El caos informático del WannaCry: haciendo de la necesidad virtud

Félix Arteaga | Investigador principal de Seguridad y Defensa, Real Instituto Elcano. Dirige el Programa de Ciberpolítica | @rielcano

No es necesario volver a describir el **caos informático** que han padecido servicios públicos, empresas y usuarios particulares de medio mundo cuando han visto sus archivos bloqueados y secuestrados hasta el pago de un rescate. No es algo nuevo ni inesperado porque la comunidad de ciberseguridad ha venido alertando de la aparición de *software* destinado a encriptar archivos para pedir rescates (*ransomware*) y a infectar a dispositivos cuyos sistemas operativos fueran vulnerables. Advirtieron de la aparición de ***Cryptolocker*** en 2013 y de la multiplicación exponencial de variantes desde 2015 con fines de extorsión. Se esperaba, algo parecido a lo ocurrido el pasado viernes 12 de mayo, aunque el ***WannaCry*** ha alcanzado una mayor dimensión debido al elevado número de sistemas operativos Windows sin protección actualizada. Gracias a esa advertencia, y a las medidas de ciberseguridad adoptadas en los últimos años, el caos registrado un viernes no se ha convertido en el "lunes negro" ni el fallo sistémico que auguraban los medios de comunicación durante del fin de semana. Desde luego se han visto afectados los ordenadores vulnerables, pero administraciones y empresas han podido mantener los sistemas y servicios que tenían debidamente protegidos.

En **España** no se ha producido ninguna situación de caos informático porque los responsables de la ciberseguridad del Centro Nacional de Inteligencia, del Centro Criptológico Nacional, del Departamento de Seguridad Nacional, del Centro Nacional de Protección de Infraestructuras Criticas (CNPIC) o del Instituto Nacional de Ciberseguridad (INCIBE), entre otras tantas administraciones del Estado han elaborado y aplicado las medidas preventivas derivadas de las estrategias y planes sectoriales de actuación. Tampoco se han venido abajo las redes y servicios de los grandes operadores privados de infraestructuras críticas, gracias a sus responsables, técnicos y medidas preventivas de ciberseguridad. Sin los anteriores, el efecto hubiera sido mucho mayor y la resiliencia, la vuelta a la normalidad, menos eficaz y rápida.

Sin embargo, y ahora que no ha pasado todo lo que se temía pudiera ocurrir, conviene recordar que los responsables y técnicos anteriores han tenido que enfrentarse en el pasado a un muro de ignorancia e incomprensión cuando han elevado sus preocupaciones a los distintos Gobiernos o a los consejeros delegados de las empresas. Estos han subestimado sistemáticamente un riesgo recién llegado que no comprendían y que no quieren reconocer ante sus electores o clientes para no revelar la inseguridad que ofrece el ciberespacio. Con estrategias de comunicación basadas en el "no se preocupen que aquí está el Estado para protegerles de todo" o en "esto no va a ocurrir en mi empresa", administraciones públicas y empresas privadas han restado a sus ciudadanos, clientes y empleados la debida diligencia. Sin esa preocupación, y acostumbrados a estar cubiertos de todo riesgo, no es de extrañar la despreocupación

de grandes sectores de la población y de las pequeñas y medianas empresas para protegerse de los **riesgos de ciberseguridad**. Una despreocupación que se torna letal cuando se une a la cultura del todo gratis en la red de los usuarios y a las estrategias de inversiones mínimas de las empresas.

Hacer virtud de la necesidad

Se puede aprovechar la alarma creada para superar algunos de los obstáculos tangibles e intangibles que han ralentizado el desarrollo de la cultura y de la política de ciberseguridad en España. La primera se ha desarrollado bastante, en la medida que se han articulado estrategias, planes, organizaciones y equipamiento para hacer frente a la ciberseguridad por el lado de los riesgos. La segunda está en construcción porque el ciberespacio no sólo ofrece riesgos sino también oportunidades y la gestión de los primeros debe acompañarse de medidas que atiendan a la regulación, transparencia, presupuestación, investigación, desarrollo, innovación, formación, talento y negocio. Este es el enfoque amplio que desarrolla el **programa de Ciberpolítica** del Real Instituto Elcano, tratando de integrar las dimensiones dispersas que condicionan la ciberseguridad y que deben habilitarse si la sociedad española desea progresar hacia su digitalización.

> "(...) es el Gobierno el que tiene desarrollar una política comprehensiva que haga frente a los retos y aproveche las oportunidades."

Hasta ahora se ha considerado que era mejor reducir la transparencia de los incidentes para evitar alarmas sociales innecesarias. Las cifras de incidentes han ido apareciendo pero los indicadores numéricos no tienen cara para los posibles afectados ni suficiente significado para quienes tratan de evitarlos. Iniciativas como la Directiva NIS europea sobre seguridad en las redes y sistemas de información obligarán a informar sobre los incidentes y facilitarán que los responsables y usuarios conozcan los riesgos que corren. También se ha creído que el desarrollo del ciberespacio se encontraba bajo el control de gobiernos y empresas, pero los técnicos y expertos que trabajan para los anteriores se enfrentan cada vez a un mayor número de especialistas que trabajan para el lado oscuro de Internet. Una legión que trabaja para Estados, organizaciones criminales o para ellos mismos poniendo a disposición de cualquiera que pague los medios necesarios para espiar, robar, chantajear, encriptar o sabotear al resto de usuarios.

Los responsables técnicos de la ciberseguridad tienen el reto de seguir concienciando a los usuarios del riesgo que corren, pero es el Gobierno el que tiene desarrollar una política comprehensiva que haga frente a los retos y aproveche las oportunidades. La digitalización de la sociedad y de la economía depende de que el ciberespacio sea seguro y para ello hace falta convicción, presupuestos, investigación, formación, industria, talento y comunicación. Una política que se puede construir desde la gobernanza y la planificación o a golpe de sustos e incidentes como los ocasionados por el *WannaCry*.