3 year build compressed into 5 minutes just for fun:
https://www.youtube.com/watch?v=6EVlGwZSoXg

What madness is this? Putting containers with weapons on ships with large flat spaces ...

full NPS paper here
https://calhoun.nps.edu/bitstream/handle/10945/68295/21Sep_Banuchi%20et%20al.pdf

If you won't do it for ASuW or land attack; at least think of doing it for for ASW Mother ships backing up their swarms of hunters with some sting - the odd container load of locusts etc would sort any boat's day

Mullets might also be reminded that the containers can be snappily removed to the wharf for provision of 'superior' large flat spaces for 'bounded by your own imagination of enhancing your place on the command plot' photo opportunities during first night in madness Cockers Ps..

> The literature review section describes the manner in which TLAM cruise missiles must be launched in salvos as large as 16 missiles to defeat a target with active defense. Due to its exceptional speed, maneuverability, and low flight path, a single hypersonic glide body missile is likely to be able to overcome an active defensive system that could defeat even a salvo attack of TLAMs. An Arleigh Burke-class destroyer is equipped with 96 TLAMs, or six salvo attacks of 16 missiles each. This means that a vessel equipped with 12 hypersonic missiles can attack as many actively defended targets as two Arleigh Burke-class destroyers firing 16-missile salvos. 12 AURs was chosen as the highest rating for this attribute because it represents the offensive equivalent of two entire vessels in the scenario where an actively defended target is being attacked. While additional hypersonic AURs on board a vessel does represent the ability to attack more targets, there are other considerations, such as cost or effect on other vessel missions, that prevent additional AURs beyond 12 from increasing the rating of this attribute. Table 7 summarizes the number of AURs that each candidate system can store.

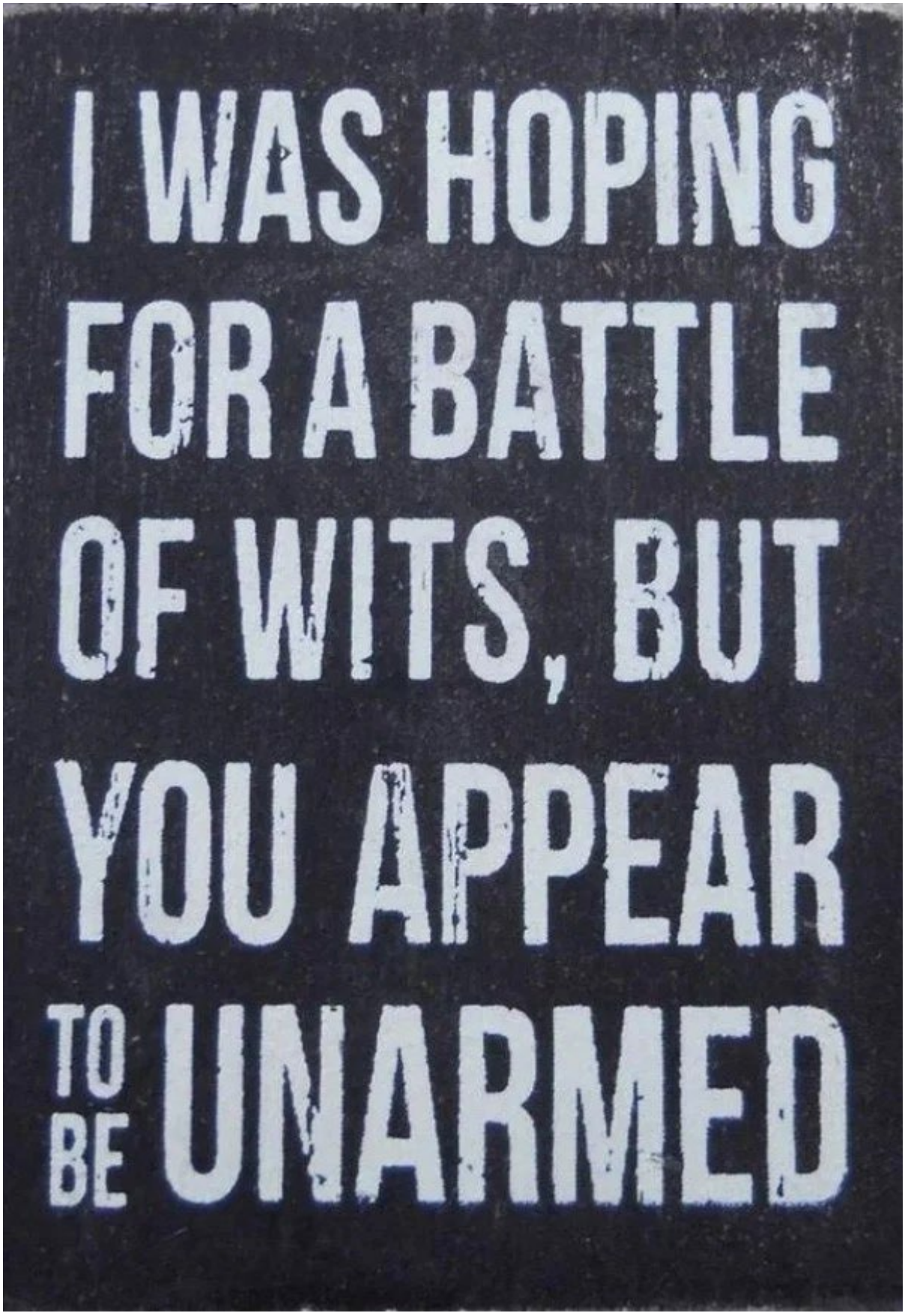
Just sweeping the intray and found this from Jan 13 - just more on the US industry base
https://seapowermagazine.org/navy-ship-construction-repair-hampered-by-lack-of-suppliers-skilled-workers/

Another from Jan 13 -

Decision to be made ‘in future’ on adding UK weapons to P-8

By
George Allison

Mention of the Mark 54 brings one of my fave jokes into play


I WAS HOPING
FOR A BATTLE
OF WITS, BUT
YOU APPEAR
TO BE UNARMED

A Minister has stated that British weapons may be added to P-8 "*once the aircraft has reached full operating capability and there has been time to study the optimal utilisation model for the UK".*

The information came to light via a Parliamentary Question.

Kevan Jones, MP for North Durham, asked:

"To ask the Secretary of State for Defence, when (a) UK torpedoes and (b) UK sonobuoys will be cleared for use for the P-8."

Jeremy Quin, Minister for Defence Procurement, responded:

"The RAF Poseidon MRA1 was delivered in the same configuration as that operated by the US Navy which enables a swifter introduction to service, economies of scale and interoperability with close allies. We envisage that once the aircraft has reached full operating capability and there has been time to study the optimal utilisation model for the UK, the Department will be in a position to make decisions on future equipment configurations."

This appears to be a softening in position. Back in 2016, then Minister for Defence Procurement Philip Dunne said:

"The Department intends to bring the P-8A into service without significant modification to ensure the delivery of operational capability as soon as is practicable. There are no current plans to integrate Stormshadow or other UK manufactured weapons onto the aircraft."

The P-8 itself is able to conduct anti-submarine warfare, anti-surface warfare and shipping interdiction along with an electronic signals intelligence role. Undertaking this role would require the aircraft (in British service specifically as the Americans already do this) to be cleared to carry various missiles and other weapons.

The Mk 54 Torpedo is so far the only weapon that has been cleared for use on the aircraft in British service.

Jeremy Quin, Minister for Defence Procurement, said earlier this week:

"As at 4 January 2022 the Poseidon MRA1 has been cleared for Anti-Submarine Warfare, Anti-Surface Warfare and Search and Rescue in support of submarines. It is assisted in these roles by its sophisticated suite of radar and data gathering equipment. The Mk 54 Torpedo has been cleared for use on the aircraft."

Cyber Torpedoes – How to Sink a Modern Ship

The version I got from the ANI doesn't include the figures which you can see if you subscribe to the ANR. The ANI website stopped communicating when I went looking and that instantly put it into the too hard basket. No matter his story is a good one - and anyone who ever questioned the obsession of Defence to kill stand alones or even just worked the DRN will have seen what he is talking about.

Also, in moments of OCD, I put the 'e' in every instance of 'Torpedos' in the original.

By Commander Robert Smilie RAN*

Introduction

One of the most dangerous threats to shipping in World War II was the German U-boat armed with torpedoes – an enemy that was below the surface, unseen, hard to detect and lethal to ships. Fast forward to today and, yes, submarines are still dangerous, but there is a new threat to shipping that is below the surface, unseen, hard to detect and lethal to ships: cyber attacks.

Advances in technology have significantly improved all aspects of ship safety. This has allowed for minimum-crewed vessels; accurate navigation, communications and tracking of vessels for safety of life at sea (SOLAS); and automation of machinery spaces and ship control. Nearly every system on a modern ship has some form of computer that has made operating ships easier and safer. But what if those same systems provide an unseen danger below the surface that is hard to detect, a new attack vector that can easily cripple a ship, a 'cyber torpedo'? Unlike a traditional torpedo, a cyber torpedo would not necessarily sink a ship, but it could achieve the same outcomes of sea control or sea denial, by preventing that ship from sailing or executing its mission.

The threat of cyber attacks is pervasive across all industries and sectors, including maritime and military. There are numerous examples of cyber attacks being used by nation-states as a mechanism for achieving strategic objectives, shaping and influencing the battlespace, intelligence gathering, and destruction. Modern technology has enabled all aspects of our lives, providing convenience, automation and safety; unfortunately for far too long security has been an afterthought or non-existent for critical safety systems, leaving them vulnerable to cyberthreats – ships included.

The RAN is undergoing its largest modernisation and capability expansion since World War II, investing over $90 billion in new naval ships and submarines.[1] These new ships and submarines come with complex interlinking systems that are connected not only to each other but also to shore infrastructure and the internet, creating a large cyber attack surface. With such a significant investment, the RAN must consider cybersecurity and defensive cyber measures seriously to ensure these capabilities are able to deploy effectively and not be vulnerable to cyber attacks.

Cyberthreats

Cyberthreat actors come in many forms including nation-state actors, cybercriminals, cyberterrorists, hacktivists, and insider threats that can be both malicious and unintentional. While all of these are creditable threats to RAN ship systems, supply chains and port infrastructure, the nation-state actors are of particular concern.

Nation-state cyber actors are well resourced, professional and highly motivated. They aim to *gain intelligence and disrupt other nations via cyber means*.[2] They operate covertly and usually do not acknowledge their actions. Nation-state actors can have a 'cyber army' or hire hackers to achieve their aims, operating in the grey zone, without fear of legal retribution. There is a rising 'cyber cold war'[3] occurring as nations strive to gain the upper hand in the information and cyber domain.

There is often a belief that a system needs to be connected to the internet to be vulnerable to cyber attacks; as a result, disconnected systems have older operating systems that are not updated to the

latest security standards and do not have antivirus software. This naive view is frequently used as an excuse to save money on often expensive cybersecurity measures.

Stuxnet[4] was a cyber weapon reportedly developed by the United States and Israel[5] to derail Iran's nuclear program. Stuxnet was successfully used against an Iranian nuclear facility, infiltrating secure systems that were not connected to the internet or outside world in any way. Stuxnet physically destroyed centrifuges in the background whilst the operators and engineers saw normal results on their control screens. It successfully delayed Iran's nuclear program by years. Stuxnet provides an excellent example of what can be achieved by an actor with enough resources and intent to compromise a non-internet-connected system and achieve a physically destructive result.

Stuxnet targeted programmable logic controllers (PLCs) used to automate machine processes. PLCs are found in most operational technology (OT), which differs from traditional information technology (IT) as it provides the link between the cyber and physical worlds. This includes national critical infrastructure such as electricity networks, water and sewerage systems, and even health devices used in hospitals. These same PLCs are used in engineering and weapons systems in ships. A cyber attack against an OT system can have a physical destructive effect, ships included.

OT systems are far more complex than traditional IT and are often not connected to the internet. A software update to an IT system is easily achieved and, with the system being offline, a mere inconvenience for a user. If there is an issue, the computer can be replaced with ease, reducing system downtime. Legacy OT systems have older operating systems, software and hardware that are not easily updated. Downtime has a physical world effect that is difficult to manage, and if there is a problem with the new hardware or software it is not straightforward to resolve. This costs time and money and results in that asset being unavailable for use. It is often easier to not upgrade the system at all and risk cyberthreats. An upgrade to a ship system would require downtime and testing to provide assurance that it will operate in the correct way when needed in an emergency or warlike situation. The risk of upgrading a system frequently for a cyberthreat is often outweighed by the risk of ensuring the system remains working correctly.

Cyber War Isn't Coming – Cyber War Is Here!

In June 2020, Prime Minister Scott Morrison announced that Australia was under attack from a sophisticated nation-state cyber actor.[6] The cyber attacks were *ongoing, unrelenting and increasing in frequency and scale*. Prime Minister Morrison described the attacks as:

… targeting Australian organisations across a range of sectors, including all levels of government, industry, political organisations, education, health, essential service providers and operators of other critical infrastructure …

While the government has not publicly attributed the cyber attacks, there are only a handful of nations, outside of the Five Eyes, capable of such sophisticated attacks, including Russia, China, Iran, Israel and North Korea. What can be gleaned is that the cyberthreat is real, is pervasive and must be considered as part of military planning and capability development.

In July 2020, the United States National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) published Alert AA20-205A – 'NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems'.[7] The alert warns that there is evidence of nation-state cyber actors targeting OT due to the criticality of the systems and the real-world effect it can have. The alert recommends that immediate action be taken to secure OT assets against these threats.

Defence and industry partners have been targeted by cyber attacks, as shown in the headlines in Figure 3. Nation states are building sophisticated offensive cyber capabilities that can be deployed against all sectors, including government, industry and national critical infrastructure. A successfully offensive cyber attack against a modern ship could result in a nation gaining sea power.

Attacks could target industry partners, port facilities, supply chains or ship systems. Disabling a critical ship safety system could prevent a ship from sailing for weeks while incident response and remediation activities are conducted. A more malicious attack on the ship's control systems could disable a ship at sea, leaving it unable to manoeuvre effectively for safe navigation or collision avoidance. Commonality of systems provides benefit for maintenance, training and ease of use. However, an entire fleet could be disabled by the same cyber torpedo through a firmware update that is shared across multiple platforms, forming a pseudo naval blockade, with ships unable to leave port.

In 2013 a research team from the University of Texas at Austin conducted several demonstrations and studies of cyber vulnerabilities in different aspects of ships. These included exploits in the electronic chart display and information system (ECDIS) or navigation display, where they were able to offset the ship's position on the chart and effect a physical ship movement through a cyber attack.[8] The research team were also able to spoof false information into the ship's automated identification system (AIS) due a flawed design in which AIS data is assumed to be genuine with no security of verification protocols.

Defeating the Cyberthreat

Offensive cyber operations are a real threat, particularly from a nation-state, but they are complex and expensive to conduct. Simple measures can be taken to make it cost-prohibitive and as difficult as possible for them to fire their cyber torpedos, as shown in the 'Cybersecurity value pyramid' in Figure 4.

Security by design in ships needs to become the norm. Defence and industry should work together closely to design systems that can be easily upgraded and have sufficient measures in place to reduce vulnerabilities and to respond to and recover from cyber attacks. Processes need to include cybersecurity measures that decrease the risk of cyberthreats infiltrating systems, such as active management of USB devices and maintenance laptops similarly to the way that weapons and ammunition are treated.

Passive defence relies on human factors. A clicked link in an email is all it can take for a successful cyber attack to occur. Humans will always be the weakest link in the cyber chain; however, they can also be the strongest with the correct awareness and training. A technical solution alone will not prevent cyber attacks; the modern sailor needs to be cyberwarfare aware to ensure they do not become the entry point for a cyber torpedo that could sink a ship. Investment in cyber awareness and cybersecurity training is required to defeat cyberthreats. Senior leadership engagement and support is essential for any cyber-awareness program to be successful. Organisations often do not invest time or money into cybersecurity measures until it is too late and they have been victim to a cyber attack.

Conclusion

Cyberthreats are persuasive and continue to grow across all sectors. For the RAN, ships are often designed and delivered without consideration of the ongoing cybersecurity requirements for systems and the need to stay contemporary to reduce risk of cyber incidents. The threats of nation-

state actors, outdated systems, lack of cyber awareness and demonstrated maritime vulnerabilities need to be considered and risk mitigated to ensure ships will be survivable from cyber attack.

Viewing cyberthreats in the context of gaining or losing sea power will assist senior decision-makers in understanding the threats and apportioning sufficient resources to mitigate them. Simple and effective measures can be implemented to defend against the growing threat of cyber torpedoes.

***Commander Smilie** joined the RAN through the Australian Defence Force Academy (ADFA) in 1998 as a Maritime Warfare Officer, graduating in 2000 with a Bachelor of Computer Science.

He has deployed to the Middle East on Operation CATALYST in HMAS *Newcastle* and has had postings as Executive Officer HMAS *Geraldton* and Commanding Officer HMAS *Wewak*. As Commanding Officer of *Wewak* he deployed to Operation ANODE, with the ship being awarded the Landing Craft Heavy Proficiency Shield under his command in 2010.

[1] Department of Defence, *Naval Shipbuilding Plan*, Commonwealth of Australia, Canberra, 2017, <http://www.defence.gov.au/NavalShipbuilding/Plan/>.

[2] J Hatch, 'The nation state actor', *BAE Systems* [website], 2021, <https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor>.

[3] R Browne, 'Chess legend Garry Kasparov warns of cyber cold war', *CNBC* [website], 20 May 2019, <https://www.cnbc.com/2019/05/20/chess-legend-garry-kasparov-warns-of-a-cyber-cold-war.html>.

[4] McAfee, 'What is Stuxnet?', *McAfee* [website], <https://www.mcafee.com/enterprise/en-au/security-awareness/ransomware/what-is-stuxnet.html>.

[5] The United States and Israel have not acknowledged any involvement in Stuxnet.

[6] A Probyn & S Dziedzic, 'Scott Morrison's "urgent" hacking warning shot shows Australia won't shy away from China's cyber attacks', *ABC News* [website], 20 June 2020, <https://www.abc.net.au/news/2020-06-20/why-australia-acted-on-china-hacking-cyber-attack-scott-morrison/12376700>.

[7] National Security Agency & Cybersecurity Infrastructure Security Agency, 'Alert AA20-205A', *Cybersecurity Infrastructure Security Agency* [website], <https://us-cert.cisa.gov/ncas/alerts/aa20-205a>.

[8] J DiRenzo, DA Goward & FS Roberts, 'The little-known challenge of maritime cyber security', 6th International Conference on Information, Intelligence, Systems and Applications (IISA), 2015.

A Melbourne-based SME has been selected to deliver key infrastructure to support the US Navy's P-8A Poseidon aircraft.

18 February 2022 By: Charbel Kadib

In the olden days before media hype we used to call them workstands. This seems abnormal

because it appears that the CoA was involved in a bit of nurturing, facilitating and even assisting to make this export happen. So, based on the story , all I can say is BZ alcon.

The US Navy has awarded a US$2.46 million ($3.4 million) contract to Victorian manufacturing firm AirFab for the delivery of 22 specialised Wide-Band Satellite Telecommunications System work stands designed to provide technicians safe access to P-8A Poseidon Maritime Patrol aircraft.

This would enable technicians to access the P-8A Wide-Band Satellite Communication station and conduct fuselage inspections without overextending.

The stands are built to withstand harsh environments, including those encountered by forward operating bases, and also include integrated safety features to provide added protection to personnel.

AirFab, based out of Ferntree Gully, Melbourne, developed the work stands in collaboration with the Royal Australian Air Force (RAAF) and the US Navy to ensure the design met the requirements of P-8A Poseidon Maritime Patrol aircraft.

Minister for Defence Industry Melissa Price congratulated AirFab, adding the contract award demonstrated the export opportunities available to local industry.

“Working with Royal Australian Air Force gave AirFab direct engagement with the US Navy that an Australian small business would not normally have had access to,” Minister Price said.

Member for Aston Alan Tudge said the export project would help bolster the local economy in Knox.

“The materials used in the stands are Australian made, with the steel and aluminium sourced from local manufacturers,” Mr Tudge said.

“The export opportunity not only provides direct growth to AirFab but allows for residual employment and training to more than 20 small and medium sized companies that AirFab works with.”

Separate to the US Navy order, AirFab is manufacturing eight work stands for the RAAF P-8A Poseidon Maritime Patrol fleet.

“The purpose-built work stands will allow technicians to access the P-8A Wide-Band Satellite Communication station and to safely conduct fuselage inspections without overextending,” Minister Price added.

“This contract recognises that Australia’s Defence industry is capable of producing and exporting high-quality safety equipment for not only our Australian Defence personnel but to our allies.”

Panel: Smaller NATO Navies Struggle with Recruitment, Awareness

By: John Grady
January 11, 2022 7:44 PM

Given what I see on DPR it's pretty clear that most Australians, including many of those inside it, wouldn't understand how its navy actually works either

from a 2019 Remuneration tribunal report Presently, the numbers of members leaving the Navy, or being unwilling to return to sea
after their initial obligation period, has resulted in workforce ‘hollowness’* in the mid-ranks which is now threatening the ability of Navy to meet government tasking and the delivery of capability.

* described as sustained shortfalls of skilled members to deliver key outputs against a valid enduring requirement, viewed in terms of rank, employment categories and levels of experience

Three senior NATO navy officers said their countrymen have cases of “maritime blindness” and don’t understand how their navies operate.

Speaking at an international navies session at the Surface Navy Association symposium in Arlington, Va., Capt. William Quinn, naval attache at the Canadian Embassy, said despite his nation’s extensive coastlines on the Atlantic, Pacific and Arctic oceans, “I run into many Canadians that don’t know we have a navy.”

In Canada, to bring attention to the sea services and boost enlistments, Ottawa has positioned its reserve components inland — in the Alberta and Manitoba provinces — to attract young people.

Canada needs to address manpower issues as the country modernizes its surface fleet while maintaining readiness, Quinn said.

The lack of naval awareness extends to NATO countries, like Germany and the Netherlands, senior NATO sea officers said.

“Germans love the sea — from a beach,” said Capt. Ivo Schneider, Germany’s naval attache in Washington.

Schneider said Germany uses a training ship to help recruits “learn to serve where they are less comfort zones” of access to digital communications and “learn to serve at sea and the maritime environment” as fundamental to their education in a naval career.

FGS Bayern at Changi Naval Base, Singapore. German Embassy, Singapore Photo

The lack of awareness has hurt the Netherlands capabilities, Marine Col. Jarst de Jong said. He noted the Netherlands’ sea services are already short 17 percent of authorized personnel and the “bottleneck” is particularly acute in the technical skills.

“Nobody in the Netherlands realizes we [in the sea services] are focused on national security,” de Jong said.

“We can’t do it alone,” de Jong said about the recruiting challenges in a nation with a shrinking population. Complicating recruiting in the Netherlands is 20 years of steady budget cuts for defense at a time when civilian careers in technology are booming. He added the new government has raised defense spending to 1.8 percent of gross domestic product, still below the 2 percent threshold that NATO established in 2014.

Some of that can be applied to recruiting and retaining high-quality recruits.

de Jong said the Netherlands government and navy is “trying to create a maritime ecosystem” to include electronics, shipbuilding and the sea services to meet national security requirements and commitments to NATO for collective defense. He added unmanned and autonomous systems could be a major step forward in easing personnel and readiness shortfalls that exist now and could worsen over time.

Looking at future needs, Quinn added, “I’m not saying take man out of the loop” in combat decision-making but there is a role for unmanned systems “going into high-risk areas.”

There are ethical concerns over AI and machine learning in warfare, Schneider said, asking a series of rhetorical questions. “How about computers leading other computers” or “how about computers leading people” in making decisions in combat.

Still to meet future needs and also retain skilled sailors, Germany is to open a new Maritime Warfare Center in Bremerhaven this fall to combine research and training.

Berlin has also worked extensively in the relatively shallow Baltic Sea on improving and modernizing anti-submarine warfare technologies and practices as Russia updated its Northern Fleet’s submarine fleet.

He added ASW remains “a major NATO shortfall area” in the North Atlantic.

Neither Schneider nor Quinn saw the Arctic as becoming an immediate security threat to Germany or Canada. Quinn said that the Northern Sea Route closest to Russia now is more attractive to merchant shipping than the poorly charted Northwest Passage.

“The bigger issue will be how we divide up that pie” of mineral and energy exploration, Quinn said. He added this has to be done while preserving environmental safeguards and the rights of the indigenous peoples.

The Arctic “is a model for the rules-based order,” Schneider said.

When asked about becoming more interoperable with the U.S. Navy, the three said their nations would be joining the USS *Gerald R. Ford* (CVN-78) strike group for exercises in the coming year.

Schenider said the German navy is also seeking opportunities to train with an American amphibious group in the coming year. De Jong added the Netherlands is also looking at improving its amphibious maritime capabilities as its national security budget rises in the future.

N221-065 TITLE: Low Cost, Small Form Factor Scalable Receive Array

OUSD (R&E) MODERNIZATION PRIORITY: General Warfighting Requirements (GWR)
Cool- the five fingers of death receiver.
TECHNOLOGY AREA(S): Sensors

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Apply innovative technology to develop a five-band compact Modular Expansive Spectrum Passive Receiver (MESPR) to address gaps in fielding passive sensor recognition and countermeasure algorithms.

DESCRIPTION: Navy surface ship and submarine probability of survival improves when protected by torpedo defense countermeasure systems. Adversarial weapons are increasing sophistication that requires the Navy to rapidly implement and integrate pace-the-threat technology via the Navy’s Technical Insertion/Advanced Processor Build (TI/ABP) process. Traditional receivers perform at a purposed frequency band of specific interest. Legacy system architectures typically do not easily support technology insertions. The Navy has invested in system updates for cost-effective technology insertions. MESPR would directly benefit Surface Ship Torpedo Defensive (SSTD) and submarine torpedo defense programs. MESPR addresses the need to counter technology improvements inherent in threat torpedoes. The innovative technology could be dual purposed to enhance or replace unmanned undersea vehicle (UUV) and torpedo sensor suites. The expansive spectrum is comprised of the Super Low Frequency (SLF), Ultra Low Frequency (ULF), Very Low Frequency (VLF), Low Frequency (LF), and Medium Frequency (MF) frequency bands as designated by the International Telecommunications Union (ITU) for radio spectrum designators and bandwidths to include:

- SLF: 30 Hz-300 Hz
- ULF : 300 Hz-3 kHz
- VLF: 3K Hz-30K Hz
- LF: 30K Hz to 300K Hz
- MF: 300K Hz to 3,000K Hz

A technology challenge will be to implement MESPR using traditional and non-traditional materials and hardware to achieve efficient transduction across the defined bandwidth. A second technology challenge addresses complex issues related to spectrum detection and correlation across a five-band receiver. A third technology challenge defines a prototype capable of performing while a local host is transmitting broadband and structured energy. To decrease technical risk for modularity and Space, Weight and Power (SWaP), improvements can be incrementally addressed as Phase II and Phase III activities progress. The SWaP of the MESPR prototype must be developed for technology insertion within three inch, four inch, and six inches countermeasure systems. Operational depth of the MESPR is up to 2,000 feet below ocean surface. The MESPR concept must include passive sensor and sensor configurations for sensitive detection with high dynamic range, dynamic array gain, volumetric localization, and beam steering. Traditional and non-traditional sensor and mechanical model and simulation analysis will support the proposed concept to meet the requirements in this Description. Modeling and simulation will address receive sensor and detection degradation caused by flow noise, local coherent signals and interferers. A variety of torpedo defense land-based and at-sea demonstrations may be utilized to assess technology performance and viability.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. Owned and Operated with no Foreign Influence as defined by DOD 5220.22-M, National Industrial Security Program Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence Security Agency (DCSA), formerly the Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances, in order to perform on advanced phases of this contract as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material IAW DoD 5220.22-M during the advance phases of this contract.

PHASE I: Define and identify a feasible concept for the innovative MESPR prototype to demonstrate performance, modularity, and SWaP constraints. Identify candidate sensor and hardware culminating in a modular and compact design approach. Perform modeling and simulation to provide initial assessments of performance and SWaP limitations. Incorporate a Transmission Control Protocol/Internet Protocol (TCP/IP) electrical to optical Ethernet interface for receipt of command-and-control messages while sending MESPR raw and processed sensor data and hardware status. The development approach will address how compact processing and programmable logic are utilized to locally process sensor receive data. Intelligent hardware must have features to meet Cybersecurity and data protection requirements. Commercial Off-The-Shelf (COTS) components must be in production currently and planned to be in production for a minimum of three years. A hardware obsolescence approach must be addressed in Phase I. Develop a risk adverse approach to incrementally demonstrate MESPR performance, modularity, and cost management. The Phase I Option, if exercised, will include the initial layout and capabilities description to implement the concept and approach in Phase II. A final Phase I report for this SBIR effort will identify an innovative and feasible approach for Phase II to demonstrate working prototypes. A schedule will be provided to identify key Phase I and Phase II component and MESPR technology milestones.

PHASE II: Develop the MESPR prototype based on Phase I modeling and analysis, Establish performance parameters through continued modeling, sensor, and hardware experimentation. Construct and demonstrate an operational prototype. Perform performance and environmental evaluation testing of the MESPR prototypes based on the derived performance parameters. Testing will be the responsibility of the executing company, to include static and dynamic testing to assess utility for passive receive sensitivity and directionality across the MESPR band of interest. A functional prototype will be demonstrated in a relevant environment at a Navy facility such as the Naval Undersea Warfare Center (NUWC) Seneca Lake Sonar Test Facility. A prototype will demonstrate temperature thermal cycling, Grade A shock, vibration analysis and cyber resilience. Prepare a technical description document and user guide. Update the schedule prepared in Phase I to identify key Phase II and Phase III technology milestones. Deliver three to five working prototypes

for further assessment by the Government. In support of Phase II prototype development and Phase III technology transition, the Navy will identify specific torpedo defense hardware targeted for MESPR integration, test, and demonstration.

It is probable that the work under this effort will be classified under Phase II (see Description section for details).

PHASE III DUAL USE APPLICATIONS: Integrate the Phase II delivered MESPR prototypes with Government identified torpedo defense hardware. Identify incremental technology improvements to achieve end goals. Demonstrate MESPR technology improvements through planned prototype updates using lessons learned in Phase II and Phase III. Demonstrate the MESPR technology can be inserted and interoperable with torpedo defensive countermeasures to achieve performance and SWaP objectives. Evaluate three to four Phase III final prototypes for delivery. Support at-sea demonstration from a U.S. Navy platform to assist evaluation of the design in a relevant environment. Technical and logistic documentation will be developed to support technology transition to a PMS415 program of record. The schedule prepared in Phase II will be updated to identify key Phase III component technological milestones and will include a 12-to-24-month technology transition schedule.

A Commercial application of MESPR could support a producer of Autonomous Undersea Vehicles (AUVs). As an example, an AUV could search for a black box from a downed airplane.

REFERENCES:

1. Burdic, William S. “Underwater Acoustic System Analysis.” Prentice Hall, Englewood Cliffs, New Jersey, 1991. https://asa.scitation.org/doi/abs/10.1121/1.391242.
2. Butler John L. and Sherman Charles H. “Transducers and Arrays for Underwater Sound.” Springer International Publishing, Switzerland, 2016.
3. Brown, Jeremy, A. “Fabrication and performance of a single-crystal lead magnesium niobate-lead titanate cylindrical hydrophone.” The Journal of the Acoustical Society of America 134, ; https://doi.org/10.1121/1.4812274.
4. Abdul, Basit. Mastronardi Vincenzo M. and others. “Sensitivity and Directivity Analysis of Piezoelectric Ultrasonic Cantilever-Based MEMS Hydrophone for Underwater Applications.” Journal of Marine Science and Engineering, 9 October 2020.
5. Eovino, Benjamin T. “Design and Analysis of a PVDF Acoustic Transducer Towards an Imager for Mobile Underwater Sensor Networks.” Electrical Engineering and Computer Sciences University of California at Berkeley. Technical Report No. UCB/EECS-2015-154, http://www.eecs.berkeley.edu/Pubs/TechRpts/2015/EECS-2015-154.html May 26, 2015.

N221-058 TITLE: Electronic Warfare Human Machine Interface Training

OUSD (R&E) MODERNIZATION PRIORITY: General Warfighting Requirements (GWR)
Just for you Sam
TECHNOLOGY AREA(S): Human Systems

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop a game-based, dynamic Electronic Support Measures (ESM) training prototype utilizing TI-20 AN/BLQ-10 automation, displays and capabilities to include realistic scenarios and environmental factors enabling stress-habituation.

DESCRIPTION: The operation of modern submarines is complex and requires continuous training to learn how to effectively operate the warfighting systems. The current trend is to extend classroom training with advanced training techniques through the Navy's "Sailor 2025" program. This program describes the urgent need for Ready, Relevant Learning (RRL) to ensure that sailors have the warfighting skills they need. RRL requires a reconstruction of training techniques, adaptability of training location (i.e., standalone systems, classroom-based workstations, or cloud-based programs), a learning continuum (to ensure skill acquisition, mastery and maintenance), and requires that training products take advantage of the latest in learning technology (i.e., serious games and YouTube-like videos). The focus of this SBIR topic is discovering the best combination of cognitive experiences and computer-guided gamification learning techniques. Coupled with existing combat system simulation systems, the trainer will use cognitive training techniques to teach sailors how to effectively learn and operate advanced Electronic Support Measures (ESM) systems quickly and accurately. This SBIR effort is about connecting with each individual and coaching them to reach their highest potential using advanced training capabilities.

PMS-435 seeks to develop an engaging, multi-modal, performance-based ESM trainer that addresses the Navy's vital need for RRL by amending the deficiencies of the current AN/BLQ-10 Computer-Based Training (CBT) as well as the lack of commercially available software to adapt to such a need by utilizing the automation and advanced displays associated with the TI-20 upgrade to the AN/BLQ-10 system. This SBIR topic seeks development of innovative training techniques and their integration with a performance-based navigation engine. The state-of-the-art trainer shall utilize an innovative training engine that calculates in-situ proficiency measurements, which provide unique learning paths through the material. The training engine will be implemented with three additional innovation areas to develop a unique trainer that accelerates learning and improves performance. The following areas of innovation are to be addressed by this trainer:

1. Dynamic Training Scenarios: The current AN/BLQ-10 CBT uses a pre-defined calibrated set of scenarios to measure performance and drive navigation. Continued use of CBT indicates that sailors become accustomed to the existing scenarios, therefore diminishing its effectiveness. The solution involves the development of a dynamic scenario generator that enables endless variances of scenarios and ensures a unique training experience each time the CBT is used. This innovative generator will incorporate traditional navigation methods with innovative techniques that allow scenarios to fit into the robust algorithms as they are made.
2. Gamification: Develop software that leverages game-based learning for its innovative training solution. Game-based learning, or gamification, is a novel teaching approach that utilizes certain gaming principles (i.e., badges, points, and leaderboards) and applies them to training practices. Studies show that gamification increases user engagement and keeps trainees in the zone of engaged development – improving skill acquisition and retention, while maintaining an exciting and entertaining game. This shall be accomplished by implementing an engaging, game-like environment with multi-modal, robust training methodology. The gamification approach shall follow extensive research on this topic in commercial gaming.
3. Stress-habituation: Sailor stress elicits physiological and emotional responses that diminish warfighting decision-making performance. Presently, the sailor is trained to read and analyze various electromagnetic warfare (EW) phenomena to make tactical decisions but does not learn how to operate under severe stress. The proposed trainer shall institute modalities that habituate sailor stress during the training cycle to utilize the brain's experience-dependent neuroplasticity. This refers to the brain's capacity to change in response to experience, repeated stimuli, environmental cues, and learning. The training solution will expose the sailor to stressful stimuli such that the brain adapts and becomes more tolerant of and less reactive toward stress, consequently preparing them for warfighting experiences.

The core of this SBIR research effort is to determine how to accelerate learning and improve stress-related responses using psychological methodologies to fulfill the Navy's need for RRL. The results will provide metrics for determining the level of each trainee's improvement during a training session, and these metrics will be logged over time. The pursued innovation will provide each trainee the ability to improve his/her training efficiency and learning retention as well as enhance their actual performance. By addressing the foundational skills at a deep level in which the sailor can act nearly instinctively in their role, the Navy will have expanded capabilities and create an advantage that empowers the fighting force with expertise in their actions and supports fielding a precision team. This is to be accomplished by developing a training solution based on the following parameters:

1. Define and develop a hardware and software architecture trainer concept that would connect to the submarine TI-20 AN/BLQ-10 system,
2. Define metrics for measuring stress and determine how to implement stress factors into the trainer,
3. Develop methods to implement and utilize dynamic scenarios, and
4. Produce a conceptual design of a game-based, dynamic, performance-based trainer and model key components such as TI-20 AN/BLQ-10 interface display, operator performance, stress metrics, and course content.

The innovative training solution shall maximize learning and gaining proficiency through easily accessible learning and training platforms. This trainer would ideally be viewed through various learning platforms, such as the Moodle Learning Management System, the Multifunctional Instructional Trainer (MIT) and/or the Submarine On Board Training (SOBT). Integration onto these platforms will enable the use of multiple, concurrent training sessions and ensure the widespread use of the trainer.

Initial testing of this trainer can be accomplished at the company site, where TI-20 automation and advanced display capabilities shall be applied in a performance-based training environment. This testing will be conducted by the developer with Government representatives. Final testing and certification will occur at the prime system integrator site and will be conducted by Government representatives in collaboration with Naval submarine force active-duty operators.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. Owned and Operated with no Foreign Influence as defined by DOD 5220.22-M, National Industrial Security Program Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence Security Agency (DCSA), formerly the Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances, in order to perform on advanced phases of this contract as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material IAW DoD 5220.22-M during the advance phases of this contract.

PHASE I: Develop a concept for an improved ESM trainer that incorporates dynamic scenarios, gamification, and stress habituation for inclusion as part of the TI-20 AN/BLQ-10 system per the requirements in the Description. Demonstrate the feasibly of the concept to meet the described parameters listed in the Description through modeling, simulation, and analysis. The Phase I Option, if exercised, will include the initial design specifications and capabilities description to build a prototype solution in Phase II.

PHASE II: Using results from Phase I, develop, validate, and deliver the prototype for an improved ESM trainer that establishes modalities to acclimatize sailor stress. The operator interface will emulate and directly interact with the TI-20 AN/BLQ-10 operator machine interface. System performance will be demonstrated through prototype evaluation and modeling or analytical methods over the required range of parameters. Develop and demonstrate a dynamic scenario environment via the generation of multiple scenario variances. Develop and demonstrate an engaging, game-based

training environment that mirrors TI-20 AN/BLQ-10 displays. Develop and demonstrate environmental factors that take advantage of experience-dependent neuroplasticity and habituate stress. Implement and test the dynamic, game-based training prototype. The field test data collection should demonstrate that operators have an improved resilience and reaction to stress-inducing environments as well as demonstrate skill level improvements in comparison to operators that use traditional TI-20 AN/BLQ-10 training methods.

It is probable that the work under this effort will be classified under Phase II (see Description section for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the technology to Navy use in which the final product delivered to the Navy will be an improved ESM trainer that incorporates dynamic scenarios, gamification, and stress habituation to increase operator skill and proficiency in employing the TI-20 AN/BLQ-10 system in a variety of operating environments. This trainer will be incorporated into the TI-20 update to the AN/BLQ-10 system on designated submarines. Work with the associated Integrated Product Team (IPT) and provide hardware and/or software to the system prime contractor for inclusion and integration. The improved ESM trainer performance will be evaluated as part of the overall TI-20 AN/BLQ-10 system testing and evaluation.

Dual use potential exists for any field where operator performance is or could be tracked and developed using CBT. Examples of potential applications include:

1. Operator response to system failures in power generation or manufacturing plants, ensuring systems are placed in a safe condition for subsequent troubleshooting and repair.
2. Operator response to vehicle and/or control system failures in transit systems, such as air traffic control, railway signaling, and subway signaling.
3. Operator response to system failures in commercial shipping vessels.

REFERENCES:

1. Wemm, Stephanie E., and Wulfert, Edelgard. “Effects of Acute Stress on Decision Making.” Applied Psychophysiology and Biofeedback, vol. 42, no. 1, 2017, pp. 1–12., doi:10.1007/s10484-016-9347-8, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5346059/.
2. Porcelli, Anthony J, and Delgado, Mauricio R. “Stress and Decision Making: Effects on Valuation, Learning, and Risk-Taking.” Current Opinion in Behavioral Sciences, vol. 14, 2017, pp. 33–39., doi:10.1016/j.cobeha.2016.11.015,
3. Dicheva, Darina. “Gamification in Education: A Systematic Mapping Study.” Journal of Educational Technology & Society, vol. 18, no. 3, 1 July 2015, pp. 75–88. JSTOR, www.jstor.org/stable/10.2307/jeductechsoci.18.3.75?refreqid=search-gateway:99da2592a1aba73429161d0e017cb0e6.
4. Davidson, Richard J, and Mcewen, Bruce S. “Social Influences on Neuroplasticity: Stress and Interventions to Promote Well-Being.” Nature Neuroscience, vol. 15, no. 5, 2012, pp. 689–695., doi:10.1038/nn.3093.