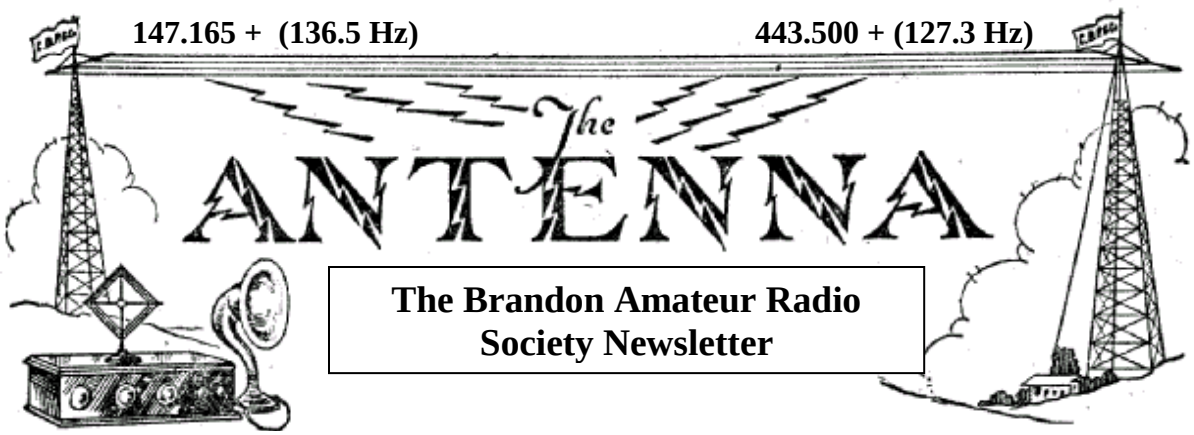
147.165 + (136.5 Hz) 443.500 + (127.3 Hz)



The Brandon Amateur Radio Society Newsletter

OVER 39 YEARS OF PUBLIC SERVICE TO THE BRANDON AREA
BRANDON, FLORIDA, USA
VOL XLIII, NUMBER 3 MARCH 2016

Come to the Club Meeting March 17th

Our meeting this month is at our usual location: Brandon Assembly of God 710 South Kings Avenue in the Annex. Things get underway at 7:30 p.m. when Doris WB9VDT bangs the gavel to start things off.

-30-

March Program

Barbara Jones, a Community Service Officer with the Hillsborough Sheriff's Department, will come to this month's BARS meeting to bring us up to date on cyber crime, identity theft, and a number of other nefarious ways the "bad guys" use to separate us from our money.

-30-

Saturday 5 March Testing Session

We had four test candidates at our March testing session The results were:
One new Technician licensee, one upgrade from Tech to General, one upgrade from General to Extra, and one who came in with no license and walked out with an Extra!
Examinations are given on the first Saturday of the month in the church annex at Brandon Assembly of God 710 South Kings Avenue in Brandon (the same location where we have our meetings).

-30

Kudos to Ron Perrett K4FZU!

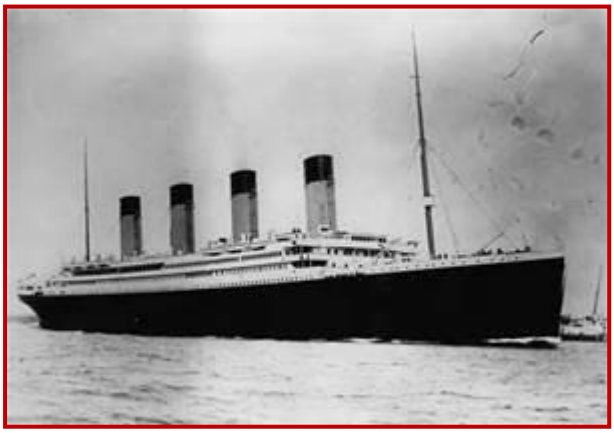
On March 1st at a commercial examination session in Brandon, Ron added another achievement to an already impressive list of attainments in radio/electronics by passing the examination for the Radiotelegraph Operator

License. We hope that Ron will soon be pounding the brass on the commercial maritime frequencies from station KKUI aboard the S.S. American Victory. Here in Brandon we can offer something that many other clubs cannot: we can also set up commercial examination sessions. These are **General Radio Telephone Operator License (GROL), Radiotelegraph Operator License, Marine Radio Operator License, GMDSS Radio Operator License, GMDSS Radio Maintainer's License, and the Ship RADAR Endorsement**.
For more information on the commercial radio exams contact Mike Fletcher NI4M or Mark Haskell WB9UJS.

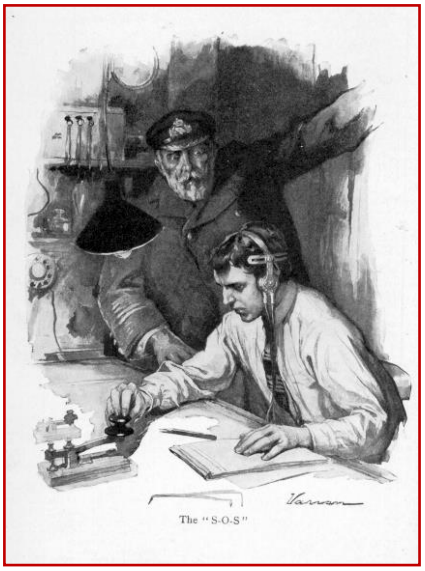
Hackers Create Danger on the High Seas
Radio Rescue System Compromised

For centuries man has traveled to all parts of the globe on the seas and oceans. Waterways were the easiest (and for centuries) the fastest means of transporting goods from one point to another.
As technology progressed sea travel became safer and more reliable. The development of the Astrolabe and later the sextant made navigation more precise and at the close of the 19th century the development of radio began to make ship travel safer because in case of accidents or sinking, help could be summoned by radio.

Radio was in general use by 1912, the year of the sinking of the RMS *Titanic*, but it was not required to be used on ships at sea. That changed after the *Titanic* disaster: ships were required to carry radio equipment and the radio operator was an officer on the ship's crew. In those days the means of communication was Morse code sent by means of a spark gap transmitter. Much of the communication was done on the Medium Frequency (MF) bands. Even today MF is still used for some Maritime Safety Information (MSI).

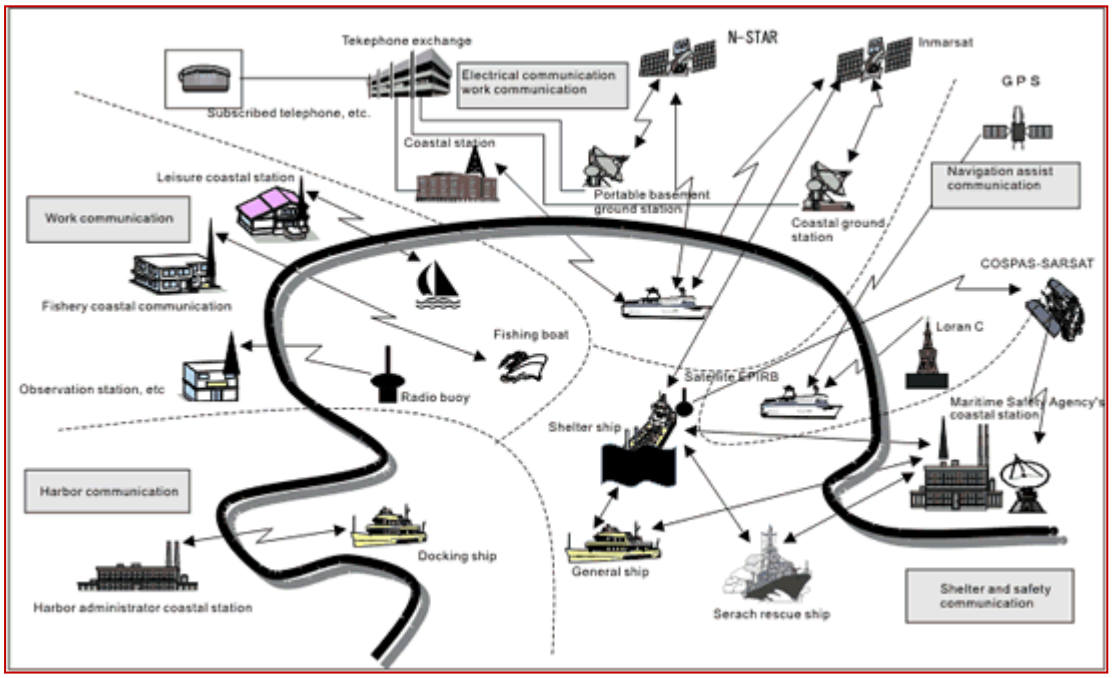


With the development of the vacuum tube Continuous Wave (CW) replaced the inefficient spark signals and radio transmitters and receivers developed greater range and reliability.



The communication system was simple, dependable, and labor intensive. It required an army of individuals on board ships and at coastal stations who were proficient in high speed (20-30 wpm) Morse code operations and who had a solid understanding of radio communication, especially HF and MF radio wave propagation. This knowledge and skill could not be developed in a radio school course. It was learned through experience in working aboard ships or at coastal stations handling radio traffic in all kinds of conditions. (Think back to one of the purposes of the Amateur Radio Service: to develop a pool of trained radio operators.)

Ships communicated with other ships and coastal stations. Communications ranged from company business: schedules, cargo, port charges, and supplies, to passenger communications, medical emergencies, or the worst case scenarios of disasters at sea and calls for rescue. In the latter part of the 20th century some people felt there was a need to change the system: make it faster, more automated, less labor intensive, and not so dependent on the skills of the Radio Operator. That's one less salary for the company to pay. A new system was developed to take advantage of advances in late 20th century communications technology: digital selective calling (DSC), satellite communications (COSPAS-SARSAT, EPIRBs), and forward error correcting systems (SITOR). It would allow authorities on shore to take control of a disaster situation at sea and it would be a system that any crewman could be trained to operate in a short period of time. The result of this endeavor was the **Global Maritime Distress and Safety System** (GMDSS). By the end of the 20th century it had replaced "Sparks", the Radio Officer on the crew. No more Morse code at sea. It was the end of the huge mega-watt coastal CW stations receiving and transmitting radio messages all over the world. It was the end of a system that had proven its simplicity and dependability for almost a hundred years.



Here is an overview of the GMDSS system in its broadest application. Note that the INMARSAT system plays a key role in linking ships at sea to coastal stations and other ships.

Is GMDSS the greatest thing since sliced bread? The system has gotten mixed reviews. When everything works it is fantastic. However, if parts of the system fail, serious problems can develop. It's like Christmas tree lights wired in series. Now most of the ship's officers and several of the crewmen are required to hold the GMDSS Operator License (DO). Reports from system maintainers and others say that generally the crew (who are not experienced in radio) do not use DSC on SITOR or HF SSB because they simply do not understand HF radio wave propagation. For example they may not understand why it's possible to communicate thousands of miles on 22 MHz during the daytime, but not at night. As a result, they depend mostly on the INMARSAT (International Maritime Satellite) system for communications. The problem is these satellites are easy to hack and that is exactly what has happened.
Kaspersky Lab, a Russian company specializing in technologies and computer security services, has revealed the existence of a real commercial network, based in Brazil, which since 2005 has distributed a malware

("toolkit") clandestinely in order to conduct cyber-attack campaigns and industrial espionage against companies. The Poseidon malware is able to access diverse communication channels, including satellites used for navigation support at sea. Unfortunately, the vulnerability of satellite links for infrastructure such as Iridium or Inmarsat have long been known. In 2014, the IOActive company had distributed a detailed whitepaper explaining the weaknesses of satellite communications (SATCOM). In the case of maritime services on the high seas, the risks are real, and have the potential to be seriously damaging. Cyber attacks against ships are not limited to the communication channels but also navigation devices and emergency communication systems. The malware infiltrates Rescue Coordination Centers (RCC) centers and other key links. Kaspersky provides some explanation about the attacks for "hijacking" of the satellite link.

During a particular campaign, conventional Poseidon samples were directed to IPs resolving to satellite uplinks. The networks being targeted were designed for internet communications with ships at sea which span coverage areas on a global scale, while providing almost no security for their downlinks.

Kaspersky Lab experts revealed that the hackers are doing this using a trick known as satlink hijacking – a technique this group has been using since 2007. It involves exploiting the vulnerability of asynchronous satellite internet connections to sniff traffic, distilling the IP addresses of satellite subscribers. All the attackers need then is to set up their servers with the same IPs, configure these addresses into their malware and, after a successful infection, wait for its call to a coastal station or a Rescue Coordination Center (RCC).

What happens next: the satellite broadcasts the request from an infected machine over the whole area of its coverage. Of course, both attackers and law-abiding subscribers receive this request. But, unlike the attackers' servers, subscriber systems are extremely unlikely to host any services on particular ports – and this traffic is simply dropped without acknowledgement, as this would increase the burden on the thin cellular upstream channel used in such asynchronous data links. After receiving the malware call, the RCC answers via regular fast landline and gets a spoofed acknowledgement, which appears to be coming from the same hapless satellite

link subscriber. The result is the ship in distress thinks their request for assistance has been answered, (it has not) or the RCC thinks they have sent a response and gotten a confirmation (that has not happened, either). The bottom line is that if a system in a given area is attacked those unfortunate folks in the water may think that their distress message has gone out and help is on the way, but the reality is nobody is coming because none of the rescue centers got the message. Nearby ships are not being directed to the site of the disaster because there is no record of the distress signal, and nobody gets rescued.

In the early days of the GMDSS implementation there were recorded instances where the satellite communication terminal failed, but the Morse code call for assistance on 500 KHz received responses from multiple ships and coastal stations resulting in no loss of life: all passengers and crew being rescued.

As Amateur Radio operators, we often have a similar experience in times of weather emergencies or disasters. The first things to fail are the multi-faceted high capacity communication links that most people take for granted. Sending pictures, data, voice, and text all over the world seems like a normal state of affairs. Most people are not aware of the requirement for the efforts of thousands of technicians to maintain networks, servers, and nodes so they can send pictures of the kids to grandma, or comments about their latest weekend trip on social media. It's all great until the system goes down. When that happens that super smart phone becomes a paperweight (and a fragile one at that). Sophisticated communications are great and they have become the norm for most people, but to operate with no dependable backup system whether on land or at sea is more than simply naïve, it is dangerous.

-30-

That wraps it up for this month. Have FUN with radio!

Keep in Mind Our Weekly Nets and Bulletins

Monday 8 p.m. The Two Meter Net 147.765 - 147.165 MHz Hosted by Doris Haskell WB9VDT

Tuesday 7 p.m. 6-meter Roundtable 50.200 MHz USB followed at 8 p.m. with the 10 Meter Roundtable 28.365 MHz USB

Send us your articles AND PICTURES! We do much more in the digital format! I would like to have pictures of BARS members and their ham shacks!

Remember to check out the BARS website:

brandonhamradio.org