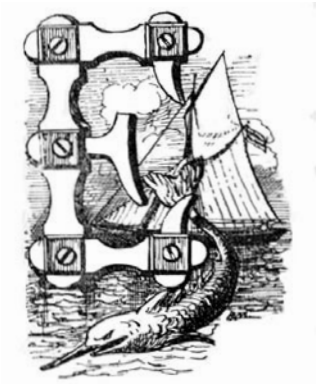
MARSEC-20. UN ESCENARIO DE CIBERSEGURIDAD MARÍTIMA

Luis PERALES GARAT

No vive el que no vive seguro.

Francisco de Quevedo.

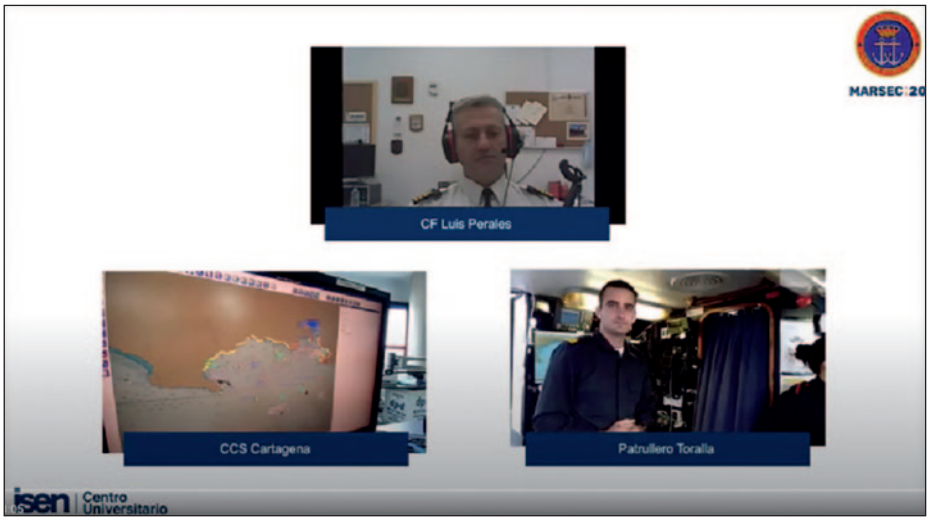


EN noviembre de 2020, superando los innumerables escollos que la COVID nos había puesto por el camino, pudimos completar el escenario de ciberseguridad del MARSEC-20. Y digo completar porque el ejercicio en sí ya había comenzado: se había «perpetrado» un número de test de penetración (PENTEST) en varios sistemas, civiles y militares.

El ejercicio lo planteamos COVID *free*. Después de muchas vueltas —y muchas reflexiones sobre el ser y el no ser, esa era la cuestión—, planeamos las fases de tal manera que, sí o sí, se pudieran realizar. Obviando los mencionados PENTEST que se habían hecho con anterioridad —y no es necesario pensar mucho para saber que a un *pentester*, que es algo así como un *hacker* bueno, no hace falta sacarle de casa para «penetrar» en tu sistema—, montamos un seminario *web* (*webinar*, que se dice ahora) retransmitido en un canal privado de YouTube, y unas pruebas en la mar, donde cada unidad era independiente.

Salió —¡vaya que si salió!— lo esperado. El ejercicio nos demostró la vulnerabilidad del entorno marítimo, incluyendo a muchos de los organismos y actores que toman parte en él. Y no hablamos solo de incidentes que afectan a nuestros datos en el ciberespacio, sino de ataques directos por medio de emisión de energía (radiación electromagnética en los espectros de trabajo de los diferentes sistemas) con efectos tangibles en los medios que se emplean diariamente en la mar, como comunicaciones, ayudas a la navegación o medios de control del tráfico marítimo.

Pero vamos a contarlo sin más, que se nos dará mejor.



Retransmisión por el canal YouTube del ISEN.

Los susodichos PENTEST

Un PENTEST es, básicamente, una prueba controlada del estado de seguridad de la infraestructura IT de cualquier organización. Con un acuerdo entre las partes —y a un precio en este caso de saldo, puesto que se hizo de manera gratuita— se realiza una penetración en un sistema para conocer cuál es su estado de seguridad ante determinadas amenazas.

En nuestro caso fue SGS (1), que hizo las pruebas «contra» aquellas empresas que se prestaron. Sin dar detalles —probablemente inadecuados, dada la confidencialidad del acuerdo entre las partes—, se procedió a penetrar en los siguientes:

— Un sistema de una agencia estatal del entorno marítimo.
— Una página de una autoridad portuaria.
— Un buque de una empresa en la mar.

Todos ellos se mostraron fácilmente vulnerables, afectando a la tríada de la seguridad: disponibilidad, integridad y confidencialidad. Es decir, dentro del límite de las pruebas se alcanzó un estado donde se podría haber limitado

(1) SGS-Cybersecurity Services, líder mundial en inspección, verificación, análisis y certificación.

Facilidad del ataque.

—léase interrumpido— el acceso a un determinado servicio (2), modificando los datos disponibles o disponer de ellos para su exposición o cifrado, es decir, secuestro de los datos (*ransomware*). Especialmente impactante es el hecho de poder acceder a los sistemas de control de un buque en la mar de manera que puedas controlar tanto su planta propulsora como sus sistemas de navegación; ¿qué no se podría hacer con un barco cargado de cualquier sustancia peligrosa?

De la misma manera, por parte del Mando Conjunto del Ciberespacio se realizó un PENTEST contra una infraestructura de Defensa. Los resultados —controlados, como en el caso anterior— fueron los mismos; en este caso, la denegación de prestaciones de un servicio *web*, con una desfiguración —*defacement*— de la página en cuestión para evidenciar que habían coronado con éxito la misión.

Los test demostraban tres aspectos fundamentales: sencillez en su ejecución, sin necesidad de disponer de un nivel de conocimiento especialmente profundo; facilidad de actuación, sin tener que disponer de privilegios especiales dentro de los sistemas, e independencia del atacante, sin precisar ningún tipo de colaboración —intencionada o no— por parte de los usuarios del sistema blanco de los ataques: 1 - 0, y Zamora de portero.

(2) DoS: *Denial of Services*.

El seminario

Como comentaba anteriormente, organizamos un seminario *web* que se retransmitió en directo (para usuarios registrados) por un canal de YouTube privado proporcionado por el Centro Universitario ISEN de Cartagena, que no solo gestionó la infraestructura *on line* precisa, sino que creó una página *web* que daba cuenta del ejercicio y permitía registrarse en las ponencias.

Durante su desarrollo pudimos contar con la aportación de ponentes de primerísimo nivel: la Dirección General de la Marina Mercante y Puertos del Estado, los principales organismos del Estado en seguridad marítima; el Centro Criptológico Nacional (CCN) y el Instituto Nacional de Ciberseguridad (INCIBE) como máximos responsables de la ciberseguridad; la Agencia Europea de Seguridad Marítima (EMSA), el Clúster Marítimo Español (CME) y empresas del sector, como SGS, OSS y el Grupo Carnival, así como los componentes militares de la ciberseguridad, el Mando de Operaciones y, obviamente, el Mando Conjunto del Ciberespacio. En resumen, los organismos responsables de la gestión de nuestras aguas y puertos, los tres CERT (3) nacionales, CCN, INCIBE y MCCE, y un número importante de actores —civiles y militares— con actividad en el área de la ciberseguridad.

Los ponentes, primeros espadas en sus respectivas áreas de competencia, nos ilustraron sobre aspectos normativos de las amenazas y vulnerabilidades, de los sucesos acaecidos, y nos contaron en vivo —en el caso de los *pentesting*— lo fácil que resulta hacerlo.

Este es un compendio de las ideas aportadas, no por conocidas de menor importancia:

— Los incidentes más habituales son el *phishing* o *spear-phishing,* es decir, el robo de credenciales con la intervención —bajo engaño— del operador.
— El ataque más frecuentes es el *ransomware*, o sea, la captura y cifrado de nuestros datos para exigir un rescate bajo la amenaza de hacerlos públicos.
— Las barreras habituales, cortafuegos y antivirus, no son suficientes.
— Los programas y sistemas no actualizados —s*oftware* y *firmware*— son una invitación para los *hackers*.
— El uso y la compartición de contraseñas, un pobre diseño y la falta de actualización son las mejores puertas de entrada.
— Los USB son capaces de transportar tu vida en imágenes... y tu muerte informática.

(3) CERT: *Computer Emergency Response Team*.

— La realización frecuente de PENTEST es la mejor manera de garantizar la actualización y seguridad de tus sistemas.
— Es necesario mantener copias de seguridad, según la regla 3-2-1: tres copias-dos formatos diferentes-una copia *off line*.
— Y, sobre todo, es absolutamente imprescindible la concienciación del personal.

Una buena noticia: de momento, el sector marítimo español se ha mantenido relativamente al margen de ciberataques, salvo el perpetrado en 2018 al Puerto de Barcelona.

Las DEMO

Como continuación del seminario montamos unas pruebas de perturbación en los diferentes sensores que son parte inherente del entorno marítimo. Para ello contamos con actores externos, principalmente el JEWCS de la OTAN y el Regimiento de Guerra Electrónica REW-31, pero también con la inestimable ayuda, de nuevo, de SGS.

Con la pandemia encima y las restricciones para moverse cambiando de día en día, no fueron pocos los retos a los que nos enfrentamos: que si los equipos están comprometidos, que si no podemos viajar, que si PCR, cuarentena... y un sinfín de preguntas, muchas de ellas sin respuesta, que decidimos obviar, no tanto por inconscientes, sino por ser un *show stopper* fuera de nuestro control. Lo cierto es que, al final, contamos con todo lo que necesitábamos y con los permisos necesarios, que incluían a las autoridades marítimas y a los responsables de las emisiones, Capitanía Marítima y Dirección General de Telecomunicaciones, para hacer todas las pruebas previstas.

Perturbación GPS

La primera de todas las pruebas, y a nadie se le escapa el problema, fue la perturbación del GPS en aguas de Cartagena. Desplegamos el NWDA (4) del JEWCS en El Portús y perturbamos los equipos del *Toralla*, nuestro *sparring* todos estos días, y de otros barcos presentes en la zona.

La perturbación, con la limitadísima potencia que habíamos solicitado, fue todo un éxito... dentro de las distancias que garantizaba esa potencia. Perturbamos los equipos fijos de a bordo y comprobamos que el apantallamiento que se conseguía con la superestructura del buque era suficiente para

(4) NWDA: *Navigational Warfare Denial Asset*.

permitir que el GPS portátil —y el móvil multiconstelación (5)— mantuviera la señal.

En una segunda fase, verificamos que ambos equipos eran también perturbados cuando los poníamos libres de obstáculos en la dirección de la perturbación. Como digo, concluyente y perfectamente alineado con la doctrina nacional en estos aspectos. Utilizando un símil de El Portús, con su conocido camping nudista, con un poco más de potencia los hubiéramos dejado «en pelotas». Dos conclusiones inmediatas:

— La necesidad de disponer de sistemas multiconstelación (6) cuando no existen medios de posicionamiento alternativos.
— La conveniencia de tener las antenas GPS (o GNSS) de manera que permitan un apantallamiento direccional (no hay que olvidar que, tal como nosotros hicimos, la perturbación proviene normalmente de una fuente física en la visual y dentro del alcance del blanco).

Amanece en El Portús y el NWDA del JEWCS está listo para perturbar.
(Fotografía facilitada por el autor).

(5) GNSS: *Global Navigation Satellite System*. Son equipos con seguimiento de varios sistemas de posicionamiento. En nuestro caso, GPS, Galileo (UE), GLONASS (Rusia) y Beidou (China).

(6) Sí, es verdad que esto no afecta de manera grave a unidades que disponen de sistemas alternativos de posicionamiento, como un navegador inercial (INS).

Perturbación radar y de comunicaciones

Con los medios del REW-31, comenzamos los ejercicios de perturbación de sistemas radáricos y de comunicaciones.

El primero de ellos, escogiendo como blanco el radar de Salvamento Marítimo en cabo Tiñoso, consiguió «cegar» al CCS, haciendo desaparecer toda la presentación que proporcionaba el radar. Fue una prueba interesante, principalmente por permitir eliminar el método alternativo de seguimiento al AIS (sí, hoy las tornas se han invertido, como pasa con el IFF en los aviones, que de radar secundario se ha convertido en el principal sistema de seguimiento).

Las pruebas de comunicaciones consiguieron, con las limitaciones impuestas por el ejercicio, negar las comunicaciones en los canales de VHF seleccionados (manteníamos como frecuencias prohibidas, tabú, todas aquellas que nos requirieron). Se trabajó con dos canales de la banda del Servicio Móvil Marítimo (SMM), consiguiendo impedir la comunicación primero en un único canal, y después entre dos canales alternativos.

Creemos que el sistema demostró claramente la posibilidad de interrumpir las comunicaciones en toda la banda de VHF marina si así se decidiera.

Perturbación AIS

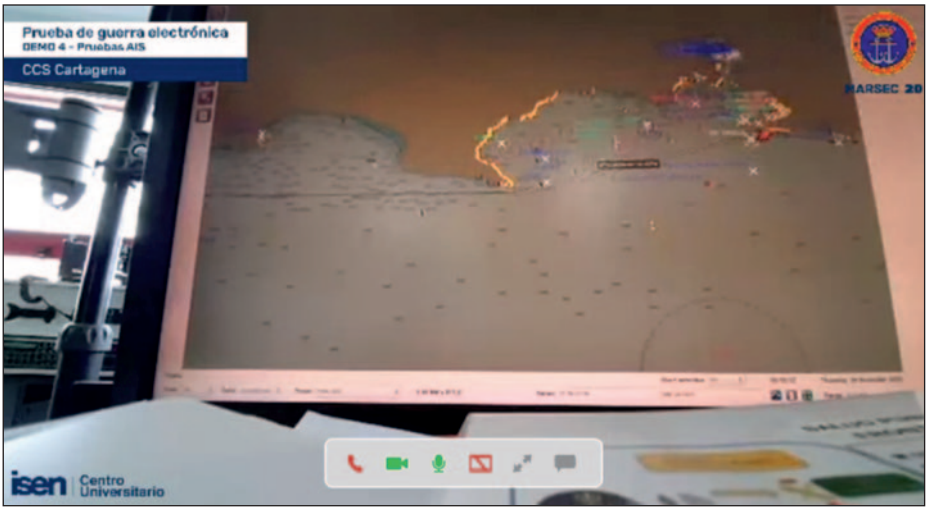
De la misma manera que con las comunicaciones, puesto que el AIS trabaja en frecuencias (y canales) del SMM, se consiguió negar la recepción AIS en la zona del ejercicio.

Dados los resultados anteriores con la banda de VHF, fue realmente simple. La única observación es la necesidad de conocer cada uno de los sistemas y aplicaciones de uso habitual (hay un número importante de aplicaciones que proporcionan información AIS: *Marinetraffic, Vesselfinder, AISLive*...) para saber el origen de los datos y los tiempos de refresco de cada sistema y ser capaces de interpretar correctamente la ausencia —o retraso de refresco— de las trazas.

Decepción spoofing *AIS*

Después de las pruebas con el REW-31, comenzamos otras si cabe más interesantes, con un sistema de engaño, *spoofing*, diseñado por SGS, que consiste en un equipo receptor y transmisor AIS, conectado a un PC con un programa que permite manejar las trazas. Su coste, todo con elementos comerciales, no excede de 1.000 euros.

Los primeros ensayos consistieron en la creación de blancos falsos en la zona del ejercicio, en las proximidades del *Toralla*, que los detectó sin ningún



♫El AIS ha desaparecido y nadie sabe cómo ha sido♫

problema (tenían un MMSI (7) falso y el sistema «cantaba» a la primera). Pero esto era solo el calentamiento para continuar con las manipulaciones.

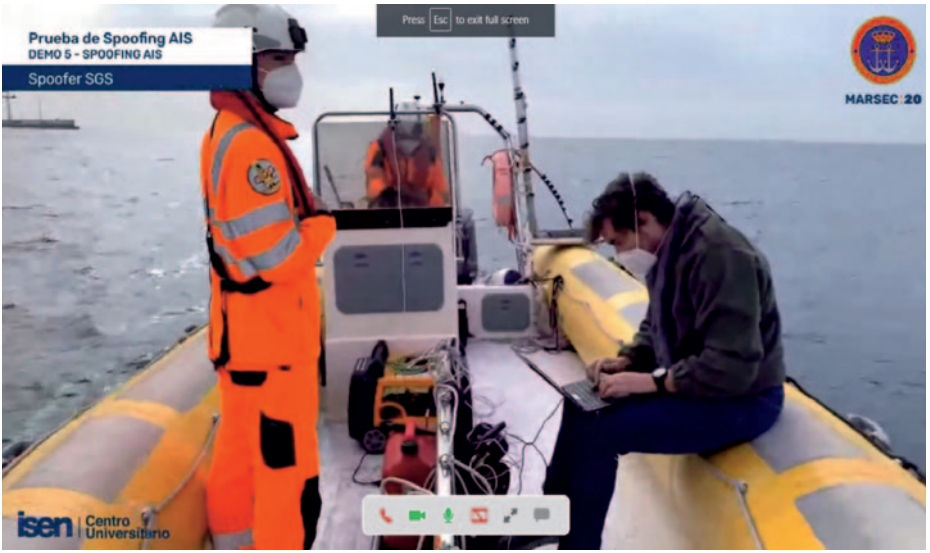
El siguiente paso fue hacer desaparecer una traza AIS que estaba en el fondeadero. Aunque el buque se reposicionó en Australia y el *Toralla* lo localizó allí a la primera, también lo podríamos haber hecho desaparecer del todo.

La siguiente prueba fue generar una traza AIS falsa con una cinemática determinada. En nuestro caso, un contacto a rumbo de colisión con el *Toralla*. De nuevo, el objetivo era que lo viera el buque y evitar cualquier incidente de navegación, con lo que el resultado fue satisfactorio, aunque fácilmente detectable.

Por último, relocalizamos una traza que estaba entrando por el dispositivo de separación de tráfico del cabo de Palos y la situamos al sur de Mazarrón. Se le ordenó al *Toralla* que nos diera una demora al contacto, que coincidía obviamente con la nuestra. Cuando el buque, supuestamente, debía dirigirse a un rumbo de interceptación, lo relocalizamos de nuevo al sur de su posición (la demora anterior era SW); el *Toralla* nos dio la demora correcta... a la traza que no existía. Cerramos el ejercicio pidiéndole, con todas las manipulaciones de traza finalizadas, que localizara al buque. Como ya he dicho, estaba en el dispositivo de Palos.

---

(7) MMSI: *Maritime Mobile Service Identity*, número único asignado a cada buque o estación por el estado de pabellón.



Equipo de *spoofing* AIS a bordo de la embarcación de OSS.

En su conjunto, las pruebas de *spoofing* AIS demostraron lo fácil que es engañar la presentación AIS, que es hoy en día la fuente principal de información, tanto para cometidos de seguridad marítima —*safety*— como de protección —*security*—, siendo de especial importancia el hecho de que todas las pruebas tenían una gran capacidad disruptiva en el tráfico marítimo a un coste muy reducido. Y aunque estas también habían producido el mismo efecto, se realizaron de una manera mucho más discreta.

Conclusiones

La organización del ejercicio fue todo un reto no solo por la especial situación por la pandemia, sino por ser la primera vez que lo organizábamos. Tuvimos que darle forma desde cero —seminario y pruebas—, hasta que al final salió como esperábamos. El ejercicio tuvo algo de histórico, al ser el primero de su tipo en el que participaban tantísimos actores, abriendo una interesante área de colaboración en el ámbito marítimo.

La conclusión más clara de todo el escenario fue la vulnerabilidad del sector marítimo a las ciberamenazas, vengan de donde vengan. Esto afecta tanto a buques como a instalaciones portuarias o a cualquiera de los posibles actores y autoridades del sector. Son múltiples los foros e iniciativas, y la normativa es profusa; pero la realidad palpable es que las amenazas están

presentes y las medidas a adoptar —muchas y diversas— no son ni fáciles ni baratas, pero sí necesarias.

Pero lo que tenemos más claro es que este escenario se tiene que repetir —se va a repetir— en MARSEC-21 (8). Buscaremos nuevas formas e ideas y más medios de cooperación para conseguir que la ciberseguridad sea un pilar fundamental de nuestro *modus vivendi*, y así evitar que el mar, ese espacio de libertad, se vea mancillado en esa característica que lo engloba y ennoblece: la libertad de navegación y de comercio.

(8) El Ejercicio se desarrollará entre los días 3 y 7 de mayo.