel to perform mundane harbour surveillance tasks and enable deployment of personnel where and when required.
The advantage of this system is in its small operational environment and low capability, therefore enabling technology to be used which can be designed and developed in the near term at low cost (for instance shorter battery lives, short range communications, low levels of equipment carried on-board etc.). Additionally, utilising a low level technology system reduces the requirement for specialist training in device operation and maintenance for RN personnel.

B. High Capability Multifunctional Swarm System

This scenario envisaged a high capability all-in-one swarm system capable of operating in a multitude of environments. The individual units would not necessarily be uniform across the swarm and may even have a modular design to adapt the capabilities of a swarm unit to a particular mission.
The operation of this system would see deployment from a ship which the swarm would then use as the operational centre for reporting information and recharging batteries. The swarm would perform surveillance and reconnaissance tasks in an area (e.g. ship, submarine and mine detection etc.) with the capability of performing defensive or offensive countermeasures.
The operational capability of this system would be vast; however it would require overcoming many technological barriers. Therefore, a system of this type would require significant investment into the design and development of various technologies with a long term delivery goal. In addition, the RN will need to target recruitment towards new disciplines and provide specialist training to ensure the systems can be operated and maintained effectively by the time the Swarm Systems enter service.

3 What challenges need overcoming in order to realise your proposal?

After considering our two future scenarios we looked into which DLODs they would affect the most and the challenges that need to be overcome before these scenarios could come to fruition. Our focus was immediately brought to personnel and from there we decided that personnel, training, equipment and infrastructure are the four DLODs altered the most by our Swarm System scenarios.

A. Low Capability Harbour Defence Swarm System

Personnel – With a low capability swarm system the change in personnel will be small; current vessels will still be in use with a similar volume of staff on board. Some personnel time will be used operating the simple autonomous systems.

Training – The swarm systems in this scenario are low capability and therefore need a lot of guidance and human input. The roles of the swarms will be simple and potentially uninteresting for operators, who will easily lose concentration; this will create a need for shorter work shifts. Staff will need to be trained in the current RN roles, as well as operating the autonomous systems.

Equipment – These systems will be cheap to make; they could be mass produced in factories by 3D printers. The technology will be similar to current tech; UxVs will not have modularity and will be simple, single role drones.

Infrastructure – The technology of these swarms is similar to today's UxVs. This means that low capacity energy storage and difficult communications make these systems very dependent on 'bases' for charging and data sharing.

B. High Capability Multifunctional Swarm System

Personnel – This scenario requires staff who can create and develop autonomous swarm devices with artificial intelligence and analysis software that can sort data collected by the swarms. There will be a shift in personnel from active seafarers to highly qualified software developers. Use of Navy vessels will decrease and so will volume of personnel. The RN will need to recruit and attract staff from industries such as gaming, robotics and space to enable this transition to happen. Making the maritime sector more visible and attractive to prospective employees will help in recruiting such staff.

Training – The training needed in this scenario will differ massively from the current need. With a large part of personnel now developing autonomous systems rather than seafaring, the focus will shift to software and AI training. Operators of the autonomous swarms will have multiple decisions to make due to the complexity of the systems' capabilities, or the computer analysis will make decisions by itself and carry out appropriate measures in reaction to a situation.

Equipment – Research and development will look into sensor technology, AI communications and energy storage. Battery technology will be crucial in the future of swarm systems aiding in the length of operation.

Infrastructure – Development into areas such as energy storage and communications is necessary for this scenario to occur. These advances will give autonomous systems much greater operating time, capability to communicate effectively with other systems and better data gathering and sharing. Modularity would be optimal, with options such as charging stations on ships, mission bays equipped with swarms and MCM capabilities.

4 What recommendations would you give to seniors in order to implement steps towards your proposal?

To conclude, as a result of the FutureNEST Swarm Systems workshop, the main areas of focus going forward are to research into different methods of powering systems, and ensuring that personnel are given the relevant training and information to carry out tasks.

The research into power methods can lead to an understanding of the technologies that could be utilised, and may already exist within the commercial market or the world of academia. A collaborative effort between these groups would need to occur, in order to achieve the ultimate goal of providing a high energy density solution to the system. This collaborative effort is already occurring within the industry, and proves to be a useful way of creating innovative ideas.

The skills and training also need to be provided to RN personnel, in order to educate them on the developing technologies that'll be used within and alongside their already developed ships and submarines; this could be demonstrated through the use of VR or other gaming technologies.

We also believe that the RN needs to be better advertised to young people starting out in their careers. Companies such as Google and Tesla appear to be more attractive companies for new graduates to apply for. These companies are visible every day, and are often in the news for their advances in technology. This makes it a lot more common for young people to be interested and attracted to these industries, due to a greater awareness of them.

Perhaps with the introduction of new technologies into the industry, young people will gain a heightened interest in the maritime sector, and aid in its future capability understanding and development.

Group Kraken Report

Group Members: Natalie Mitchell (BAE Systems CS&S), Sam Kent (SEA Ltd), Hannah Reid (Dstl), Ewan Gray (Babcock International Group)

This report outlines the discussion that took place around the future use of Autonomous Swarm Systems for the Royal Navy during a workshop at the MoD Main Building on the 22nd of March 2018.

Key Drivers

The following key drivers were identified, for why the Royal Navy must change:

Budget – Following significant growth in defence spending up to the early 1980s, UK defence spending has now been in decline since 2010-11. While the UK has NATO commitment to maintain 2% of GDP on Defence it is likely that continued budgetary pressures will remain the norm.

Cyber vulnerability – Control systems are vulnerable to attack from both inside and outside the control system network. With the increasing "openness" of control networks, the potential for cyber-attacks is greater than before, specifically with the increasing skills of cyber hackers.

Communications – Communications in the underwater environment are far more challenging than those in air. In the underwater battlespace covert communications are a frequent concern, whereby active transmissions may expose asset locations and bandwidth and range are both severely limited.

Increase in state-sponsored aggression – The rise of nationalism is increasing the threat of the use of violence by sovereign states to attain strategic and political objectives by actions in violation of the law. The rise of state-sponsored aggression has already been observed in the world today.

Energy resource – The depletion of fossil fuels has led to an increase in the use of renewable energy resources, it is important for the Royal Navy to also follow this trend. Additionally, the use of resources such as the nuclear reactors on submarines must start to be used at a lower rate to ensure the resource is available for the life of the platform, without the need to refuel.

Operational Background

The Royal Navy primarily exists for two reasons. First, to ensure that confidence in using the maritime environment to conduct trade and harness resources remains high – constabulary type "simple" operations. Second, when threats to the nation need to be dealt with at range, the Royal Navy must continue to be able to use the maritime environment to project power to reassure and ultimately protect our national interests – these could be deemed "complex" operations, which may have an aspect of lethality associated them.

"Simple"

- Monitoring
- Deterrent operations
- Anti-drugs operations

"Complex"

- Risk to life
- Fast reaction
- Offensive operations

Due to the ethical, legal and regulatory environment about using autonomous systems for lethal operations being unclear it is suggested that the Royal Navy would employ swarm systems to complete the "simple" constabulary operations, therefore increasing the availability of larger naval assets and personnel for operations that require human intervention.

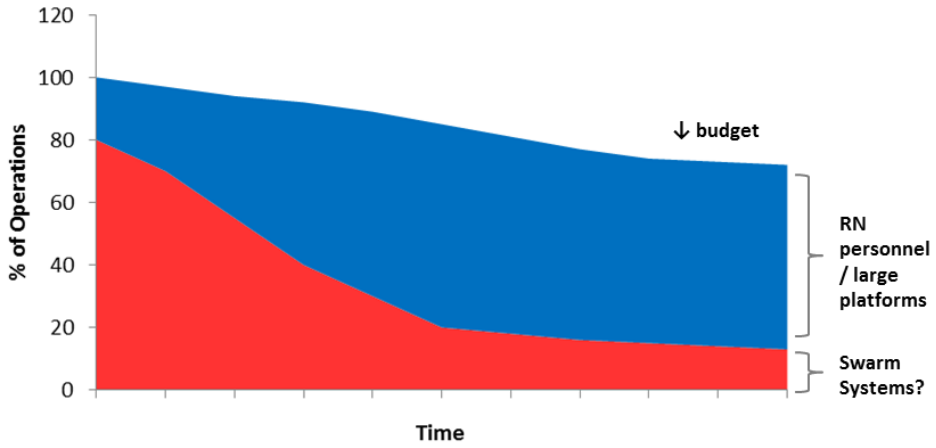

Figure 1: Types of Operations for the Royal Navy

Suggested Use Case

The swarm is made up of child and parent drones.

The child drones are smaller, low power and passive/reactive by design. These are capable of short-distance communication across the swarm.

The parent drone is active, requires more power but is capable of long-distance communication to the command centre. This may be used to gather more detailed information and perform an offensive action when permitted.

Once a suspect object/vessel is detected by a single child drone the location data is communicated to other local child drones, Figure 2.

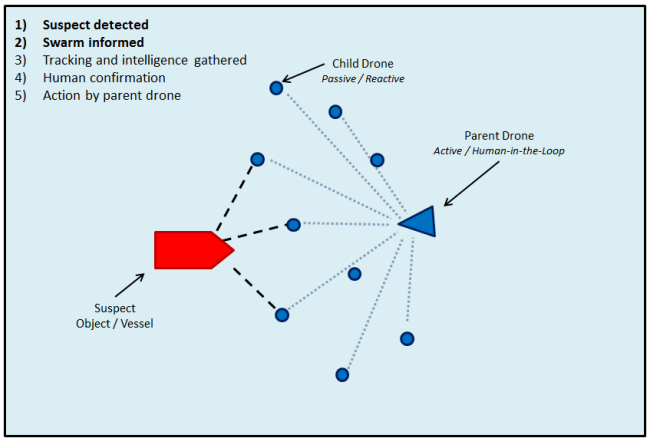

Figure 2: Scenario Parts 1 & 2

These then move to track the suspect, gathering further data through other sensors, Figure 3.

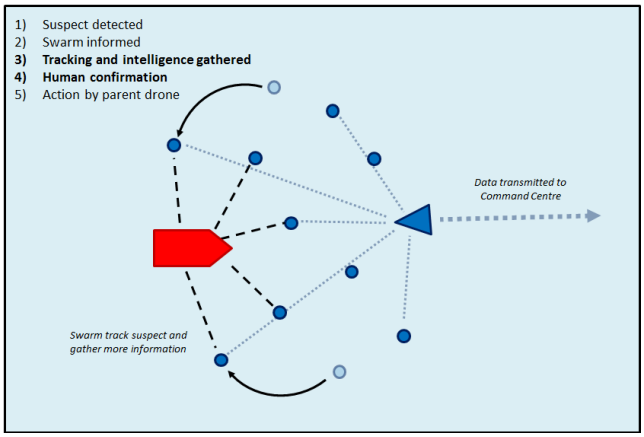

Figure 3: Scenario Parts 3 & 4

This data is transmitted to the larger parent drone, which in turn passes it to the command centre. In the command centre the data is further analysed and evaluated by an operator, this operator is the human-in-the-loop, Figure 4.

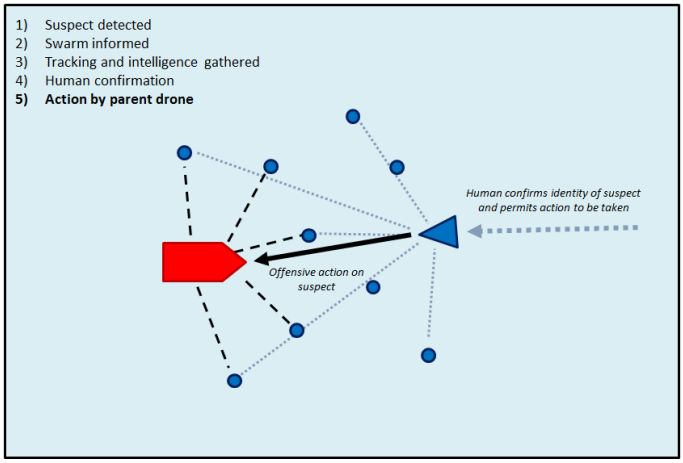

Figure 4: Scenario Part 5

It is desirable to have a human-in-the-loop system as it removes the legal and ethical barriers surrounding autonomy with regards to offensive actions.

The operator confirms whether the suspect is a viable target and permits the parent drone to conduct an offensive or disruptive action. This could be used to gather further intelligence or deter the suspect from entering the area, Figure 5.

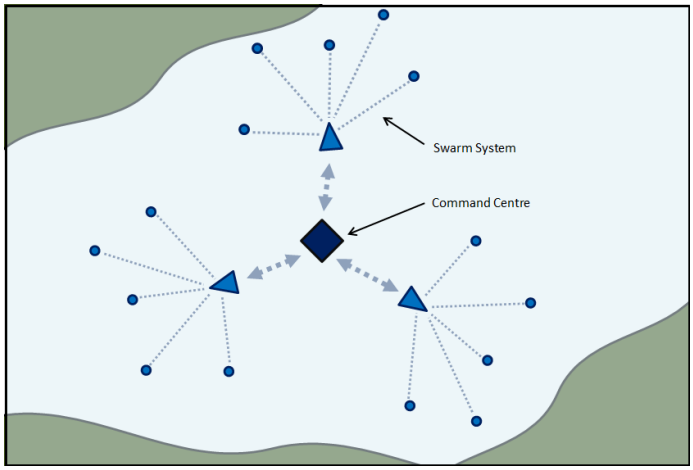

Figure 5: Scenario Swarm Overview

Separate swarm systems could be coordinated in order to provide maximum area coverage from a single command centre or platform.

Technological Assumptions

Child Drone Communications –The child drones can both send and receive communications with each other under the water. The child drones can both send and receive communications with the parent drone under the water. This communication could be by short range sonar.

Parent Drone Communications – The parent drone can both send and receive communications from the child drones under the water, perhaps via short range sonar. The parent drone can both send and receive communications with a command centre whilst on the surface or under the water, perhaps via radio signals or long range sonar.

Sensors – The child drones have small sensors capable of gathering information about passing ships/submarines. The parent drone has more powerful sensors to allow for further information to be gathered if required.

Power – Battery technology will need to be developed to allow the swarm prolonged periods of operation with re-charging. Alternatively another method of powering the drones, perhaps through renewable energy, will need to be found.

Challenges

While investigating this swarm system several challenges were identified using the Defence Lines of Development (DLODs) system.

Logistics – One logistical challenge is finding the best method of deployment for this system. Depending on how the completed system operates, it may simply be a case of dispatching it directly into the water by the user or via a more bespoke system fitted to a platform.

Communication is also an important logistical challenge to consider, not only with the operator, but within the swarm itself. It was suggested that within the swarm communication could be via short range sonar, and then long range sonar could be used to communicate with the operator. Alternatively, one UUV could detach itself from the swarm and physically transport information from the swarm to the operator.

Infrastructure – In addition to potentially fitting bespoke launching systems to platforms (as mentioned above) there are challenges associated with the manufacture of swarm systems. Building these systems will involve high volume production with short lead times. The supply chain for these systems has yet to be established and will require development as this technology becomes available to the Royal Navy. **Equipment –** Finally, a key challenge for a swarm system is energy. Their energy source, storage and overall usage will have a considerable effect on how these systems can be used and the longevity of the missions they can undertake. Our system could conserve energy by maintaining a passive sleep mode, only activating when it detects threat activity. Commercial developments in battery technology may also be applied to this system, and research into potential renewable sources of energy would be beneficial.

Recommendations

To overcome the challenges described above it is recommended that:

- Expertise is drawn from other industries to explore how best to manufacture and power an underwater swarm system of this kind.
- Research is carried out into small scale renewable energy sources and low power solutions for this system.
- Reapplications of current technologies such as mine-countermeasures are investigated.

Group Nelson Report

Group Members: James Bauld (Rolls Royce), Max Nicholson (BAE Systems Submarines), Bethany Ross (Thales), Tony Sandhu (MOD) & Catherine Shewell (Babcock International)

Executive Summary

This document is a summary of the findings from Group Nelson that were discussed and then presented at a FutureNEST workshop held on the subject of Autonomous Swarm Systems. The document covers the processes that were followed and then how the key drivers were chosen. From this the group gives an overview of the issues and the associated recommendations for the use and development of autonomous swarm systems.

The format of the workshop was based on the collective thinking and discussion, around the target subject, by young engineers based in different companies involved in the UK naval industry. Group Nelson was composed of individuals with a wide trade experience, ranging from policy makers to naval architects and concept designers to build/in-service support engineers.

To workshop the groups themes for the day, a number of lateral thinking tools were used. Included in these methods was the PESTLEE analysis, considering Political, Economic, Social, Technological, Legal, Environmental and Ethical key words, relating to Autonomous Swarm systems. Over 100 key words/phrases were identified, before honing down to 4 key themes. In addition, a number of capabilities were identified, using the words/phrases generated in the PESTLEE format.

A swarm is defined to be 1 or more unmanned vehicles; this could be air, surface or underwater. It has been assumed that swarms consist of a large number of the same vehicle; these units might have some differences between them depending on the sensors required or the configuration, i.e. if a 'queen' unit is being used.

Capabilities

Figure 1 presents a summary of the proposed capabilities identified for Autonomous Swarm Systems.

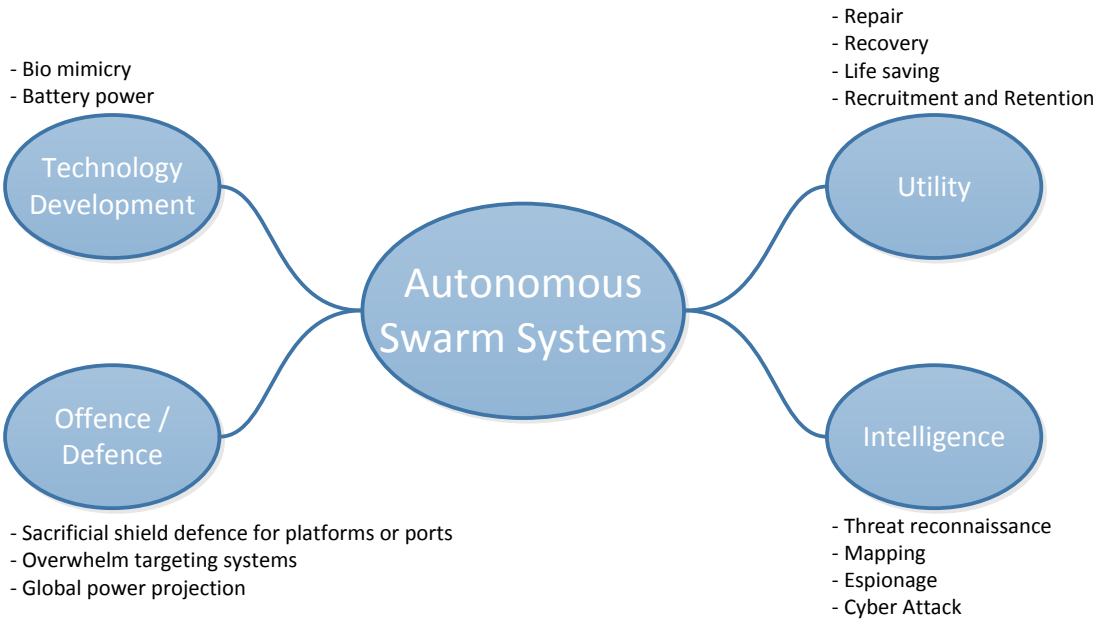

Figure 6 Proposed Capabilities for SWARM Systems

Scenario 1: Improvement in Cyber Security and Ethics

Cyber security and Ethics were identified as key drivers in autonomous technology and therefore are also applicable to swarm systems. Cyber security was identified due to the requirement for assured, robust and secure C4ISTAR capability plus organic data protection (Data at rest) and the links this will have to ethics and cultural acceptance. There will presumably be links into existing classified networks would could therefore lead to accreditation / integration risk. Security in all defence sectors is of paramount importance and this extends to the cyber realm. The development of adversaries, peer and asymmetric, will push the defence sector into using commercial and sovereign encryption standards and data mediums such as the cloud for the RN to maintain global superiority. From research around the subject and information published in the Strategic, Security and Defence Review (SSDR), it was highlighted that major areas of concern were protecting communication lines and defending against hacking [1]. Cyber security was separated from the actual physical security of the drone components.

A cyber-attack is understood to be, but is not limited to, stealing of data, deployment of viruses, or hacking to manipulate the actual drones.

Ethics is defined to be the moral principles that govern behaviour or the conducting of an activity.

Ethical concerns around autonomous systems are:

- The 'kill chain' – would a human have to be involved?
- Could an autonomous system harm another autonomous system?
- What, if any, geographical boundaries would apply?
- Can the data from an autonomous be fully trusted?
- How much intelligence should be given to an autonomous system?
    - At what point in the system should AI be used? At the sensor, in the platform, the command GCS?
- How should an autonomous system interact with human beings, depending on the type of system should it take into account religions and races during these interactions?
- If the autonomous system does malfunction, who is liable (the software engineer/the owner/the individual that gave it its mission/etc.)?
- Who shall certify the autonomous system? Is the system auditable?
- What sort of/level of task should the autonomous system be able to react to?
    - Common understanding so far is that drones will be complimentary or used in dirty, dangerous and dull tasks
- How is a threat defined for the autonomous system to react to?
- How is the privacy of the general public protected?
- How is an autonomous system certified?
    - Currently there is no baseline or standard to meet to ensure that an autonomous system is ethical so how does industry design and sell-off a system?
- Public perception and value seen
    - Autonomous cars are already being used, and autonomy in manufacturing is already proven as more effective and efficient. Could the progress of autonomy in these sectors be capitulated on?

- Because of budget cuts in other sectors, such as health and education, each expense from the military is scrutinised by the public, and due to this the public have formed strong opinions about defence programmes.
- It is likely that there will be no new money for drones and autonomy, so what is going to be given up?

Table 1 Scenario 1: Cyber Security vs. Ethics

High Ethics – Low Cyber Security Improvement	High Ethics – High Cyber Security Improvement
Limited ability to protect against cyber-attacks. Slow to innovate and change with technology due to culture and ethics.	Greater ability to protect against cyber-attacks. Less flexibility, higher scrutiny and authorisation / reason for use, when wanting to use the swarms as a high level of ethics would prevent their use in certain situations. High moral image portrayed to the public – maintains their investment. High level of success against attacks could prove to be a political driver for the party in power. Higher cost and complexity
Low Ethics – Low Cyber Security Improvement	**Low Ethics – High Cyber Security Improvement**
Inability to protect against cyber-attacks. Potential back lash from the public as the RN could be seen to be unethical. The data received by the swarm system would have to be subjected to intense scrutiny to ensure that it had not been tampered with which means potentially contracting in an external company to provide their expertise on cyber security. New doctrine and concepts could allow for this. Low complexity and low cost systems may offer the information required or even be disposable.	Greater ability to protect against cyber-attacks. Potential back lash from the public as the RN could be seen to be unethical. A lack of a framework for the ethical use of these swarm systems could cause future legal/political issues if the systems are deployed in, what would later be defined as, off-limit areas. Political relationships would be strained as each country is attempting to determine what capabilities the others have.

Scenario 2: Improvement in Power Technology and an Increased Threat Level

An improvement in Power Technology is defined to be a higher density power cell with extended life and usage.

An Increased Threat Level is defined to be a greater number of individuals or groups with the means and the incentive to attack the UK.

This was the primary scenario that the team focused on as these were thought to be the top two drivers that were identified in the workshop.

As the threat against the UK and its allies evolves over time, a pro-active approach is required in developing our own technologies which can act as a deterrent to any hostile Governments or organisations. The ability to prevent engagement by demonstrating a capability which is technologically advanced holds much value as resources are saved and the impacts of conflict are not imposed upon populations of people.

A point of focus is regarding the evolution of power technology against the increasing threat posed. This involves considering the impacts developing power technology would have on the future level of

threat, the uses and applications that could be realised if power technology was optimised. Increasing power density, identifying new power sources and optimising the use of existing power sources are all research streams which are currently being explored but the potential capabilities which could be achieved within the Defence industry resulting from advancement in any of these fields could offer the next generation of equipment.

The Maritime domain has much potential should power technology be exploited further. New civilian and military applications will be realised with the requirements of more advanced, power intensive activities feasible. It can be assumed that other Governments around the world are looking into improving their power technology and there is the potential that our capabilities could fall behind increasing the threat level.

Historically, there has been the Arms race, the space race and even now there are technology races taking place which will redefine the next generation of weapons and Defensive capabilities. The field of power is one part of the drive to develop future capabilities and may be considered as one of the foundational elements in achieving state of the art technology.

Table 2 Scenario 2: Power vs. Threat Level

High Power Technology Improvement – Low Threat Level	**High Power Technology Improvement – High Threat Level**
Longer mission times Reconnaissance Persistence Increased cost New weapon technologies (EMP, DEW)	Longer mission times Reconnaissance Defence during aid missions Potential physical barriers of interconnecting swarm devices
Low Power Technology Improvement – Low Threat Level	**Low Power Technology Improvement – High Threat Level**
Home defence – shorter mission times and distances to travel Use in schools to raise awareness of the RN Local benign tasks Environmental, communications, ISR	Home defence – shorter mission times and distances to travel Expendable systems that can be used in more hazardous locations (battery systems is not as expensive). Could have a self-destruct mechanism should it be captured or designed and accepted as consumable.

Challenges facing Swarm technology

Following discussions during the workshop, it became apparent that many challenges exist which face the adoption of swarm technology. These challenges will demand a significant amount of thought, time and cost. The key challenges identified during the workshop are summarised below:

- Ethics & Law:
  One of the main challenges which recurred throughout the workshop was that of ethics. Mainly what role can a swarm system play when you take into account the ethics of the situation? On one hand it may be ethical to reserve swarm technology for purely defensive and intelligence gathering activities. On the other hand it is worth considering whether our opponents will consider ethics in the development of this technology and whether we are

making the UK vulnerable in doing so. Opinions on this topic are likely to change depending on whether we are at war or in peace time. However it will be necessary to implement policy & law guiding the use of swarm technology for Defence projects in the UK, but also to develop the CONUSE of the system, its development assurance and certification.

- Powering:
  Another major challenge facing the adoption of swarm technology is the state of powering technology. In order to unlock the full potential of swarm technology and UxV's a significant improvement in power density and endurance is required. Thought should be given to whether this is likely to occur in the near future or whether attention should be focussed on what can be achieved with today's technology. This will require looking into other industries to find the solution such as the mobile phone and computing industry. Should each individual element have greater power resources, it will enable the entire swarm to function faster / longer or enable each one to carry a wider variety of sensors and therefore be used in a multitude of environments. They will be able to respond to a greater number of threats or perform a greater number of tasks without the need for refuelling or replacement, making them much more efficient. The process of refuelling would also have to be considered depending on the type of power source used, could mid-air / sea power transfer by mother drones be utilised for increased persistence?

In addition to those key challenges discussed above, several others exist. During the workshop, it was felt that these challenges are common and well known across many Defence projects. However it is important they are considered when looking to develop the role(s) of swarm technology and UxV's in the future.

- Cyber Security:
  Whilst the form that swarms will take in the future is undecided, it is essential that any data stored within the swarm remains secure.
- Command and control, communication, computation and information (C4I), with cyber it becomes C5I:
  Similarly, underwater communications are also a key factor to consider. It is essential that the swarm can communicate within itself securely, intra swarm communications. It is also essential that the swarm can interface with the outside world. Challenges will come in the form of long range underwater communication and may require innovative solutions such as docking stations and underwater infrastructure.

In order to overcome these challenges, transverse working is critical. Several work streams need to operate side by side with both short and long term goals to ensure continued development of technology and capability. Without this the impact of swarm technology and UxV's will be limited but with it, the RN could unlock increased efficiencies and benefits.

Recommendations

Having discussed autonomous swarm systems, influencing factors for future defence, technological advances and roadblocks, the group have some recommendations for consideration.

Legal

The team felt that the complications that could arise due to moral and legal matters could be significant and potentially hinder progression. Without the technologies being accepted then it cannot be used.

For this reason we felt it was important to start engaging with the correct stakeholders, such as governments, manufacturers, operators etc., to ensure that the correct approval process is in place to maintain a technological advantage over our adversaries.

Cyber Security

Cyber security was discussed as a point of concern in detail by the team. This is concern is supported by various literature regarding future Defence capability including the 2015 Strategic Defence and Security Review [1], NATO Autonomous Systems report [2], Rolls Royce Remote and Autonomous Ships [3] and the DTU Pre-analysis on Autonomous Ships [4].

Look to use less conventional methods of communication within the swarm. Potentially look at the manner in which animals in swarms communicate. Ants use pheromones to create a feedback loop to allow the colony to follow the "best" path between their food sources and nest [5]. Bees perform a "dance" to communicate [6], could movement of individuals to influence the decisions of the rest of the swarm a possibility? LIDAR communication may be a possibility and significant research is being conducted into this as a surveying method [7]. These communication methods would allow operations and advantage in denied and degraded environments.

Powering

Significant research in areas such as propulsion, fuel and energy storage, are being undertaken. These advances could improve the capability of swarm technology hugely, see Section 0.

For this reason it was felt by the team that this was a beneficial area for investigation, particularly more renewable types of energy. A possibility is using currents in combination with air multiplier technology [8] as a method of propulsion.

In addition it was felt that looking at methods of reducing resistance would energy efficiency, therefore research into areas such as shark skin technology [9] could be advisable.

Materials Technology

The team felt that the use of Smart Materials [10] could change the manner in which UxV's behave, for example an electrical current causing an ability to change structural shape allowing a "sprint" and "dormant" hull form; electrically changing signature, increasing stealth, and allowing for counter measures.

Parallel Research

Finally the team also felt that due to technologies emerging at different rates (disruptive technologies), that concepts should be developed in tandem with the research into the technologies, allowing the defence sector to use the technology as soon as it becomes available.

This would involve not just designing for what we currently have available, which is obviously necessary but also designing in a “blue sky” manner in parallel by considering what could be available well into the future. Disruptive thinking workshops that are not constrained by current CONOPS or doctrine would be fundamental in developing these technologies.