**[](https://rntfnd.org/)**

[Home](https://rntfnd.org/) » » [Blog](https://rntfnd.org/blog) » Mass GPS Spoofing Attack in the Black Sea? – Maritime Executive

July 12, 2017

******

***Blog Editor’s Note: The MarEx editors added the question mark in the title. See photos at the end of the text.***

[**Maritime Executive Article Here**](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea)

By [**Dana Goward**](http://www.maritime-executive.com/author/dana-goward) 2017-07-11 20:22:39

An apparent mass and blatant, GPS spoofing attack involving over 20 vessels in the Black Sea last month has navigation experts and maritime executives scratching their heads.

The event first came to public notice via a relatively innocuous [**safety alert**](https://www.marad.dot.gov/msci/alert/2017/2017-005a-gps-interference-black-sea/) from the U.S. Maritime Administration:

*A maritime incident has been reported in the Black Sea in the vicinity of position 44-15.7N, 037-32.9E on June 22, 2017 at 0710 GMT. This incident has not been confirmed. The nature of the incident is reported as GPS interference. Exercise caution when transiting this area.*

But the backstory is way more interesting and disturbing. On June 22 a vessel reported to the U.S. Coast Guard Navigation Center:

*GPS equipment unable to obtain GPS signal intermittently since nearing coast of Novorossiysk, Russia. Now displays HDOP 0.8 accuracy within 100m, but given location is actually 25 nautical miles off; GPS display…*

After confirming that there were no anomalies with GPS signals, space weather or tests on-going, the Coast Guard advised the master that GPS accuracy in his area should be three meters and advised him to check his software updates.

The master replied:

*Thank you for your below answer, nevertheless I confirm my GPS equipment is fine.*

*We run self test few times and all is working good.*

*I confirm all ships in the area (more than 20 ships) have the same problem.*

*I personally contacted three of them via VHF, they confirmed the same.*

*Sometimes, position is correct, sometimes is not.*

*GPS sometimes looses position or displays inaccurate position (high HDOP).*

*For few days, GPS gave a position inland (near Gelendyhik aiport) but vessel was actually drifting more than 25 NM from it.*

*Important: at that time, GPS system considered the position as “Safe within 100m”.*

*See attached.*

*Then last night, position was correct despite several “lost GPS fixing position” alarm that raised couples seconds only; then signal was back to normal.*

*Now position is totally wrong again.*

*See attached pictures that I took on 24 June at 05h45 UTC (30 min ago).*

*Note: you can also check websites like MarineTraffic and you will probably notice that once in a while all ships in the area are shifting inland next to each other.*

*I hope this can help.*

To back up his report, the master sent photos of his navigation displays, a paper chart showing his actual position and GPS-reported position, and his radar display that showed numerous AIS contacts without corresponding radar returns (below).

One of the photos was of the navigation receiver’s “GPS Information Screen.” 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. They point to the receiver saying its antenna is 39 meters 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 percent (normal is less than 10 percent).

The RNT Foundation has received numerous anecdotal reports of maritime problems with AIS and GPS in Russian waters, though this is the first publicly available, well-document account, of which we are aware.

Russia has very advanced capabilities to disrupt GPS. Over [**250,000 cell towers in Russia have been equipped with GPS jamming devices**](http://fmso.leavenworth.army.mil/OEWatch/201610/FMSOs%20OE%20Watch%20Oct%202016.pdf) as a defense against attack by U.S. missiles. And there have been press reports of Russian GPS jamming in both Moscow and the Ukraine. In fact Russia has boasted that its capabilities “[**make aircraft carriers useless**](http://www.spacedaily.com/reports/Russian_E_Warriors_Render_Aircraft_Carriers_Useless_999.html),” and the U.S. Director of National Intelligence recently issued a [**report**](https://rntfnd.org/2017/05/14/us-adversaries-focusing-on-jamming-gps-other-satellites-dir-national-intelligence/) that stated that Russia and others were focusing on improving their capability to jam U.S. satellite systems.

Assuming Russia is behind this, why would they do such a thing?

Maybe it was to encourage use of the Russian GLONASS satellite navigation system or their terrestrial Loran system, called Chayka, instead of GPS.  
Perhaps it was for some security reason known only to them.

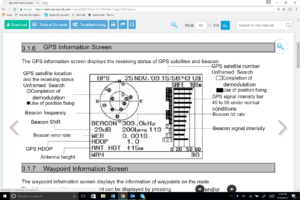
Whatever the reason, we are reminded of a maritime GPS disruption incident last year and the U.S. Coast Guard’s [**subsequent advice**](https://rntfnd.org/2016/01/19/uscg-issues-safety-alert-gpsgnss-trust-but-verify/) about GPS and all satnav – “Trust But Verify.”

*Dana A. Goward is President of the Resilient Navigation and Timing Foundation.*









**[https://rntfnd.org/wp-content/themes/newoffer/images/icons/digg_16.png](http://www.digg.com/submit?phase=2&url=https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/)[https://rntfnd.org/wp-content/themes/newoffer/images/icons/stumbleupon_16.png](http://www.stumbleupon.com/submit?url=https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/&title=Mass+GPS+Spoofing+Attack+in+the+Black+Sea%3F+%26%238211%3B+Maritime+Executive)[https://rntfnd.org/wp-content/themes/newoffer/images/icons/facebook_16.png](http://www.facebook.com/sharer.php?u=https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/&t=Mass%20GPS%20Spoofing%20Attack%20in%20the%20Black%20Sea?%20%E2%80%93%20Maritime%20Executive)[https://rntfnd.org/wp-content/themes/newoffer/images/icons/email_16.png](mailto:EMAIL%20ADDRESS?body=https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/)**



[](http://www.maritime-executive.com/)

Vrh obrazca

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | |  |

Dno obrazca

* [**NEWS**](http://maritime-executive.com/)
* [**FEATURES**](http://maritime-executive.com/features)
* [**MAGAZINE**](http://maritime-executive.com/magazine)
* [**NEWSLETTER**](http://maritime-executive.com/newsletter)
* [**BLOGS**](http://maritime-executive.com/blog)
* [**DIRECTORY**](http://www.maritime-executive.com/maritime-directory)
* [**SUBSCRIBE**](http://maritime-executive.com/subscribe)
* [**ADVERTISE**](http://mediakit.maritime-executive.com/)

[inShare](javascript:void(0);)189

[submit to reddit](http://www.reddit.com/submit)

# Mass GPS Spoofing Attack in Black Sea?



By [**Dana Goward**](http://www.maritime-executive.com/author/dana-goward) 2017-07-11 20:22:39

An apparent mass and blatant, GPS spoofing attack involving over 20 vessels in the Black Sea last month has navigation experts and maritime executives scratching their heads.

The event first came to public notice via a relatively innocuous [safety alert](https://www.marad.dot.gov/msci/alert/2017/2017-005a-gps-interference-black-sea/) from the U.S. Maritime Administration:

A maritime incident has been reported in the Black Sea in the vicinity of position 44-15.7N, 037-32.9E on June 22, 2017 at 0710 GMT. This incident has not been confirmed. The nature of the incident is reported as GPS interference. Exercise caution when transiting this area.

But the backstory is way more interesting and disturbing. On June 22 a vessel reported to the U.S. Coast Guard Navigation Center:

GPS equipment unable to obtain GPS signal intermittently since nearing coast of Novorossiysk, Russia. Now displays HDOP 0.8 accuracy within 100m, but given location is actually 25 nautical miles off; GPS display…

After confirming that there were no anomalies with GPS signals, space weather or tests on-going, the Coast Guard advised the master that GPS accuracy in his area should be three meters and advised him to check his software updates.

The master replied:

Thank you for your below answer, nevertheless I confirm my GPS equipment is fine.

We run self test few times and all is working good.

I confirm all ships in the area (more than 20 ships) have the same problem.

I personally contacted three of them via VHF, they confirmed the same.

Sometimes, position is correct, sometimes is not.

GPS sometimes looses position or displays inaccurate position (high HDOP).

For few days, GPS gave a position inland (near Gelendyhik aiport) but vessel was actually drifting more than 25 NM from it.

Important: at that time, GPS system considered the position as "Safe within 100m".

See attached.

Then last night, position was correct despite several "lost GPS fixing position" alarm that raised couples seconds only; then signal was back to normal.

Now position is totally wrong again.

See attached pictures that I took on 24 June at 05h45 UTC (30 min ago).

Note: you can also check websites like MarineTraffic and you will probably notice that once in a while all ships in the area are shifting inland next to each other.

I hope this can help.

To back up his report, the master sent photos of his navigation displays, a paper chart showing his actual position and GPS-reported position, and his radar display that showed numerous AIS contacts without corresponding radar returns (below).

One of the photos was of the navigation receiver’s “GPS Information Screen.” 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. They point to the receiver saying its antenna is 39 meters 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 percent (normal is less than 10 percent).  
      
The RNT Foundation has received numerous anecdotal reports of maritime problems with AIS and GPS in Russian waters, though this is the first publicly available, well-document account, of which we are aware.

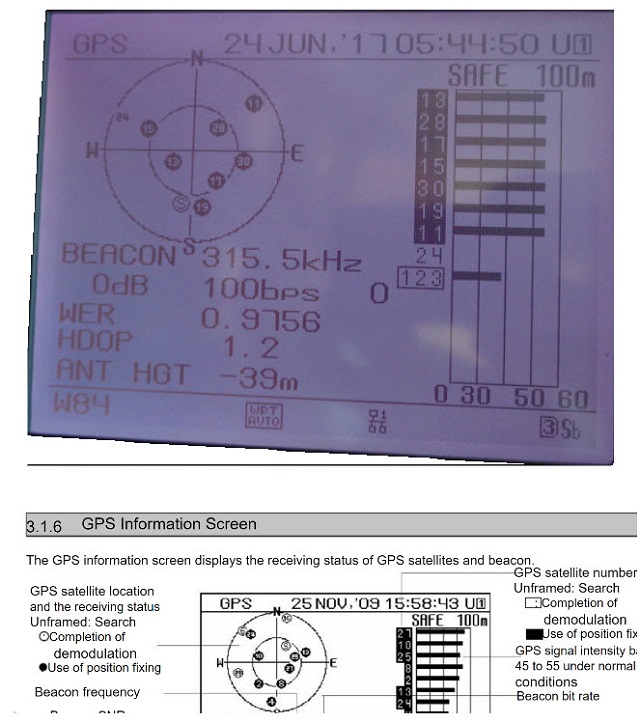
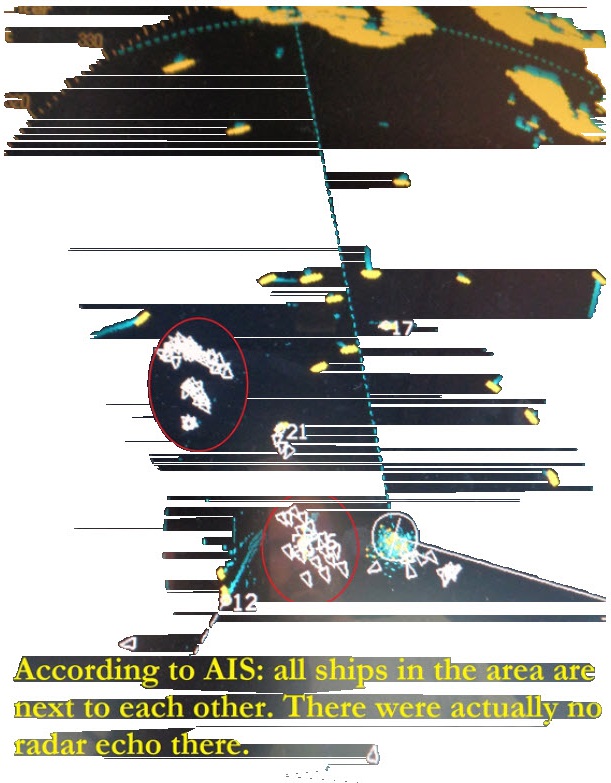
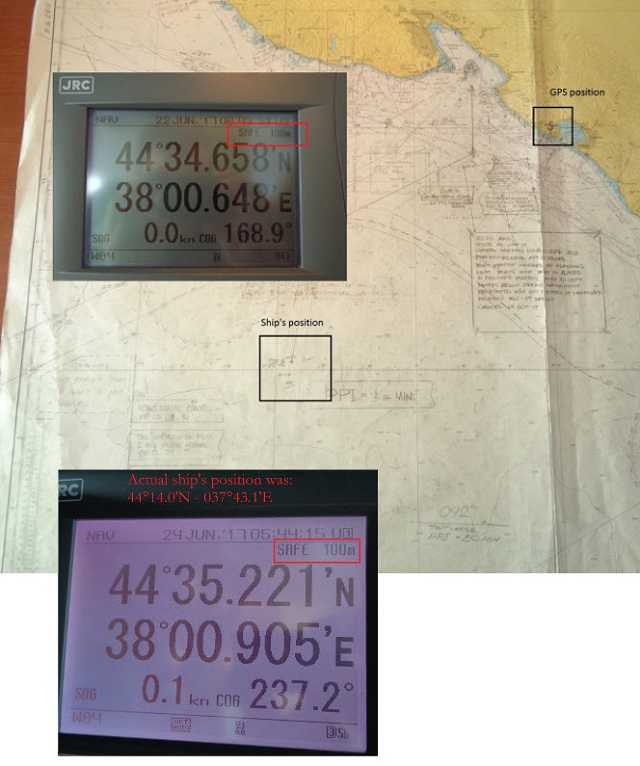
Russia has very advanced capabilities to disrupt GPS. Over [250,000 cell towers in Russia have been equipped with GPS jamming devices](http://fmso.leavenworth.army.mil/OEWatch/201610/FMSOs%20OE%20Watch%20Oct%202016.pdf) as a defense against attack by U.S. missiles. And there have been press reports of Russian GPS jamming in both Moscow and the Ukraine. In fact Russia has boasted that its capabilities “[make aircraft carriers useless](http://www.spacedaily.com/reports/Russian_E_Warriors_Render_Aircraft_Carriers_Useless_999.html),” and the U.S. Director of National Intelligence recently issued a [report](https://rntfnd.org/2017/05/14/us-adversaries-focusing-on-jamming-gps-other-satellites-dir-national-intelligence/) that stated that Russia and others were focusing on improving their capability to jam U.S. satellite systems.

Assuming Russia is behind this, why would they do such a thing?

Maybe it was to encourage use of the Russian GLONASS satellite navigation system or their terrestrial Loran system, called Chayka, instead of GPS.  
Perhaps it was for some security reason known only to them.

Whatever the reason, we are reminded of a maritime GPS disruption incident last year and the U.S. Coast Guard’s [subsequent advice](https://rntfnd.org/2016/01/19/uscg-issues-safety-alert-gpsgnss-trust-but-verify/) about GPS and all satnav - “Trust But Verify.”

Dana A. Goward is President of the Resilient Navigation and Timing Foundation.

**

***The opinions expressed herein are the author's and not necessarily those of The Maritime Executive.***

## [MarExFeatures](http://www.maritime-executive.com/features)



[](https://disqus.com/by/disqus_ueIzS2cChg/)

[**Mike Forsyth**](https://disqus.com/by/disqus_ueIzS2cChg/) • [13 minutes ago](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3414568482)

Another form of spoofing is probably technically much easier than spoofing the satellite signal. A transmitting station could "impersonate" one or more vessels by transmitting the vessel's identifying information, but with a different position, course, speed, destination, etc. Amen on the celestial. And use the "acquire" button on the ARPA radar just to be sure the real-time radar blip is moving the same way that AIS says it is.

* + •
  + [Reply](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
  + •
  + Share ›

[](https://disqus.com/by/HussarLitewski/)

[**HussarLitewski**](https://disqus.com/by/HussarLitewski/) • [8 hours ago](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3414181861)

Interesting.

* + •
  + [Reply](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
  + •
  + Share ›



**Buddenberg** • [17 hours ago](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3413568198)

This issue is not kinetic energy but rather RF energy and what we call r-squared. As the distance from a transmitter increases, the energy a receiver has to deal with decreases proportional to the square of the distance. In the case of GPS satellites, r is something like 15,000 miles (depending on slant ranges) so the signal is very (like VERY) faint. It takes very little energy from a nearby source to blank that signal; leakage from side frequencies on transmitters can do it.   
So the first issue is jamming -- a nearby source outshouts the satellites. That's been with us from the beginning of GPS and is common to all satnav systems.  
Spoofing (the opposite of authentic) is what the master here is reporting (convincingly). Faking the satellite signal and convincing the shipboard receiver to follow the bogus signals rather than the real ones. Like jamming, the spoofing signal needs to be 'convincing' and 'stronger' is one of the ingredients. This has not been with GPS from the beginning because the electronics necessary to fake a satellite payload are somewhat more sophisticated than a simple jammer. But they're obviously here.  
Dana speaks with experience. He's been carrying the torch for re-establishing the Loran system for several years. But both legislative and executive branches of US government have been, er, apathetic, with a few exceptions.

Shifting subjects. All three national saltwater academies are teaching celestial navigation these days.

* + [1](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
  + •
  + [Reply](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
  + •
  + Share ›



**joe Tenaglia** • [20 hours ago](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3413207808)

Our enemies and adversaries have had the ability to jam/spoof GPS for many years. In a war we cannot assume GPS will be operational. Its like the threat from EMP, its easier to ignore, until its too late. Hang onto your charts and sextants.

* + [1](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
  + •
  + [Reply](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
  + •
  + Share ›

[](https://disqus.com/by/disqus_3rVwb6Qxm0/)

[**Ohso**](https://disqus.com/by/disqus_3rVwb6Qxm0/) • [21 hours ago](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3413163516)

"master sent... a paper chart showing his actual position"

Was it wrapped around a Dinosaur Bone?  
Anyone who understands Kinetic Energy know how vulnerable All space based systems are, as there is no need for sophisticated bombs targeting satellites when simply sending a load of ball bearings or other 'space junk' (as with the highly realistic movie 'Gravity') in to the proper orbit is all that is really needed.

* + •
  + [Reply](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
  + •
  + Share ›



**Nabo** • [a day ago](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3412311047)

Celestial Navigation is good but not enough in today's world. One should consider having to type of GNSS instead of depending upon GPS

* + •
  + [Reply](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
  + •
  + Share ›



**Nabo** [Nabo](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3412311047) • [a day ago](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3412586230)

corrections "two types of GNSS"  
There are GNSS receivers available in the market capable of receiving all type (SBAS, QZSSS, GLONASS, Galileo)....

[](https://disqus.com/by/disqus_2ZTB864IsW/)

[**Angel**](https://disqus.com/by/disqus_2ZTB864IsW/) • [2 days ago](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3412187159)

This is why we must be proficient navigators using time tested methods including Celestial Navigation. It is impossible for humans to spoof celestial bodies! In case of war any good admiral would want to deprive the enemy's ability to navigate, communicate and to spoof GPS and over GPS like systems like GLOSSNAS or GALILEO that the enemy's weapons use for navigating to their target. This is a real thread and a real concern!

* + [2](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
  + •
  + [Reply](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
  + •
  + Share ›

[](https://disqus.com/by/disqus_wqkxkQI6nZ/)

[**Rick Sullivan**](https://disqus.com/by/disqus_wqkxkQI6nZ/) [Angel](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3412187159) • [21 hours ago](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3413095200)

It should be remembered that the military is using a completely different Code for the GPS reception from civilian ships. I certainly agree that you can not spoof the heavens. It's interesting to know that several years ago the US Navy did away with the classes to educate our young officers in Celestial Navigation usage. It's only been in the Last several months that officers are once again being trained to use a Sextant and DR procedures. I'm glad someone on the Fleet is thinking ahead.

* + - [1](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
    - •
    - [Reply](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
    - •
    - Share ›
      * 
      * [−](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)

[](https://disqus.com/by/disqus_2ZTB864IsW/)

[**Angel**](https://disqus.com/by/disqus_2ZTB864IsW/) [Rick Sullivan](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3413095200) • [12 hours ago](http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#comment-3413936853)

You are right! I am an Electrical Engineer and I can tell you that GPS, satellite communications, etc are very vulnerable to jamming, spoofing, cyber warfare, electronic counter measures, etc. It is essential to bring the paper charts back and the traditional communication methods.

* + - * •
      * [Reply](https://disqus.com/embed/comments/?base=default&f=maritime-executive&t_i=mass-gps-spoofing-attack-in-black-sea&t_u=http%3A%2F%2Fwww.maritime-executive.com%2Feditorials%2Fmass-gps-spoofing-attack-in-black-sea&t_d=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&t_t=Mass%20GPS%20Spoofing%20Attack%20in%20Black%20Sea%3F&s_o=default)
      * •
      * Share ›