Combating the unseen threat: How will navies weather the sea change of the digital revolution?

As networked sensors and assets permeate military environments, how will navies respond to exponential technologies and interconnected IoT infused domains? Anika Torruella investigates digital defences in naval cyber warfare

After the 21 August collision of US Navy (USN) Arleigh Burke-class guided-missile destroyer USS John S McCain (DDG 56) with 30,000 gross tonnage Liberian merchant oil tanker Alnic MC east of the Strait of Malacca and Singapore, Chief of US Naval Operations Admiral John Richardson called for a fleet-wide "operational pause" to coincide with further investigation.

The episode marked the fourth incident in the Pacific region with the USN Seventh fleet since January 2017: Ticonderoga-class guided-missile cruiser USS Antietam (CG 54) ran aground 31 January near Yokosuka, Japan, damaging the ship’s propellers and causing a hydraulic fluid leak; Ticonderoga-class guided-missile cruiser USS Lake Champlain (CG 57) collided with 9.8-tonne South Korean fishing vessel Namyang (502) on 9 May about 56 m south of Ulleung Island off the Korean Peninsula; and on 17 June Arleigh burke-class guided-missile destroyer USS Fitzgerald collided with Philippine container ship MV ACX Crystal 56 n miles off the southwest coast of Honshu, Japan, damaging that ship's starboard side and killing seven sailors.

The John S McCain collision resulted in the deaths of 10 sailors, injuries to five others, and significant damage to the ship’s hull that caused flooding to nearby crew berthing, machinery, and communications compartments. The Maritime and Port Authority of Singapore reported the Alnic MC also suffered damage, although without fuel leaks or injury to the crew.

The possibility of cyber intrusion was raised by Adm Richardson in a tweet on 21 August where he said there were "no indications right now ... but [the USN] will review and consider all possibilities".

According to Adm Richardson, the operational pause called for by the USN was to enable the investigation of contributing factors and root causes surrounding the collisions of McCain and
Fitzgerald, as well as provide the USN fleet commanders with an opportunity to assess and review "fundamental practices to safe and effective operations" within their commands.

Adm Richardson also called for a separate review of the Seventh Fleet's maintenance, personnel, and equipment in the Pacific region – led by Admiral Phil Davidson, commander of the US Fleet Forces – that would include the Naval Inspector General's office, Naval Safety Center, and representatives from other services as well as the private sector. The review would scrutinise processes the USN uses to train and certify "forward-deployed forces in Japan" and its surface warfare community including tactical and navigational proficiency.

"This is obviously an extremely serious incident and is the second such incident in a very short period of time – within inside of three months – and very similar as well, and is the last of a series of incidents in the Pacific fleet in particular," Adm Richardson told reporters at the Pentagon.

Adm Richardson reiterated this in an all-hands call with Master Chief Petty Officer of the Navy Steven Giordano, which was streamed live on the USN's Facebook page on 30 August, stating, "There is a bit of a thread of conversation that there might be some kind of cyber attack or cyber intrusion that is involved with these collisions. And I will tell you we have given that an amazing
amount of attention. It is a reality of our current situation that part of any kind of investigation and inspection is going to have to take a look at the computer, the cyber, and the information aspects of our business. We are doing that with these inspections as well," he said.

[Continued in full version...]

Next-generation warships such as the Zumwalt-class (center) and Littoral Combat Ship (left and right) are envisioned to achieve technological advancement and greater operational efficiency from their increase of resident sensors, digital connections, and automated systems. They also have cyber components that could become vulnerable unless defence of the digital databases that drive analytical ability is better understood. (USN)

Cyber attack, capabilities to detect digital foul play, hardening to frustrate threats, and cultivation of warning and deterrence capabilities, is a prodigious global concern. The growth in automated elements, software and artificial intelligence (AI) applications, and networked assets, components, electronics – including sensors and actuators – in maritime environments reflects the growth seen in the Internet of Things (IoT). According to Pew research, the growing connection of devices is inevitable. It noted that US-based research and advisory firm Gartner, Inc. forecasts USD8.4 billion connected ‘things’ will be in use worldwide in 2017 and that number will reach 20.4 billion by 2020.
An information systems technician monitors a network aboard the Arleigh Burke-class guided-missile destroyer USS Carney in the US Sixth Fleet in June. As naval vessels increase integration of advanced information, networking, and automation equipment and technology, especially in command information center, leadership seeks to better understand the cyber vulnerabilities, defence, and security that are disruptive to combat and noncombat operations. (USN/Weston Jones)

Pervasive transference of mission roles and capabilities to the IoT, such as situational awareness; threat identification and targeting; power and energy allocation; maintenance and repair management; environmental monitoring; and harbour, port, and ship inspection not only provides benefits that include lower costs for technological advancement and faster decision making, but also increases cyber vulnerabilities and fundamentally changes the way navies operate.

[Continued in full version...]
A warfare tactics instructor at the Naval Surface and Mine Warfighting Development Center, monitors tactical action officers during a missile exercise aboard the Ticonderoga-class guided-missile cruiser USS Bunker Hill (CG 52) in May. Admiral Bill Mora told US Congress on 7 September that, in some cases, fundamentally basic improvements such as shifting to the most current and updated version of the Windows Operating System provides the USN with essential commercial cyber protection. (USN)

Battlespace spoofing

Possible threats include spoofing ship-based anti-collision systems (AIS): a pre-digital age automatic tracking system used for vessel traffic services, communications, and collision avoidance, which is vulnerable to cyber attack and malicious code.

For instance, in December 2016, Michael Gilmore, director of the US Secretary Of Defense's Operational Test and Evaluation Office (DO&E), said that testing conducted in fiscal year 2014 on Lockheed Martin/Fincantieri-built USS Fort Worth (LCS 3), in 2015 on Austal USA-built Littoral Combat Ship USS Independence (LCS 2), and in 2016 on Austal USA-built USS Coronado (LCS 4) had revealed significant deficiencies in the ships' ability to "protect the security of information and prevent malicious intrusion".

According to Gilmore, the USN made substantial changes to Coronado's networks in early 2016, calling the effort "information assurance remediation", and aimed to correct deficiencies in network security and the ship computing environment on Independence, the baseline Independence-class aluminium trimaran LCS variant.

"The navy designed and implemented the IA [information assurance] remediation programme to mitigate or eliminate some of the vulnerabilities found during the 2015 test aboard LCS 2 and was successful in eliminating some of the deficiencies that placed the ship at risk from cyber attacks conducted by nascent [relatively inexperienced] attackers," Gilmore told Congress. "Unfortunately,
because of numerous limitations, the navy's testing aboard LCS 4 was inadequate to fully assess its survivability against cyber attacks originating outside of the ship's networks, [an outsider threat].

"The testing was adequate to determine that some deficiencies remain when attacks occur from an insider threat; however, it was not adequate to determine the full extent of the ship's cybersecurity vulnerability or the mission effects of realistic cyber attacks."

The USN plans a second phase of information assurance remediation to correct additional network deficiencies, although Gilmore was unaware of the plans to install or test these changes on future ships, or whether these changes will correct the problems observed during the LCS 4 test.

In addition, spoofing GPS and GPS interference at sea impairs or challenges the capability of a ship's sensors to identify proximity threats, such as the 22 June US Department of Transportation's Maritime administration warning of GPS interference, degradations, disruptions, and other incidents or anomalies in the vicinity of position 44-15.7N, 037-32.9E in the Black Sea, near the coast of Novorossiysk, Russia.

Photo of the paper chart showing the actual position (left) and GPS-reported position (right) reported to the US Coast Guard from the master of a commercial vessel during the 22 June black sea GPS-spoofing incident. Although 25 miles off shore in the Black Sea, for several days the ship's GPS receiver showed it to be at an airport several miles inland. The receiver showed its location accuracy to be within 100 m. (Resilient Navigation and Timing Foundation)

According to Dana Goward, president of the Resilient Navigation and Timing (RNT) Foundation, a non-profit, public benefit entity seeking to protect critical infrastructure, the warning was the result of a report made to the US Coast Guard (USCG) Navigation Center and the incident involved more than 20 vessels in the Black Sea. Shipboard equipment was only able to obtain GPS signals intermittently, resulting in location discrepancies of about 25 n miles, while ship GPS self-diagnostics indicated signal anomalies were safe within 100 m.

"This has allowed navigation experts to conclude this was a fairly clear, if not subtle, case of 'spoofing' or sending false signals to cause a receiver to provide false information," Goward said in a blog post on the RNT Foundation website that was also carried with Maritime Executive. "They point to the receiver saying its antenna is [39 m] underwater, that all the GPS satellites it is using have the same high signal strength, and that the WER, or Word Error Rate, is 97% [normal is less than 10%].

[Continued in full version...]

© 2017 IHS. No portion of this report may be reproduced, reused, or otherwise distributed in any form without prior written consent, with the exception of any internal client distribution as may be permitted in the license agreement between client and IHS. Content reproduced or redistributed with IHS permission must display IHS legal notices and attributions of authorship. The information contained herein is from sources considered reliable but its accuracy and completeness are not warranted, nor are the opinions and analyses which are based upon it, and to the extent permitted by law, IHS shall not be liable for any errors or omissions or any loss, damage or expense incurred by reliance on information or any statement contained herein.
Compared to other satellite systems, solar-powered GPSs are relatively fragile and have low signal strength that make the probability of interference or jamming more likely. China, Iran, Russia, and the United States have overt capabilities to control, circumvent, or disrupt sensors and information systems, and inexpensive commercial off-the-shelf (COTS) technology enables less capable nation states and asymmetric adversaries, with little to no conventional means of warfare, to equally acquire capabilities to control, spoof, circumvent, or disrupt information systems and wage offensive campaigns against well-established powers or release highly co-ordinated specialised attacks intended for one-time use against a specific target. The cost of such capabilities "start at around [USD50] and increase with the size of the desired impact area", Goward also noted.

Spoofing unmanned systems has long been a threat. In 2010 Hezbollah claimed it had intercepted a video from an Israeli unmanned aerial vehicle (UAV) that provided intelligence for a 1997 ambush in southern Lebanon. In December 2009 an unsecured downlink from a US military UAV was intercepted by Iraqi insurgents using file-sharing software developed to intercept satellite television feeds, and in December 2011 and December 2012, Iran claimed to have hacked the GPS signal of a US Lockheed Martin RQ-170 Sentinel and a Boeing ScanEagle long-endurance UAV respectively. While improvements have been made to UAV waveforms, hackers and hacking software are also constantly improving spoofing devices and software as indicated by more recent reports by the Federal Trade Commission hacking Parrot's AR Drone Elite Quadcopter, DBPower's Hawkeye II 2nd FPV Motion Sensing Quadcopter, and Cheerson's oneCase CX-10w. A warning was also issued by the US Army in August 2017 regarding the use of China's DJI UAVs due to cyber vulnerabilities. DJI UAVs are also in use by the Israel Defense Forces (IDF).

In addition, cyber threats do not need to take control of platforms to be effective in disturbing the operational ecosystem. 'Logic bombs' can be uploaded to aircraft during maintenance, repair, or flight preparations through datalinks that can be timed to create false fire alarms, trigger or delay electronic warfare (EW) early warning systems, create radar anomalies, or affect other pieces of the aviation infrastructure to confuse or distract pilots or UAV operators during mission operations.
Digital tandem

As the digital evolution of technology significantly alters naval warfare, these changes are also bringing about specific technologies that can make a substantial difference to achieving or maintaining maritime superiority. Within this new maritime landscape, technologically advanced conventional warfare must operate in tandem with cyber warfare, often as a precursor to kinetic hostilities.

The RNT Foundation noted the US Director of National Intelligence Daniel Coats’s statements to the Senate Select Committee on Intelligence that "Russia, China, Iran, and North Korea are expected to continue their efforts to disrupt GPS signals along with other space assets".

On 14 May the RNT Foundation stated that the best way to protect assets in space, such as GPS, is to "reduce their desirability as targets". Important space-based assets needed to have complementary non-space-based capabilities on the ground, such as "reconnaissance aircraft paired with imaging satellites, terrestrial radio systems paired with communications satellites, and eLoran paired with GPS". Enhanced long-range navigation, or eLoran, for instance, operate in between 90 kHz to 110 kHz to provide position, navigation, and timing (PNT) and are based on the internationally standardised, hyperbolic navigation system, Loran-C, which was terminated in 2010 by the USCG following operational reliance on GPS.

Coats also noted that counterspace weapons are a global trend and that EW attacks against space systems will likely increase in number and types of weapons. "Development will very likely focus on jamming capabilities against dedicated military satellite communications (SATCOM), synthetic aperture radar (SAR) imaging satellites, and enhanced capabilities against global navigation satellite systems (GNSS), such as the US GPS.

"Blending of EW and cyber-attack capabilities will likely expand in pursuit of sophisticated means to deny and degrade information networks. Chinese researchers have discussed methods to enhance robust jamming capabilities with new systems to jam commonly used frequencies. Russia intends to modernise its EW forces and field a new generation of EW weapons by 2020. Iran and North Korea are also enhancing their abilities to disrupt military communications and navigation," he stated.

Digital twins

NATO began studying military applications of IoT in January 2016, including command and control (C2) of combined operations logistics support; tactical-level situational awareness; medical care and battlefield health monitoring; security, identity, trust management, and service architecture in the military IoT domains; and technologies required to exploit IoT, such as data fusion, big data, or other techniques.

Digital replicas and simultaneous modelling can help mitigate the threat of cyber attack-based intrusion, denial, interruption, manipulation, or control through early warning, continuous prediction, and dynamic optimisation.

According to Dr Colin Parris, vice-president of GE Software research, creating a digital replica or ‘twin’ of an asset provides early warning of malfunctioning or irregularities, continuous prediction of...
future maintenance or performance capabilities, and dynamic optimisation to balance changing operational needs.

The digital twin is a virtual model based on a physical model, such as a sensor or actuator. Actual digital data is provided by the physical model so the virtual model is adaptable: the virtual sensors combined with physical sensors give a large amount of additional data that enables machine learning to determine new capabilities.

For instance, the digital twin can calculate the corrosion of an unmanned underwater system (UUS) or level of cumulative damage over time based on weather conditions and salinity data, number of times deployed, and service mission roles. By understanding the physics and environment the UUS has been operating in, the digital twin can recommend component replacement, order logistic spares, or dynamically predict service life changes without having to retrieve the asset for inspection or maintenance.

Such prediction and digital modelling has the potential to increase service life by reducing repairs and maintenance that stem from operationally heavy workloads. Ship maintenance has recently been problematic for the USN, according to a November 2016 Government Accountability Office (GAO) report that stated, "The navy concluded in 2010 that the material readiness of the surface ship force was well below acceptable levels to preserve ships to their full service lives, finding that deferrals of scheduled maintenance and reductions in the amount of time allowed for completing major repairs contributed to persisting deficiencies. These deferrals and reductions also had not remedied the longstanding problem of cost and schedule growth in ship maintenance availabilities."

In 2015 the USN transitioned to a different contract strategy for the maintenance and modernisation of surface ships aimed to improve the readiness of its non-nuclear surface combatant and amphibious warfare ships. The Optimized Fleet Response Plan (OFRP) introduces a revised operational schedule intended to provide a predictable scheduling of tasks for ship maintenance and alleviate cost and schedule growth incurred during availabilities.

As a result of its machine-learning capabilities, the digital twin can receive actual data from each physical asset, such as when human operators make corrections due to errors, automated systems make adjustments to counteract cyber attacks, or when virtual modelling and tests have been run in a research environment. The digital twin is enabled to learn which approaches are the most successful and then update the entire networked or cloud-based system of fleet-wide sensors, so the data is not only sourced from a fleet of physical assets, but each individual asset in the fleet also benefits.

In addition, since the digital twin receives actual real-time information and can learn from its physical twins, it can be controlled or manipulated in place of the physical assets at a distance to increase or adjust performance, or it can be used to replace information that a faulty or compromised asset is providing to the rest of a networked system.

[Continued in full version…]
This analysis is taken from Jane’s Defence Industry & Markets Intelligence Centre, which provides world-leading analysis of commercial, industrial and technological defence developments, budget and programme forecasts, and insight into new and emerging defence markets around the world.

Jane’s defence industry and markets news and analysis is also available within Jane’s Navy International. To learn more and to subscribe to Jane’s Navy International online, offline or print visit http://magazines.ihs.com/

For advertising solutions visit Jane’s Advertising