Comentario THIBER:

Los retos tecnológicos de ciberseguridad en el FCAS

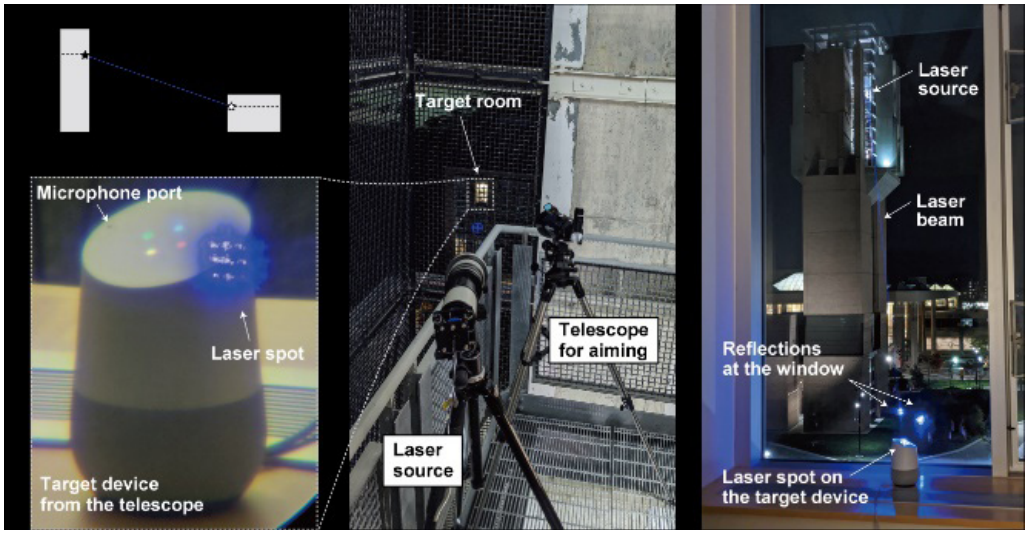
AUTOR: por THIBER

Fuente: Airbus

Cuando se habla de los retos tecnológicos en ciberseguridad para el Future Combat Air System (FCAS), es fundamental tener en cuenta el concepto de Sistema de Sistemas y su infraestructura inteligente de servicios, comunicaciones e información, que habilita al propio *Next-Generation Weapon System* (NGWS) operar en modo sistema de sistemas. Esto es, se ha de entender la ciberseguridad como aquella del sistema de sistemas, y no la de un simple sistema como hasta ahora.

Dicha operativa del Sistema de Sistemas se articula, a nivel de ciberseguridad al menos, en el pilar de la Combat Cloud. La Combat Cloud tiene como uno de sus principales objetivos, garantizar la sincronización y seguridad de la información y recursos a través de un campo de batalla distribuido y en red. Como se podrá uno imaginar, los requisitos técnicos que emanan de la afirmación anterior suponen un cambio de paradigma en el concepto de operativa de la ciberseguridad de una misión de combate aérea. Es más, hay que tener en cuenta que no solo cambia el hecho de añadir y conectar multitud de nodos de forma dinámica al sistema en red, sino que, además, la jerarquía y roles de gestión puede ir mutando y reaccionando a las amenazas del campo de batalla, tanto físicas como digitales, aumentando considerablemente la complejidad de gestionar la ciberseguridad del sistema de sistemas.

Y todo esto, teniendo en cuenta que el IOC del NGWS, *initial operational capability*, se espera para el 2040. Por esta



En FCAS es fundamental diseñar ahora una arquitectura de ciberseguridad abierta y modular, capaz de no solo actualizar componentes Core, sino además, remplazarlos completamente si fuera necesario

razón, la realidad es que el detalle de las amenazas ciber a las que pueda estar expuesto el FCAS son pues completamente desconocidas, y sus retos, por tanto, basados en la proyección y prospectiva tecnológica. ¿Se puede uno imaginar el que alguien concibiese la seguridad y respuesta ante amenazas en el 2001 para cubrirnos en el 2021?

Ante este panorama de incertitud tecnológica a 20 años vista, el concepto de modularidad tecnológica y arquitecturas marco de seguridad ganan un peso aún mas relevante. Se presupone que ciertas tecnologías Core, y componentes clave de una solución de ciberseguridad, irán evolucionando entre el 2021 y el 2040, ya sea de forma incremental, evolutiva o radical. Se trabajará bajo la hipótesis que los bloques tecnológicos serán remplazados, con una especial relevancia en los bloques de ciberseguridad. Para ello, es fundamental diseñar ahora una arquitectura de ciberseguridad abierta y modular, capaz de no solo actualizar componentes Core, sino además, remplazarlos completamente si fuera necesario.

A modo de ejemplo, si bien la computación cuántica de propósito general para atacar un eslabón de la seguridad no es técnicamente factible a enero de 2021, no cabe duda de que lo será en el 2040. Lo mismo ocurre con los vectores de ataque basados en la convergencia Cyber e Inteligencia Artificial, o inyección de código malicioso en el entrenamiento de redes neuronales; Uno se puede imaginar que existirán, pero a día de hoy se desconocen todos sus efectos o lo que es peor, todos los potenciales vectores de ataque.

Sin ir más lejos, un buen ejemplo de la convergencia tecnológica para crear vectores de ataque impredecibles tuvo lugar el año pasado, en donde unos investigadores, *Light Command*, demostraron que con un telescopio y un puntero laser corriente conectado a un ordenador se podía acceder a una vivienda con un sistema de demótica avanzado..