# *Curtis Wilbur* takes part in ROK bilateral exercise Foal Eagle

**Story and photo by Ensign Tyler Kranz, *USS Curtis Wilbur* Public Affairs**

The annual Republic of Korea (ROK) bilateral exercise Foal Eagle concluded for *USS Curtis Wilbur* (DDG 54) and the ROK 3rd Fleet in Buson harbor March 20 after a rigorous four day exercise.

After a day of rough seas, the exercise began with a small boat transfer over to the ROK flag ship, *Yang Manchun* (DDH 973), where several ROK 3rd Fleet representatives awaited key personnel from *Curtis Wilbur* for a conference to discuss the coordination of the exercise between the two nations.

Safety was the primary concern throughout the conference for both navies as well as effective communication with the rest of the fleet. Two liaison officers from the ROK navy were embarked aboard *Curtis Wilbur* and proved to be great assets to the "Steel Hammer" by improving the coordination of any issues with the ROK 3rd Fleet.

*Curtis Wilbur*, the only U.S. ship attached to the ROK 3rd Fleet, played a key role in making every evolution count towards effective training and cooperation between the various ROK fleets. The combined fleet conducted several detailed exercises including anti-submarine warfare which encompassed searching and tracking Korean diesel submarines on the East China Sea.

"The many anti-submarine warfare evolutions went well," said anti-submarine assessor and *Curtis Wilbur* Weapons Department Chief Sonar Technician Surface Orlanda Lilly. "The long hours and training paid off for everyone that took part in the evolution. You really have to know what you are doing to catch the South Korean diesels."

During seamanship training, the ship turned off its surface search radars, eliminating the surface picture for the bridge team. This reinforced the bridge team to work together and use equipment such as an optical rangefinder (stadimeter) to find ranges to the other ships in the formation. Navigational charting tools such as moboards and the peloris were used extensively during the evolution making the bridge team much more skilled in the use of both.

"It was a great evolution because it taught the junior Sailors to use the charts and report bearings to the chain of command instead of relying on computers," said *Curtis Wilbur* Weapons Department Quarter Master 1st Class Jason Lloyd. "The officers also put in some great training, completely relying on visual fixes and moboards to stay in sector for the formations."

**(Right) *USS Curtis Wilbur* (DDG54) Commanding Officer Cmdr. Paul H. Hogue exchanges gifts with the commanding officer of the South Korean destroyer Yang Manchun (DDH 973) after the successful completion of the bilateral exercise Foal Eagle March 20.**

Foal Eagle directly contributes to the partnership the U.S. Navy has with South Korea and the bilateral exercise has once again improved the relationship and cooperation between the United States and the ROK.

# Department of Defense policy requires digital signatures on e-mails

**By MC2(SW) Christopher Koons,**
**Naval Network Warfare Command Public Affairs**

The Department of Defense (DoD) has implemented a policy requiring employees to digitally sign all e-mails containing a link or an attachment.

A digital signature is also required for any e-mail that provides direction or tasking, requests or responds to requests for resources, promulgates organization position, discusses any operational matter, discusses contract or finance matters or discusses personnel management matters. The need exists to ensure that the originator is the actual author and that the e-mail was not tampered with in transit.

The policy, which was updated for the Navy in September 2008, applies to all unclassified e-mail sent from a DoD-owned, operated or controlled system or account to include desktops, laptops and personal electronic devices such as a BlackBerry.

"It ensures that the information from links and attachments comes from a trustworthy source," said Lt. Cmdr. Damen Hofheinz, U.S. Fleet Forces deputy for Information Assurance. "If an e-mail contains a link, you need to know that it leads you to a valid Web site."

A digital signature is a "stamp" on an e-mail, which is unique to the user and provides an accurate means of identifying the originator of a message. Its toolbar icon is an envelope with a red seal on top. A digital signature assures the recipient that the original content of the message or document is unchanged. It also provides the sender with proof of delivery and the recipient with proof of the sender's identity and reassurance that the e-mail's originator is its actual author.

Some e-mails require added protection in the form of the encryption key, which, like the digital signature key, has an envelope icon but has a blue lock rather than red seal on it. Navy policy requires encryption of all e-mails that contain privacy act information, health insurance portability and accountability act information, contract information, classified as 'for official use only' (FOUO) or that may serve as an operational security (OPSEC) indicator.

"If you send an e-mail which contains personally identifiable information (PII) such as your social security number or if the message is for official use only, you need to encrypt as well as digitally sign it," Hofheinz said. "Encryption provides an extra level of protection."

Encrypting e-mail is made much easier when personnel publish their certificates to the global address list (GAL). This can be accomplished in Outlook by opening the "Tools" menu then selecting "Options." On the "Security" tab there is a "Publish to GAL" button. Clicking on this button will ensure that other users on the network can send encrypted e-mail back to the originator.

Outside the continental United States, Navy Enterprise Network (ONE-NET) has already implemented a network policy for all e-mails to be digitally signed and Navy-Marine Corp Internet (NMCI) started implementation Feb. 12. Users will have to deselect the digitally signed button in Outlook to send unsigned e-mails. "It is one part of our overall public key infrastructure (PKI) implementation, which is designed to prevent bad guys from accessing information we send over the Internet," said Hofheinz.