Más madera...

Luis Fernández Delgado
Editor
lfernandez@codasic.com

A contracorriente de la cruda realidad, o quizá ajeno a ella, un interviniente en el RootedPanel convocado por SIC en el multitudinario RootedCON en marzo pasado, aseveró que todo buen hacker, lo que tenía que hacer era centrarse única y exclusivamente en su 'código'. Y punto. En su onanista y 'tierna' visión, lo correcto era negarse a involucrarse en el maquiavélico ciberentorno dibujado en el debate, que planteaba la cruda necesidad de que actores decisivos de la sociedad civil –países, gobiernos, corporaciones, ciudadanos– necesitasen superexpertos debidamente formados y capacitados –a modo de sofisticados "ciberfrancotiradores"– para emprender acciones ofensivas que eventualmente pudieran requerirse por altercados de toda índole en el asilvestrado mundo digital actual.

Lamentablemente, frente a esta acomodada y acaso utópica visión del susodicho, que se repantinga en la filosofía de los tres monos sabios (tan sordos, ciegos y mudos ellos) y proclama la buenista bondad del no intervencionismo, emerge metafóricamente la aseveración gallega de que "…haberla, hayla" y que, por tanto, no valen actitudes de brazos cruzados, de Love & Peace revestida de hierba californiana. La fatídica y compleja realidad sí existe, guste o no guste; no es cómoda y es un deber afrontarla.

En diversas páginas de esta revista se atisban hechos fácticos que lo corroboran. Así por ejemplo, es de resaltar el denominado Manual de Tallín 2.0, por el que más de 50 estados han colaborado en la elaboración de un documento que examina cómo poder aplicar las normas existentes en el derecho internacional en casos de conflicto y guerra cibernética. Este proyecto desgranará el marco jurídico internacional que se aplica a este tipo de conflictos cibernéticos. Una tarea colosal, nos tememos.

En cuestiones más pragmáticas la era Obama va a dejar un desorbitado legado. De cara a 2017 EE.UU. dotará a su programa de ciberseguridad nada menos que de 19.000 millones de dólares (un incremento de 5.000 millones frente al consagrado en el año anterior); y de esa cantidad 62 millones se destinarán a ampliar los esfuerzos para atraer y retener a profesionales cibernéticos cualificados que trabajen para el gobierno estadounidense.

Al tiempo, Estados Unidos ha anunciado la reestructuración de su Agencia Nacional de Inteligencia con un flamante -y opaco- proyecto bautizado como NSA21 a "fin de dotar a la Agencia de los mejores recursos para hacer frente a cualquier amenaza cibernética que ponga en peligro la seguridad nacional". Como anécdotas complementarias a estas acciones cabe señalar que la propia Casa Blanca, por fin, ha decidido contratar a un CISO antes de la llegada del verano. Asimismo, en marzo pasado hasta el mismísimo Pentágono invitó a hackers a atacar sus páginas web para comprobar y mejorar la ciberseguridad de sus infraestructuras.

Por su parte, ha trascendido por fuentes cercanas a su Ministerio de Defensa que su oponente histórico tradicional, Rusia, dispondría de una inversión de entre 180 y 250 millones de euros destinada expresamente a fortalecer sus capacidades ofensivas de ciberseguridad.

> "A nadie se le escapa que los vaticinios de una abultada demanda de especialistas en ciberseguridad –con pericias más o menos sofisticadas– es innegable. Los guarismos van del millón a los seis millones de expertos a nivel mundial de aquí a un lustro. Tal es la previsión que a las fuentes habituales de suministro de formación se vienen sumando otros agentes con recorrido, acaso incluso con una visión más pragmática".

Sin ir más lejos, ya están a la vuelta de la esquina las II Jornadas de Mando Conjunto de Ciberdefensa español, cuyo evento a finales de mayo en Madrid está concitando gran interés por abordar el estado del arte de las operaciones militares en esa nueva dimensión bélica que es el ciberespacio.

A nadie concernido se le escapa que los vaticinios de una abultada demanda de especialistas en ciberseguridad –con pericias más o menos sofisticadas– son un hecho innegable. Los guarismos van del millón a los seis millones de expertos a nivel mundial de aquí a un lustro. Tal es la halagüeña previsión que a las fuentes habituales de suministro de formación (universidades, másteres y organismos trasnacionales de impartición técnica) se vienen sumando otros agentes con recorrido, acaso incluso con una visión más pragmática. Me refiero a las compañías consultoras, prescriptoras e integradoras con pedigrí en seguridad y los propios líderes de la industria de proteccion TIC. Para muestra unos botones: de aquí, las propuestas de Deloitte CyberSOC Academy, S21Sec, S2 Grupo, Alhambra-Eidos o la Cyber Academy de SVT; y de acuyá: la Fortinet Network Security Academy, que anticipa un tsunami de equiparables en este epígrafe.

Llegados a este punto a un servidor le viene a la mente Groucho Marx y sus estrambóticos camaradas de sangre entonando el emblemático "…¡Más madera!" en la mítica "Los hermanos Marx en el Oeste". Como esa hilarante familia, esta sociedad, la que nos ha tocado, la nuestra, parece irremediablemente dispuesta a zambullirse en la vorágine digital con los machos poco atados, alimentando la locomotora de su desbocado tren, que traquetea inconsciente y utópicamente feliz hacia el salvaje oeste digital, ajena a los demonios que ella misma ha desatado: una nueva carrera armamentística, ahora en modo ciber, que –nos guste o no– ya es imparable y no es solo defensiva. Quizá ese sea el precio a pagar por haber consentido la construcción de un apabullante mundo conectado sin railes. ●