Cyber attacks as big a threat to warships as missiles and torpedoes, Navies developing cyber security measures and technologies

US Navy considers that it faces threats from adversary nations like Russia, China, Iran, and North Korea, which have developed significant information warfare capabilities and interested in exploiting the Navy's networks to conduct espionage operations, either by stealing information and technical data on fleet operations or preventing the Navy from taking advantage.

One of the threat is spoofing and jamming attacks on the position, navigation, and timing (PNT) systems, that are dependent on Global Positioning System (GPS) satellite constellation. GPS spoofing attempts to manipulate a GPS receiver by broadcasting counterfeit signals remains the most likely attack method it due to its simplicity. This form of attack involves overpowering the receiver by broadcasting signals that are synchronized with the legitimate signals detected by it, thereby forcing GPS to provide false information.

In July, 2017 the US Maritime Administration reported an incident in which at least 20 Russian ships appeared on trackers to be in the same spot 20 miles (32 kilometres) inland, despite being at various positions in the Black Sea. While this initially appeared to be a glitch, experts now

suggest that Russia may have been testing a new system for spoofing GPS.

Researchers suspect that Iran used same methods to two United States riverine patrol boats in January 2016 when they unknowingly sailed into Iranian waters and were accused of violating Iran’s territorial integrity. As the Iran’s cyber warfare capabilities are increasing and its relations with US are deteriorating there is increasing threat of Iran using Cyber Warfare against US Navy.

North Korea, a close military partner of Iran, has reportedly used GPS jamming to disrupt air and naval traffic within the demilitarized zone as reported by Ian W. Gray in The Diplomat. The South Korean counter-espionage agency which launched a probe into an alleged hacking attack on a naval warship building firm last month says it believes North Korea may be behind the hack. On 20 April, Hanjin Heavy Industries & Construction Co, the largest naval shipbuilders in South Korea, was hit by a cyber-attack leaving possible classified files exposed.

Cyber warfare has moved to maritime domain. “The risk of cyber attacks against our ships and submarines is as real a threat as traditional weapons such as rockets, missiles and torpedoes,” Royal Navy says. Navies around the world are now developing new cyber security measures and technologies and carrying out exercises to test the operational effectiveness of warships, submarines and Marines in responding to cyber incidents that may unfold during a real-life crisis.

IMO has issued MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management. The guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management.

Cyber Threats in Maritime domain

In 2016, the Baltic and International Maritime Council (BIMCO) in their "Guidelines on Cyber Security Onboard Ships," warned about the vulnerability of Merchant ships from cyber attacks due to their increased networking and automation systems onboard. Navies are moving to network centric systems in which all the sensors weapons and command and control on ships, aircraft, submarines, and unmanned vehicles are 'networked' , which also enhances vulnerability.

Cruise ships could be sunk by cyber terrorists, official Government guidance has warned in a drive to improve protections from online attacks. Vessels could be vulnerable to "kidnap, piracy, fraud [and] theft of cargo" if their computer systems are compromised, the Transport Department said. At worse a cyber-hack could result in "risk to life and/or the loss of the ship", the industry was also told.

The concern is that hackers could distort mapping equipment or the ship's controls, causing it to hit another vessel or run aground. The dire warnings were made in a "Cyber Security for Ships" code of practice, written by the Institution of Engineering and Technology and distributed by Whitehall.

Overall, the Navy faces the same technological challenges confronting the rest of the Defense Department and even the world at large, declares Vice Adm. Mike Gilday, USN, commander, U.S. Fleet Cyber Command/U.S. 10th Fleet. One of the Navy's top concerns is that an adversary would deny the fleet its cyber capabilities in a conflict. The service is working to enable its forces to operate in this kind of denied environment, but Adm. Gilday emphasizes that this does not represent an abandonment of cyber as a key warfighting tool. "Cyber is absolutely a key enabler, particularly early in a fight when we want to increase the fog and friction of war and place ourselves in a position of advantage against an adversary," he declares. "Cyber is absolutely, positively part of how we have to fight in the future—and how we have to shape that environment right from the onset."

Post Snowden/NSA disclosure another serious type of threat that has potential to cause irreparable harm to the Navy's interests is the insider threat. Presidential Executive Order 13587, signed in 2011 to improve federal classified network security, further defines an insider threat as "a person with authorized access who uses that access to harm national security."

Mr Searle said cyber attack "is a real threat, certainly, it's something we take very seriously, particularly areas of the combat system, communications systems, power and propulsion control systems. "We put a lot of effort into ensuring the security of those systems from software, from a communications point of view." The Armed Forces must be able to defend themselves against cyber attacks to ensure their operational capability and also be prepared to carry out cyber attacks

themselves to gain an operational advantage.

Cybersecurity Policy

Navy Secretary Ray Mabus has called for the implementation of a layered approach to cyber defense and the establishment of a department wide program to tackle insider threats. Navy organizations, including the Marine Corps, “shall implement a defense-in-depth/defense-in-breadth [cybersecurity] strategy to mitigate information security risks throughout the entire life cycle of a system or network,” the memo states.

“The [Department of the Navy] shall establish an integrated set of policies and procedures to deter, detect and mitigate insider threats before damage is done to national security, personnel, resources and/or capabilities,” the memo states. The memo also updates acquisition strategy by calling on officials to make sure cybersecurity is considered at every phase of a system’s development and implementation. The memo also rebrands the DON Information Assurance Program as the DON Cybersecurity Program.

IMO Cyber Risk Management

Maritime cyber risk refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

Cyber risk management means the process of identifying, analysing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders. The overall goal is to support safe and secure shipping, which is operationally resilient to cyber risks.

These Guidelines present the functional elements that support effective cyber risk management.

.1 Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

.2 Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
.3 Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.
.4 Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
.5 Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

Cybersecurity Measures

The Royal Navy is running its first ever large-scale cyber war games, to protect warships and submarines from cyber attacks. Dubbed Information Warrior 17, the training exercise is designed to ensure the Navy is prepared for the challenges that a new era of warfare could pose, as project director

Colonel Dan Cheesman of the Royal Marines explained. Thousands of members of the navy, air force and army will take part in Information Warrior 17, as part of an even bigger Nato training exercise, Joint Warrior, in Scotland. During the exercise, the navy will use artificial intelligence to set up a “ship’s mind”, which will allow warships and submarines to make decisions automatically.

The new Type-26 Global Combat Ship, which is designed to be the workhorse of the Royal Navy when it is built, has been designed to protect its weapons, engines and systems from cyber warfare as reported by Ben Farmer, Defence Correspondent. Geoff Searle, head of the Type-26 programme at BAE Systems, said: “It is an equally important threat to the more traditional threats and one that we take very seriously and design the ship to be confident it can withstand that.”

Automation, a tool for attackers, is key to Navy cyber defense. Adm. Gilday says it is required for protection that goes beyond boundary and point defenses. He calls for greatly increased investment in artificial intelligence and cognitive computing. Artificial intelligence should be leveraged to provide a greater understanding of activities deep inside Navy networks. “We need to move beyond touch labor, in terms of being able to respond rapidly to a threat,” the admiral declares. “We have great detection systems that alert us to known or suspected bads, but the challenge is to be able to quickly identify and respond to an intruder deep inside your networks.”

US Navy Diversifies Ships' Cyber Systems to Foil Hackers

The Defense Department has said that warships are are broadly vulnerable to cyberattacks. The problem led the Navy to create the RHIMES system, a new effort to protect the electrical and mechanical systems of warships

U.S. Navy has developed a Resilient Hull, Mechanical, and Electrical Security (RHIMES) defense system to protect its ships against hackers who threaten to disable or take control of critical shipboard systems. Dr. Ryan Craven, a program officer of the Cyber Security and Complex Software Systems Program in the Mathematics Computer and Information Sciences Division of the Office of Naval Research, explained that RHIMES is designed to prevent an attacker from disabling or taking control of programmable logic controllers—the hardware components that interface with physical systems on the ship.

"Some examples of the types of shipboard systems that RHIMES is looking to protect include damage control and firefighting, anchoring, climate control, electric power, hydraulics, steering and engine control," explained Craven. "It essentially touches all parts of the ship." The loss of one or more such systems could prove especially devastating in the middle of a naval operation or battle; especially if hackers turn the ship's systems against itself.

Traditionally, computer security systems protect against previously identified malicious code. When new threats appear, security firms have to update their databases and issue new signatures. Because security companies react to the appearance

of new threats, they are always one step behind. Plus, a hacker can make small changes to their virus to avoid being detected by a signature.

“Instead, RHIMES relies on advanced cyber resiliency techniques to introduce diversity and stop entire classes of attacks at once,” Craven said. Most physical controllers have redundant backups in place that have the same core programming, he explained. These backups allow the system to remain operational in the event of a controller failure. But without diversity in their programming, if one gets hacked, they all get hacked.

“Functionally, all of the controllers do the same thing, but RHIMES introduces diversity via a slightly different implementation for each controller’s program,” Craven explained. “In the event of a cyber attack, RHIMES makes it so that a different hack is required to exploit each controller. The same exact exploit can’t be used against more than one controller.”

“The purpose of RHIMES is to enable us to fight through a cyber attack,” said Chief of Naval Research Rear Adm. Mat Winter. “This technology will help the Navy protect its shipboard physical systems, but it may also have important applications to protecting our nation’s physical infrastructure.” “Vulnerabilities exist wherever computing intersects with the physical world, such as in factories, cars and aircraft,” Craven said, “and these vulnerabilities could potentially benefit from the same techniques for cyber resilience.”

Navy awards deals potentially worth $1B for cybersecurity

US DOD will give Northrop Grumman San Diego at least $88 million to develop and test better computer systems for Navy warfighters, including the kind of software that detects and fights cyberattacks. The work will be performed over the next three years on behalf of the Space and Naval Warfare Systems Command (SPAWAR) in San Diego, which covers everything from the control systems on warships to the intelligence and surveillance equipment on unmanned aerial vehicles (UAVs). Us Navy is regularly hit by hackers, including “state sponsored” adversaries in China, Russia and North Korea.

The Navy has awarded seven companies contracts totaling at least $609 million for cyberspace science, research, engineering, and technology integration. Each of the contracts, awarded separately, is for three years and each has a two year option. If all options are exercised, the total value of the deals would exceed $1 billion.

The seven companies, chosen from among 13 that had submitted bids, will provide services including technology assessment, development and transition; requirements analysis; systems engineering; operational and technical support; experimentation support; hardware and software development and prototyping; modeling and simulation; training; and security engineering/cybersecurity, according to the contract announcements.

The companies awarded contracts, along with the base value and maximum five-year value of the contracts are:

Raytheon, $98 million, $165.9 million
Leidos, $89 million, $149.9 million
Booz Allen Hamilton, $88.6 million, $149.8 million
Northrop Grumman Systems, $88 million, $148.3 million
SAIC, $84.6 million, $142.2 million
Scientific Research, $81 million, $137.5 million
Vencore, $80 million, $134.9

At the beginning of the year, the Space and Naval Warfare Systems Command issued its 2016 strategic plan, which described cyber as “the all-encompassing domain of or related to computing,” and said its “vision is to rapidly deliver cyber warfighting capability from seabed to space.”

References and resources also include:

https://www.onr.navy.mil/en/Media-Center/Press-Releases/2015/RHIMES-Cyber-Attack-Protection.aspx

http://thediplomat.com/2016/05/cyber-threats-to-navy-and-merchant-shipping-in-the-persian-gulf/

http://www.reuters.com/article/us-iran-navy-wargames-idUSKBN165094

http://www.telegraph.co.uk/news/uknews/defence/11786558/Cyber-attacks-as-big-a-threat-to-new-warships-as-missiles-and-torpedoes.html

http://www.sandiegouniontribune.com/news/sd-me-northrop-cybersecurity-20160918-story.html

http://www.afcea.org/content/?q=navy-seeks-technologies-cyber-fight

http://maritime-executive.com/editorials/the-cyber-vulnerabili

ty-of-the-us-navy

https://defensesystems.com/articles/2016/09/16/navy-cyber-contracts-seven-companies.aspx

https://fcw.com/articles/2016/05/20/navy-retools-cyber.aspx

http://www.telegraph.co.uk/news/2017/09/16/cyber-attack-could-sink-cruise-ships-government-advice-warns/

http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/cyber-security.aspx