Developing the Quantum Warship

J Rigby* BEng MSc CEng

** BMT, UK*
* Corresponding Author. Email: jake.rigby@bmtglobal.com

Synopsis

New advancements in quantum technologies look to provide significant improvements in capability for combat platforms in navies across the world. From communications systems to weapon targeting and navigation, there are countless possibilities for the enhancement and augmentation of current systems. Due to the current low technology readiness levels quantum systems are often considered a distant threat/opportunity, over the timeline horizon. However, due to the dramatic and transformative end results promised by some researchers, the ship designer of today needs to understand the potential impact of this wildcard technology. This latest paper describes what a quantum enhanced warship of the future could look like and the current progress towards the required accuracies and capabilities.

Keywords: Quantum; Warship; Technologies; Future; Sensing

1. Introduction: What are Quantum Technologies

Quantum Technologies are a rapidly emerging area of physics that utilises the characteristics of Quantum (subatomic) particles, such as photons, electrons or quarks. Broadly speaking the technologies can be grouped into three different areas linked to the three different underlying quantum mechanic principles of 'superposition', 'entanglement' and 'sensitivity'.

1.1. Superposition – Quantum Computing

Probably the most famous of the three main phenomena is superposition, the driver behind the new field of Quantum Computing. In regular computing, information is made up of binary elements of information, called a 'bit'. This 'bit' is just like a switch and can either be on or off. In a quantum computer, because of quantum mechanics, an element of information is called a 'qubit' and it can be 1, 0 or both at the same time. This third state may at first glance seem inconsequential, but due to the greater variation allowed can enable significant performance enhancement. Using this technique some developers claim they can produce computers '158 Million Times Faster Than the World's Fastest Supercomputer' (Medium, 2021).

1.2. Entanglement – Quantum Communications

Next the phenomena described by Einstein as 'Spooky' allows for the effective and secure transmission of information. Entanglement is where two particles are 'connected' even when separated by large distances. Once two particles are 'entangled' they are linked, small disturbances seen by one can also been measured by the other.

1.3. Sensitivity – Quantum Sensing

And finally but by no means the least, by capturing a quantum particle you can detect extremely small disturbances in the wider environment, creating a new field of 'Quantum Sensing'. Although often forgotten compared to the other more famous phenomena, this sensitivity is just as powerful, giving the potential to provide extremely powerful, accurate and long range sensing capability.

Author's Biography
Jake Rigby is the Research and Development Lead, responsible for the portfolio management of internal research projects in defence. He is a charted engineer and Member of the Royal Institute of Naval Architects originally training as a Naval Architect specialising in ship signatures before his current role of R&D lead. Jake is also responsible for Academic Engagement at BMT. In recognition of his work to progress Academic Engagement in the maritime sector he was recently awarded the title of Honorary Associate Professor at the University of Exeter, and continues to engage in a range of collaborative research projects.

2. Why Do We Need Quantum Technologies?

We live in an increasingly uncertain world, where the pace and scale of technological development is increasing year on year. We are seeing the rise in information warfare; knowledge has always been the key to success, but in an a digital and connected world cyber attack may be seen as the preferable option by many nations and non-state players. To counter this there is a strong requirement for secure communications, where information security can be guaranteed.

Recent years have also seen the increasing importance of large area surveillance. With new hypersonic missiles and greater numbers of Uncrewed Underwater Vehicles (UUVS) being deployed for military use, greater sensor performance is required to maintain current reaction times. Technological development is often a double-edged sword, providing equal levels of opportunity and risk. While the same can be said for quantum technologies, the capability enhancement is so large that it could enable the effective counter of a wide range of existing threats.

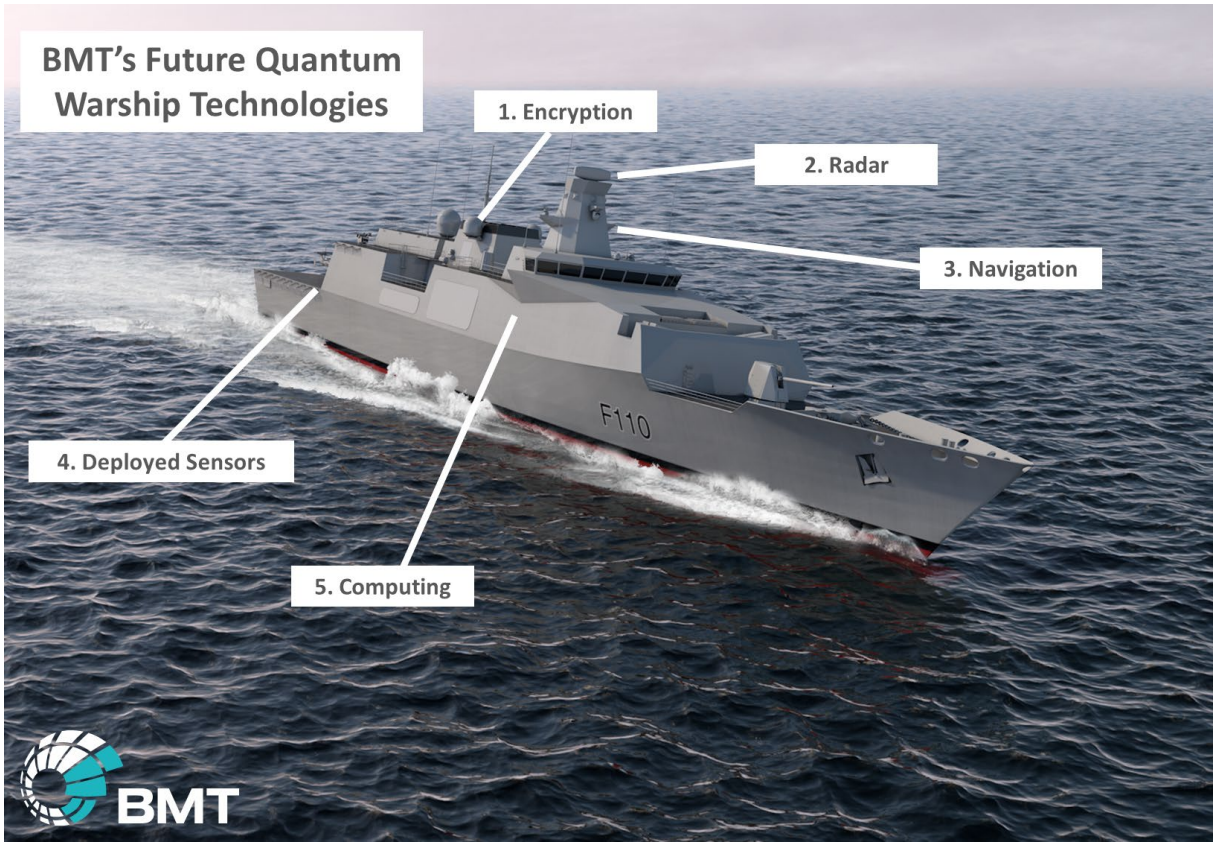

Figure 1: A Quantum Warship of the future is expected to look much the same as traditional warship, but it is the technology inside that sets it apart in five main areas.

3. Developments and Applications

The core development and application areas of Quantum Technologies in a Warship can be summarised into five key sections, as identified in Figure 1. These development areas are Encryption, Radar, Navigation, Deployed Sensors and Computing. The UK National Quantum Technologies Programme (NQTP, 2015) outlines how these different elements are being matured in the UK by a flagship government research programme designed to put the UK on the map as a quantum development hub. Other global hubs for the development of quantum technologies include the US, China, Japan and Germany with each having their own specialist development areas.

3.1. Encryption

Encryption technologies have the potential to enable secure and uninterceptable communication channels across large distances.

3.1.1. Quantum Random Number Generation

Cryptographic algorithms often require random values exclusively articulated as numbers, known commonly as a RAND. Implementations of these algorithms need access to a Random Number Generator (RNG) which will provide random numbers when required. A Quantum Random Number Generator (QRNG) is an RNG that relies on constructions based purely on quantum mechanics for its entropy. QRNGs do not provide any new mitigation against the threat from quantum computers to traditional public key cryptography; however, they can generate random numbers at very high speed, and, the constructions produce truly unpredictable numbers.

Methods for integrating these RNGs into larger systems and assessing their behaviour are well established. In practice, the unpredictability that QRNGs can potentially offer is hard to realise. A significant reason for this is that QRNGs will necessarily sit inside classical circuitry for collection and processing, and this classical circuitry adds noise to the measurement of the quantum state.

3.1.2. Quantum Key Distribution (QKD)

QKD is a mechanism for agreeing encryption keys between remote parties, relying on the properties of quantum mechanics to ensure that the key has not been observed or tampered with in transit. Since traditional public key cryptography algorithms may be vulnerable to a future large-scale quantum computer, new approaches are required that do not share this vulnerability. QKD claims to offer a potential mitigation since its security properties are based on the laws of physics rather than the hardness of some underlying mathematical problems.

QKD protocols provide a mechanism for two remote parties to agree a shared secret key, where the key cannot be observed or tampered with by an adversary without alerting the original parties. However, because QKD protocols do not provide authentication, they are vulnerable to physical man-in-the-middle attacks in which an adversary can agree individual shared secret keys with two parties who believe they are communicating with each other.

3.2. Quantum RADAR

The working principles behind quantum RADAR are simple; instead of using conventional microwaves it entangles two groups of photons, which are called the 'signal' and 'idler' photons. The signal photons are sent out towards the object of interest, whilst the idler photons are measured in relative isolation, free from interference and noise. When the signal photons are reflected back, true entanglement between the signal and idler photons is lost, but a small amount of correlation survives, creating a signature or pattern that describes the existence or the absence of the target object, irrespective of the noise within the environment.

While quantum entanglement in itself is fragile in nature, quantum radar has a few advantages over conventional classical radars. For instance, at low power levels, conventional radar systems typically suffer from poor sensitivity as they have trouble distinguishing the radiation reflected by the object from naturally occurring background radiation noise. Quantum illumination offers a solution to this problem as the similarities between the signal and idler photons (generated by quantum entanglement) makes it more effective to distinguish the signal photons (received from the object of interest) from the noise generated within the environment. The inherent benefit of quantum radar is that it will, in theory, be able to compromise attributes that constitute stealth technologies to render them invisible to conventional radar. The only downside is that this technology is still significantly far away from effective delivery and some fundamental concerns exist about if it could ever be a cost-effective solution to be mounted to a warship.

Alternatively, there are options to use quantum timing elements to create a next generation ‘networked radar’ instead. Traditional Radar systems are limited in their sensitivity by the co-location of transmission and reception signal units. By separating this out into multiple distributed transmitters and receivers it is possible to overcome fundamental sensitivity limitations so that smaller targets can be seen at longer ranges (UK QT Hub S&T, 2021).

3.3. Navigation

Using a range of different techniques new alternative navigation technologies can be developed to reduce the reliance on GPS systems. The UK is currently leading the development of such quantum navigation systems as seen by the Imperial University ‘Quantum Compass’ (Dunning, 2021).

3.3.1. Quantum Inertial Navigation System

Inertial Navigation Systems (INS) use a range of technologies to track the true movement of a platform, but all require a positional fix both to define the initial origin of the INS and then periodically afterwards to update the filters developing the ongoing assessment of position. As errors continually build a pool of errors grows around

the INS and the platforms precise position becomes less accurately known, until a new positional fix must be generated and the INS bought back to the platforms true position.

Typically these errors are of a magnitude of around 2000 yards over a 24 hour period, which means that the lay-over period between accurately establishing the platforms position is low. In open ocean a loss of Global Navigation Satellite Systems (GNSS) such as GPS for any period of time would push the conventional INS beyond the layover period and quickly impact combat effectiveness. A Quantum INS offers a revolution in accuracy and lay-over period, with the potential to practically eliminate the dependency on GNSS for own platform position and, more significantly, completely mitigate the immediate operational impact of both GNSS Spoofing and Jamming. Current estimates of the game changing inertial capability provided by quantum give an error margin of only 100m after 100 days (UK QT Hub S&T, 2021). Current UK development timelines predict this capability may be incorporated into a complete navigation solution as early as 2027.

3.4. Deployed Sensors

Quantum sensing in a range of forms has the huge potential to transform the naval domain and provide reliable long distance identification of threats.

3.4.1. Navigation

While the Quantum Inertial Navigation System will provide a step change in lay-over period the performance of navigation system is enhanced when positional information can be used to supplement the performance of the INS. Using an organic Quantum Gravimeter the platform will be able to conduct Simultaneous Location And Mapping (SLAM) as it moves through its operating areas and maintain a constantly updating assessment of its true position. The use of both Quantum capabilities in tandem will make the navigation system independent of GNSS and enable it to operate indefinitely without access to external positioning signals.

3.4.2. Anti-Submarine Warfare

Quantum Gravity Sensors are capable of detecting even very small changes in gravity, and therefore the presence of large submerged objects, with the potential to revolutionise the detection and localisation of submarines. With evolving technology readiness levels, stability Quantum Gravimeters will become viable in Maritime Patrol Aircraft, followed by the development of lighter sensors which could give platforms the opportunity to deploy gravity sensing drones to sanitise the water ahead of a moving Task Group or conduct Anti-Submarine operations over wide areas. These types of operations are made possible through the application of cold atom gradiometers. To give some indication of the units and the signal strengths involved, a 1 metre diameter hollow spherical void in soil at a depth of 30cm gives a gradiometer signal of only 10^{-7} s^{-2} (UK QT Hub S&T, 2021). In order to be able to detect submarines from aircraft or low earth orbit current systems measurement distance would need to be improved by a factor of 100 or more.

Alternatively new highly powerful ‘Double Resonance’ Magnetometers are being developed with potential applications in the defence market. These new sensors have a target sensitivity of 1 pT/√Hz in 0 - 2kHz bandwidth in order to provide a game changing capability (UK QT Hub S&T, 2021). For this to happen significant optimisation of the ‘physics package’ and control electronics is required.

3.5. Quantum Computing

As previously discussed these devices exploit the complex nature of quantum information and superposition. Because qubits can be put into many states at once, a quantum computer can process many inputs simultaneously instead of having to go through them one by one like a conventional machine. For some types of problem, this can mean a much faster solution.

For this reason quantum machines are much faster at searching large databases and factoring large numbers which is of critical importance because it is behind the most common form of cryptography, which is used to protect financial and other sensitive data. There are other applications in design and modelling that would vastly improve and expedite current processes, including aircraft, ship, boat and weapon system design. It should however be noted that these systems are not currently as flexible as a regular computer, and cannot be used to solve every type of mathematical problem. The current ‘quantum annealing’ solutions can only solve certain types of problem, but utilises effects known as ‘quantum fluctuations’ to find the best solution. This has lead to many companies claiming to have achieved ‘Quantum Supremacy’ when quantum computers outpace traditional computers and thus countering traditional global encryption techniques, but due to the limitations of the technology this is widely disputed. Quantum annealing computers require problems to be expressed in the language of

operations research problems, and so for now global cryptography is safe. However, in the near future software solutions could be developed to convert traditional gated problems into annealing applicable languages.

4. Conclusions

In conclusion, there are huge opportunities for the application of quantum technologies for use in commercial shipping and warships. However, on the whole the technologies are still quite immature, currently confined to lab based demonstrations and a long way off full implementation. The UK government is working hard to rapidly develop the supporting technologies, forming the National Quantum Technologies Programme as a partnership between EPSRC, Innovate UK, Dstl, NCSC, NPL and BEIS; spending over £270 million over the last five years (NQTP, 2021).

One prominent quote that explains the complexity of the problem is from Richard Feynman, an American Quantum Physicist from the 20th century. When talking about the paradox of quantum physics Feynman said 'The "paradox" is only a conflict between reality and your feeling of what reality "ought to be". If you are not completely confused by quantum mechanics, you do not understand it' (Feynman, R., 2021). This quote explains how this is not a simple topic and there is still a lot that needs to be done to understand Quantum Mechanics and the tools required to capture its full sensing power.

Some of the overarching key challenges include:

- **Reduce Size, Weight, Power and Cost (SWaP-C)** – Moving away from lab based demonstrations to affordable and practical system units.
- **Economic quantum particle capture and cryogenics** – Many of the current lab based systems require cryogenic temperatures close to absolute zero to enable the effective capture and tracking of a particle. This needs to become economical or find a way to increase overall temperatures.
- **Sensitivity and Focus** – Some sensor systems that have got working lab based protoypes can also be too sensitive and overwhelmed with information. We need to find a way to channel and focus the detection power to make the outputs useful.
- **Reducing Qubit Error** - Manipulating individual qubits can introduce errors in calculations, and unless that error rate falls below a certain allowable level, then entangling more and more qubits will only add more noise to the system. We need to find a way to reliably upscale from singular qubit systems. In order to help tackle this challenge the UK government has launched a 'Technical Roadmap for Fault-Tolerant Quantum Computing' (Fruchtman and Choi, 2016).

Although these challenges are large on paper, the rewards are equally huge. If these problems and others can be resolved; if true quantum supremacy can be obtained then it will signal the biggest technological leap in sensing and computational technology the world has ever seen.

Acknowledgements

The authors would like to acknowledge all those who supported the quantum technologies research conducted at BMT and the production of this paper.

References

Dunning, H., 2021. Quantum 'compass' could allow navigation without relying on satellites | Imperial News | Imperial College London. [online] Imperial News. Available at: https://www.imperial.ac.uk/news/188973/quantum-compass-could-allow-navigation-without/ [Accessed 06 October 2021].

DWave, 2021. Quantum Computing Primer. [online] Dwavesys.com. Available at: https://www.dwavesys.com/tutorials/background-reading-series/quantum-computing-primer [Accessed 06 October 2021].

Feynman, R., 2021. Richard P. Feynman Quotes (Author of Surely You're Joking, Mr. Feynman!). [online] Goodreads.com. Available at: https://www.goodreads.com/author/quotes/1429989.Richard_P_Feynman [Accessed 06 October 2021].

Fruchtman, A. and Choi, I., 2016. *Technical Roadmap for Fault-Tolerant Quantum Computing*. UK National Quantum Technologies Programme.

NQTP, 2015. *A roadmap for quantum technologies in the UK*. UK National Quantum Technologies Programme.

NQTP, 2021. *EPSRC Quantum Technologies Community Webinar – 1st July 2021*. UK National Quantum Technologies Programme.

Medium, 2021. Google's Quantum Computer Is About 158 Million Times Faster Than the World's Fastest Supercomputer. [online] Medium.com. Available at: https://medium.com/predict/googles-quantum-computer-is-about-158-million-times-faster-than-the-world-s-fastest-supercomputer-36df56747f7f# [Accessed 06 October 2021].

UK QT Hub S&T, 2021. *QT Hub Sensors and Timing Technology Roadmap*. June 2021. UK National Quantum Technologies Programme.

Word Count:2873