IMPACTO DE LA CONVIVENCIA CON LOS DISPOSITIVOS MÓVILES PERSONALES A BORDO DE BUQUES EN OPERACIONES ACTUALES Y FUTURAS

Pedro José GARCÍA ELVIRA

No es fe en la tecnología. Es fe en la gente.

Steve Jobs.

Introducción

A rapidez con que la tecnología avanza supera en muchas ocasiones no solo la capacidad de su aprendizaje, sino también el simple hecho de llegar a conocer su existencia. Hace un par de décadas, cuando todavía aspiraba al ingreso como oficial, tuve el privilegio de disponer de mi primer móvil, que sin duda redujo enormemente el tiempo que empleaba en buscar una cabina telefónica que estuviera libre para hablar con mis padres. Todo el que esté leyendo este artículo en cierto modo tendrá un recuerdo parecido y, tras unos cuantos años, se habrá percatado de cuál es la situación actual y cuán exponencial ha sido la evolución.

Los dispositivos móviles en todas sus facetas de uso son tan cotidianos como el timón de nuestros buques. Alrededor del *Internet of Things* (IoT) nuestra vida está más que conectada, y poco a poco influye de manera más trasversal a todos los grupos de edad. Por lo general, actualmente casi todos tenemos un *smartphone* o una *tablet,* y estos dispositivos, que podríamos considerar ordenadores, nos dan unas inmensas posibilidades en el día a día. Muchos de nosotros, cada uno con su afición o *hobby* particular, disponemos de un *smarthwatch* o de un reloj con geoposicionamiento y pulsómetro,

que nos permite analizar y disfrutar de un sinfín de disciplinas deportivas. En la oficina, y con el reciente despegue del teletrabajo obligado por el confinamiento debido al COVID-19, hemos descubierto numerosas aplicaciones para gestionar llamadas grupales por videoconferencia. Pero es que en casa también podemos disponer de un aspirador que levanta un mapa 2D del salón en tu *app* móvil, o de un robot de cocina que hace la lista de la compra, o de uno de los famosos asistentes de las grandes compañías que se manejan por voz y que han hecho posible la llegada de la domótica a un precio asequible.

Es evidente que algunos de estos dispositivos se vienen con nosotros a las unidades y nos facilitan enormemente el trabajo y el ocio diario a bordo. En varias ocasiones me he planteado si somos capaces de evitar la nomofobia (1) y si realmente nuestras dotaciones estarían preparadas para una desconexión real y prolongada.

¿Qué problemas van asociados al uso de los dispositivos móviles?

La principal herramienta que utilizan nuestros dispositivos son las aplicaciones. El catálogo y distintas funcionalidades que existen hacen que la oferta sea extremadamente amplia, pero no todas ofrecen garantías de seguridad y privacidad. Algunas de ellas se instalan de forma oculta y supusieron la principal incidencia que sufrió el usuario en 2019, causando un aluvión de ataques furtivos sobre los dispositivos en 2020 (2).

El acceso y exposición de nuestras vidas en las redes sociales, más acusado en la juventud, pone de manifiesto que estas puedan suponer una fuga de información aparentemente inocua y una puerta de entrada a nuevos problemas. Sabemos que son una posible fuente de información para el enemigo o delincuente, a través de la cual se distribuyen *malwares* o se utiliza la información que la geolocalización ofrece mediante los metadatos de nuestras fotos.

El teletrabajo obligado durante el confinamiento nos ha permitido usar aplicaciones de videoconferencia grupales, algunas de ellas para reuniones oficiales con su correspondiente licencia y otras más accesibles para coordinación diaria que podían accionarse desde nuestras *tablets* (Skype, Teams, Zoom, Discord, etc.). Sin embargo, esto supone una sobreexposición a las amenazas que existen. Son conocidos casos en los que trabajadores del Departamento de Defensa estadounidense sufrieron ataques a través de la aplicación

(1) Miedo a salir a la calle sin el móvil.

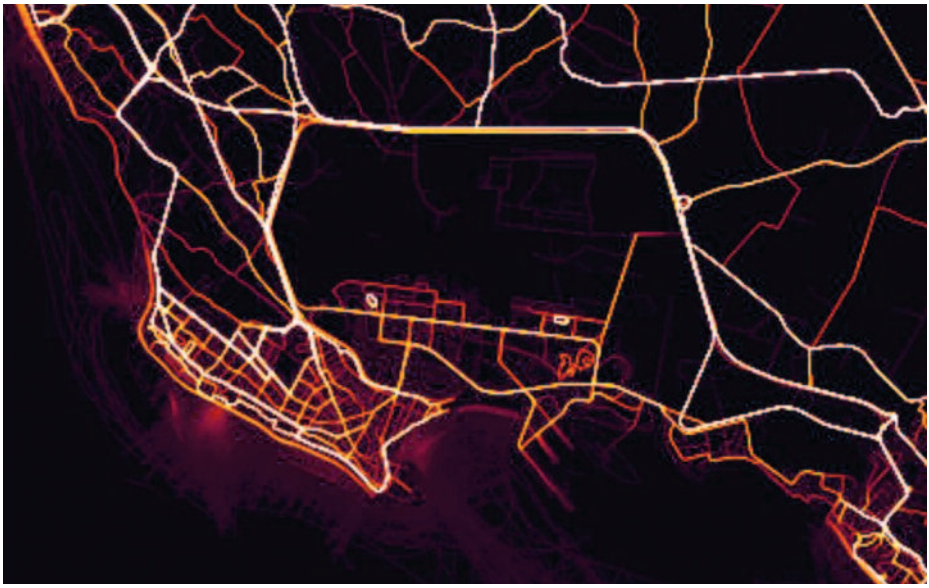
(2) Informe sobre amenazas móviles 2020 de McAfee, *www.mcafee.com/content/damconsumer/en-us/docs/2020-Mobile-Threat-Report.pdf*.

Dotación del patrullero de altura *Centinela* (P-72) en un momento de descanso.

Tik Tok (3), por lo que recibieron la orden de desinstalarla o, como la Guardia Civil aconsejaba, solucionar problemas de seguridad con la aplicación Zoom, que tanta popularidad alcanzó en el estado de alarma al comienzo de la pandemia.

Según estamos viendo, tenemos en nuestras manos unas herramientas que con facilidad pueden dejar de serlo; pero el problema no solo está en el delincuente, sino que presuntamente existen estados que dedican gran cantidad de medios y financiación para explotarlas. De hecho, se puede aseverar que, sin ser superpotencias, determinados países muy especializados ocupan un puesto de referencia en este asunto. Sirva como ejemplo Estonia, que sufrió un ataque en 2007 que paralizó el país y a día de hoy tiene una conciencia digital mayor que el resto, como lo demuestra la designación de un embajador estonio para el ciberespacio, entre otras medidas.

(3) ARBAIZA, Alfonso: «Teletrabajo y la delgada línea que separa lo profesional de lo personal en ciberseguridad», *www.libertaddigital.com* (5-2-2020).



Mapa de calor de la Base Naval de Rota. (Fuente: *Strava.com*).

¿Qué problemas van asociados al uso de los dispositivos móviles en las Fuerzas Armadas?

El primer ejemplo que me viene a la mente es el de unos insurgentes en el año 2007 en Irak que destruyeron un *AH-64 Apache* gracias a los datos de geolocalización provenientes de unas fotografías que algunos soldados americanos subieron a la red. O Irán, que supo a través de la concentración de señales móviles la disposición de las tropas israelíes en el Líbano en 2006 (4). Otro más reciente es el de la aplicación deportiva Strava que, gracias al uso de relojes y dispositivos de entrenamiento, ha perimetrado numerosas bases militares en todo el mundo (5).

Casos como estos suponen unas importantes lecciones aprendidas en el plano táctico/operacional que están siendo aplicadas no solo en el mundo de la ciberseguridad, sino que ya forman parte de los planeamientos. En 2015, el coronel Paul G. Craft, Chief of Cyber and Commandant US Army Cyber School, dijo sobre la formación de sus oficiales: *Much of the curriculum is*

(4) «Insurgents Used Cell Phone Geotags to Destroy *AH-64s* in Iraq», *www.military.com* (15-3-2012).

(5) GÓMEZ, José Andrés: «Así es la app de 'running' que ha revelado dónde están las bases militares secretas de Estados Unidos», *www.elespañol.com* (29-01-2018).

coming directly from lessons learned from the operational force, and includes a mixture of cyberspace operations, electronic warfare and information operations (6).

La ciberembajadora de Estonia, Heli Tiirmaa-Klaar, asegura que «no habrá una ciberguerra. Habrá una guerra real con una faceta ciber» (7). Y efectivamente, nosotros contemplamos este hecho en la definición de las acciones híbridas (8).

El Mando Conjunto de Ciberdefensa (MCCD) acuña un mensaje de fuerza para hacernos ver el compromiso que tenemos las personas: «Delante del teclado, todos somos combatientes» (9). Me gustaría ampliar esta misiva para que seamos conscientes de que donde dice «teclado» podemos traducir «dispositivos móviles», y por qué, como me enseñaron en la especialidad, el principal culpable es el usuario; en nuestro caso, estar navegando con estos dispositivos no nos resta responsabilidad ni nos debe hacer pensar que a nosotros no nos va a afectar por estar en alta mar.

¿Cómo convivimos en los buques con los dispositivos móviles?

Desde hace bastante tiempo, la importancia que ha dado la Armada a la moral y el bienestar del personal es notable. Que las comunicaciones sociales sean más frecuentes ha incrementado la necesidad de relacionarnos con nuestras familias y con el mundo que dejamos atrás cuando salimos a la mar.

De todos los dispositivos que existen —de algunos ya se ha hablado anteriormente—, me quiero centrar en el *smartphone*, la *tablet* y el reloj con GPS, ya que el número de miembros de una dotación que los embarcan asiduamente es considerable. Mientras hay cobertura, y en momentos de esparcimiento fuera de la guardia, nos permiten estar en contacto con los nuestros, con la actualidad e incluso con los *hobbies* digitales. El enlace con el mundo fuera del buque sigue siendo posible. Cuando no hay cobertura, es posible tener acceso a través de terminales satélites civiles que nos facilitan la conectividad. Cuando no tenemos nada de esto, todavía podemos seguir sacándoles partido a bordo. Tenemos cámara de fotos, reproductor de música, linterna y despertador, entre otras muchas opciones. Por cierto, este último esgrimido como argumento para no pasar ni un segundo sin el móvil por la noche. ¿Qué fue del reloj despertador?

---

(6) POMERLEAU, Mark: «The Army's cyber school now teaches information operations», *www.fifthdomain.com* (enero 2016).

(7) PÉREZ COLOMÉ, Jordi: entrevista publicada el 1 de enero de 2020, *https://elpais.com/tecnologia/2019/12/21/actualidad/1576886357_152918.html*.

(8) Definido en la Estrategia de Seguridad Nacional de 2017.

(9) Boletín Infográfico del MCCD.

IoT. (Fuente: presentación previa despliegue MCCD).

Las *tablets* pueden tener dos vertientes principales en su uso: para trabajar de manera personal con aplicaciones de agenda y tareas que ayudan mucho a la productividad y a la organización (Any.do, To Do, Wunderlist, OneNote, etc.), y para el ocio cinéfilo o lector. Las plataformas de contenidos multimedia nos permiten descargar las películas y series que más nos gustan, ya sea para pasar el tiempo o hacer oído con el inglés, por ejemplo.

Los relojes con GPS suelen medir también datos del entrenamiento, como frecuencia cardiaca, tiempos, pasos, etc., motivando a las personas para continuar con la actividad deportiva dentro de una comunidad o red social específica.

Ya sea mucho o poco el tiempo libre disponible si estamos navegando, hemos conseguido traer a bordo muchas de las costumbres que tenemos en nuestros hogares. Quizás este sea uno de los motivos por los que la vida en las cámaras se ha reducido si lo comparamos con épocas pasadas.

¿Existe un impacto?

En mi humilde opinión sí lo hay, y es muy hondo. Por diversas circunstancias, durante el tiempo que he permanecido embarcado el procedimiento

Rivercity (10) se ha llevado a cabo de manera real en varias ocasiones. Por lo general, el nivel de concienciación es alto, así como su ejecución, pero hasta ahora siempre ha sido por períodos reducidos. En las ocasiones que ha ido más allá del tiempo utilizado normalmente durante ejercicios específicos, empieza a ser una preocupación, por un lado, controlar la información de acuerdo con la situación, como no puede ser de otra manera, pero por otro, a medida que los minutos y las horas pasan, el poder recuperar esa normalidad y conectividad.

La realidad es que no estamos acostumbrados a vivir sin nuestros dispositivos y esto es un factor más a tener en cuenta en los buques cuando una situación operativa puede obligar a una desconexión más prolongada de lo normal y que va a afectar psicológicamente a la dotación o a parte de ella. El procedimiento se prepara, se adiestra y se ejecuta, pero ¿por un tiempo suficiente? La probabilidad de tener que permanecer en la mar sin comunicaciones de ocio debido a una amenaza convencional es baja en este momento, pero sería útil el adiestramiento en este aspecto que, como hemos visto, ya tiene su eco en la guerra híbrida, y no solo nos afecta a nosotros, sino también a quienes tenemos al otro lado del WhatsApp.

Tal y como nos enseña el MCCD, hay que instruir en cierto modo a nuestras familias y a las personas con las que mantenemos un contacto habitual (11). Es evidente que, dependiendo de la unidad y de la posible actividad, conocen de manera aproximada los momentos en los que vamos a estar disponibles, pero el problema viene cuando la frecuencia se interrumpe y no saben por qué, lo que puede llegar a generar ansiedad por el hecho de saber que la parte contraria está preocupada debido al «silencio radio».

Este impacto no solo se ve afectado por el tiempo de desconexión que una dotación puede entrenar o sobrellevar, sino también por las posibles derivadas que la información incontrolada puede significar. Como hemos visto anteriormente, los dispositivos móviles son una fuente de información para el enemigo. Un buque anfibio del que salen 700 señales móviles puede facilitar la identificación y su posición en diversas circunstancias. Son conocidos también los casos en los que personal desplegado en el Báltico ha visto cómo sus líneas telefónicas se veían pirateadas.

Las cámaras de fotos o vídeos suponen otro problema. Aunque al instante pueda prohibirse su uso, el impacto de una foto una vez se levanta esa prohibición —ya sea por lo que cuenta, dónde lo cuenta o cuándo lo cuenta— puede tener consecuencias muy serias.

---

(10) Este procedimiento se ha diseñado para adaptar el flujo de información que entra/sale desde/hasta el buque en las diferentes condiciones de Seguridad Operativa de la Información (OPSEC).

(11) *Guía de buenas prácticas para el uso en redes sociales*. MCCD.

Petroleo del *Cantabria* con la fragata *Cristóbal Colón*.
(Foto: *www.flickr.com/photos/armadamde*).

Para nuestros compañeros de submarinos, estos posibles problemas están muy minimizados por su propia naturaleza, pero no olvidemos que también llevan dispositivos móviles, y al atracar en un puerto fuera de base todos encienden sus teléfonos.

Consideraciones

La empresa proveedora de servicios de seguridad en internet McAfee asegura que un usuario medio tendrá unos 15 dispositivos conectados para el año 2030 (12), por lo que se espera que los futuros ataques se dirigirán a través de los canales donde este se mantenga más tiempo. Es un hecho que, exceptuando los períodos para el trabajo delante de un ordenador corporativo, el resto estaremos acompañados por dispositivos móviles de todo tipo. ¿Podría suponer esto que en un futuro se debiera prohibir embarcar algunos dispositivos antes de irse de misión o desplegado? Podría pasar. Estados

(12) «Ataques ocultos, el gran reto para el usuario móvil», *cso.computerworld.es* (3-3-2020).

Unidos no permite en la actualidad los de la marca Huawei, y las restricciones de uso de móviles son mayores en los embarques.

El eslabón más importante, pero el más frágil, seguimos siendo nosotros, y por mucha tecnología que adquiramos y por muchos procedimientos que redactemos, tenemos que ser conscientes de que en torno al 90 por 100 de todos los ataques que se realizan en la red necesitan de la interacción de la víctima (13). Sería un error pensar que todos tenemos un alto dominio de la tecnología y de nuestros dispositivos pues, como estamos viendo, sus avances son imparables.

Conclusión

La evolución de dispositivos móviles y conectables es muy rápida y nuestra dependencia de ellos cada vez es mayor. Forman parte de nuestras rutinas, y muchas de ellas embarcan con nosotros. Esto significa que los problemas de seguridad derivados del uso de los mismos que puedan influir en las operaciones no van a verse disminuidos con el paso de los años.

No podemos perder de vista que si nos adiestramos como combatimos, necesitamos seguir concienciando a nuestras dotaciones de la importancia de adoptar las precauciones de seguridad en el uso de los dispositivos móviles y que, llegado el caso, deben estar preparadas para un posible período de desconexión prolongado real. A día de hoy, es poco probable; pero si dejamos que la dependencia de estos aparatos a bordo siga aumentando, el día que sea imperativo tendremos dificultades. En febrero del ya finalizado 2020, nadie pensaba que un virus podría confinar al mundo; cual película de Hollywood, parecía solo ficción.

(13) JIMÉNEZ, Javier: «El 90% de los ataques son por fallos humanos», *www.redeszone.net* (13-5-2020).

El *Galicia* visto desde un *SH-3D* en aguas del golfo de Cádiz, noviembre de 2020. (Foto: Marcos Vales Fincias).