FARO DE VIGO
MARTES, 27 DE OCTUBRE DE 2015

CLUB FARO DE VIGO

Suárez: "El crimen a través de internet es algo de lo que difícilmente nos libramos"

"La privacidad es cosa del pasado", dice el experto en tecnología ▶ "Los ciberataques se mueven a la velocidad de la luz y no tienen fronteras" ▶ "Cambia el concepto de guerra"

F. FRANCO ▪ Vigo

"El crimen a través de internet es algo de lo que difícilmente nos podemos defender", dijo ayer en el club FARO Alejandro Suárez Sánchez-Ocaña, refiriéndose evidentemente al crimen como delito grave y no en el sentido "sanguíneo" que le otorga mucha gente. "El quinto elemento: ciberespionaje, ciberguerra y terrorismo" fue el título de una charla sorprendente en sus contenidos, que le presentó el periodista de Onda Cero Rubén Rey.

Antes de entrar en materia, Suárez, consejero delegado del grupo Gestiona, expuso cuatro casos paradigmáticos, el primero de ellos como antecedente de este mundo sofisticado de las redes digitales en las que ahora parece jugarse la partida: los papeles del Pentágono, Wikileaks, el caso Snowden y y el que en España vino en llamarse el caso de Superlópez, ese gran ejecutivo que con su paso de General Motors a Volswagen desencadenó una guerra encendida de ámbito judicial -pero no solo- con el espionaje económico e industrial como objeto de litigio.

Su libro reciente en la editorial Deusto, "El quinto elemento", sustenta una idea básica que ayer expuso: "Ante el poder creciente de ese quinto elemento que son las tecnologías digitales, la privacidad es definitivamente cosa del pasado y la seguridad de las personas podría verse comprometida por culpa de esa misma tecnología que nos maravilla. Entramos en una guerra fría tecnológica ante dos bloques: los que usan la tecnología para el bien y los que se apoderan de dichos avances para el mal creando nuevos problemas que no estaban en nuestra hoja de ruta".

Alejandro Suárez (derecha) fue presentado por el periodista de Onda Cero Rubén Rey. // Ricardo Grobas

Público en el auditorio vigués del Areal para asistir a la charla sobre redes y crimen. // Ricardo Grobas

Papá Estado no puede

Sobre el espionaje económico e industrial empezó diciendo que," si el espionaje siempre existió, el gran cambio que aporta la era cibernética es que permite que sea masivo, sin apenas coste y sin riesgos. Contó el caso de la importantísima empresa de seguridad Telvent en Madrid, en la que se infiltraron los chinos interceptando las comunicaciones de las redes internas desde una simple furgoneta aparcada en sus cercanías quizás para robarle datos de índole económica. "Papá Estado -dice Suárez- no tiene la capacidad de proteger a todas sus empresas de ataques exteriores que pongan en riesgo el sistema y por eso es acuciante que cada país cree un tejido de empresas de seguridad informática muy dotadas tecnológicamente para defenderse de intromisiones informativas como las de Echelon, que recopila informaciones económica s sobre empresas que luego facilita a compañías norteamericanas para favorecer su posición en el mercado global". En este caso que cuenta Suárez podríamos hablar de un espionaje con fines patrióticos pero en este escenario están también los que venden información a la competencia o los que piden un rescate a una cuyo acceso les han vetado. "¿Qué empresa no va a pagar para poder seguir funcionando", dice el experto.

> "El ciberterrorismo busca con las redes adeptos y modos de financiar su causa"

Y entró específicamente en el significado del cibercrimen. "Consiste en el uso de herramientas digitales para cometer algún tipo de actividad ilegal, es decir, de ciberataques, que se mueven a la velocidad a la luz y no se detienen ante fronteras físicas o políticas. El robo, por ejemplo, por Internet y con virus, no tiene porqué contentarse con una persona sino que puede ser masivo".

¿Y el ciberterrorismo? Tras poner varios ejemplos como en Irak, donde varios soldados se fotografiaron ante helicópteros de última tecnología que fueron localizados -geolocalización- y destruidos, dijo que las redes sociales deben ser usadas con cabeza porque, si le ocurre al ejército, qué no podrá ocurrir con Facebook y Twitter a donde particulares suben sus datos y fotos todos los días. "Uno de los usos más importantes que organizaciones armadas como el Estado Islámico da a la red busca la captación de adeptos a su causa, así como fondos para financiarla. En Europa, el número de tarados mentales que se suman al ISIS es alarmante".

¿Y la ciberguerra? "Siguiendo a Clausewitz -dice Suárez- la guerra debe ser sangrienta pero las nuevas tecnologías nos llevan a una transformación del concepto de guerra y de ejércitos. Tal vez estemos entrando en una nueva guerra fría tecnológica, tanto por el carácter remoto de los ataques como por el hecho e que pueden ser llevados a cabo sin necesidad de disparar una sola bala. El hecho de que una guerra digital no haya sido declarada no significa que no se esté librando. Y resulta de todos modos cuestionable que la ciberguerra no implique violencia o que no vaya a implicarla muy pronto".

"Una nueva contienda mundial comenzó"

En su libro de Deusto, "El quinto elemento", una idea central: los clásicos hablaban de cuatro elementos: tierra, agua, fuego y aire, así como de un quinto invisible, el éter. Estos cuatro elementos son también las cuatro divisiones de los ejércitos, a los que ahora se añade un quinto elemento: el ciberespacio (también, como el éter, invisible y casi indetectable). "Una nueva contienda mundial ha comenzado -dice Suárez- y todos somos soldados en las trincheras. El nuevo gran conflicto internacional trasciende las fronteras físicas y se libra simultáneamente en cientos de países. El nuevo escenario de la lucha son las redes digitales, el ciberespacio y el iceberg de la gran Internet oculta que no conocemos".

"El desarrollo tecnológico y la sofisticación de las herramientas digitales han convertido a Internet en el campo de batalla más grande que ha conocido el hombre y sus consecuencias son todavía imprevisibles, incalculables. La web ya no es la manzana mordida de Apple sino la manzana podrida. Quien domine la información y la sociedad interconectada controlará el mundo", afirma. ¿Qué papel tienen en ello los gobiernos mundiales, con agencias como el CNI español o la NSA estadounidense? ¿Cómo aprovechan este nuevo escenario criminales y terroristas? ¿Qué papel tienen las empresas y cómo se aprovechan o se defienden de ellos, según los casos? ¿Puede un ataque informático sembrar el caos y provocar un desplome económico mundial? ¿Son tus datos sólo tuyos o hay quien puede utilizarlos en tu contra? Espionaje de las telecomunicaciones, control de las agencias a sus propios ciudadanos, ciberataques y competencia empresarial, ciberterrorismo... de eso habló ayer y habla su libro.