La lucha contra el cibercrimen en España afecta a todos

Vivimos en un mundo cada vez más dependiente de la tecnología. El dominio del ciberespacio se ha configurado como una dimensión más de nuestras vidas. Con ciertas particularidades que configuran un conjunto de retos, de amenazas pero, de igual modo, de oportunidades, que debemos enfrentar y aprovechar con el fin de generar valor para toda la sociedad. Esa sociedad que nos provee de servicios, de derechos y que, no lo olvidemos jamás, requiere que afrontemos nuestras responsabilidades para crecer de forma sana y equilibrada.

Sí, el dominio del ciberespacio se encuentra en un periodo de exploración. Aún estamos explorando, como humanidad, qué nos ofrece. Los procesos de toma de decisión en el mismo se caracterizan, por un lado, por su inmediatez y, por otro, por su, cada vez, más extrema complejidad. Mal asunto unir, en un mismo espacio-tiempo, estas dos características. Más aún si introducimos un nuevo elemento distorsionador como es el de su aterritorialidad. Esta característica induce el riesgo adicional de la inaplicabilidad de las leyes nacionales en muchos casos en los que personas o grupos organizados consideran la realización de actividades ilícitas.

Somos conscientes del momento en el que vivimos y, sucesivos gobiernos, de uno y otro signo, han trabajado para dotar a nuestro país de una estructura de toma de decisión adecuada para enfrentar los riesgos que induce el ciberespacio. En un entorno económico caracterizado por la carestía de recursos, se han intentado maximizar los disponibles, con el fin de mantener a nuestro país dentro de los estándares que su posición requiere. De esta forma, tanto el CCN-CERT como Incibe y el CNPIC han desarrollado, a lo largo de los últimos años, un trabajo duro y, a veces, poco conocido, orientado a asegurar la resiliencia de nuestras administraciones públicas, nuestro tejido productivo pyme y nuestras infraestructuras críticas.

Hemos llegado a este momento de nuestra historia con luces pero, sin duda, también con sombras. Por el camino de la crisis económica hemos perdido mucho talento. Talento necesario para poder enfrentar los riesgos y amenazas que se empiezan a dibujar en un nuevo escenario en el que los actores clásicos ya no son los únicos jugadores.

Los Estados, con acciones orientadas a mantener o mejorar su posición geoestratégica; las corporaciones transnacionales, con recursos que superan, con creces, los de muchos de los Estados y que, además, son las detentadoras de las infraestructuras de comunicaciones, de datos, de información, de conocimiento y de inteligencia, finalmente, que configuran nuestro mundo globalizado y cuyos intereses no tienen por qué estar alineados con los de los Estados o los de los ciudadanos de los mismos; los grupos de interés o de acción que, configurados como redarquías, buscan posicionarse u obtener beneficios de forma legal, alegal o directamente ilegal… Todos ellos desarrollan sus actividades en un tablero de ajedrez en el que las dimensiones no son dos, las reglas de movimiento de las piezas no existen y el objetivo último del juego tampoco es demasiado evidente, si es que, en realidad, es posible señalarlo.

Los procesos de toma de decisión son cada vez más complejos poniéndose fuera del alcance de las capacidades del ser humano y trasladándose, cada vez más rápidamente a la acción de algoritmos que, de forma inexorable, se van cargando de inteligencia para ese proceso de toma de decisión que ha de ser en tiempo real.

Se abren, como vemos, nuevos perímetros de defensa que ya no solo afectan a elementos técnicos o tecnológicos sino que impactan, y de qué manera, en los procesos de toma de decisión automatizados.

Si hace pocos años teníamos que defender un perímetro más o menos estático en el

Enrique Ávila Gómez, Director del Centro Nacional de Excelencia en Ciberseguridad

que los dispositivos eran el núcleo de esa defensa, ahora nos encontramos con la desaparición de un perímetro identificable y donde estos mismos escenarios son híbridos.

Derechos y libertades

El ser humano se convierte, de esta forma, en el sujeto más vulnerable e incontrolable dado que, a menudo, entran en juego derechos y libertades del mismo a los que no podemos (ni debemos) renunciar en nombre de la seguridad. Debemos de aquilatar el riesgo en función de la pérdida de libertad y asumir parte del primero si queremos mantener una sociedad sana que no se eche en brazos de una seguridad completa a la que, en ningún caso, se puede acceder.

Ello no impide que debamos introducir mejoras en nuestros sistemas de seguridad con el fin de minimizar los riesgos señalados y, sobre todo, trabajar en la mitigación de los efectos que pudieran derivarse de un ataque con éxito contra una empresa o una institución.

Trabajar en la monitorización y la trazabilidad es fundamental a la hora de poder determinar el responsable de una acción ilícita sobre o contra nuestros sistemas. Resulta clave prestar atención a estas dos dimensiones de la seguridad, a menudo dejadas de lado frente a otras.

Del mismo modo, habremos de trabajar en el despliegue de tecnologías que aseguren la transparencia y la trazabilidad en los procesos de toma de decisión, de tal manera que seamos capaces de dotarnos de un conjunto de medidas de autocontrol sobre nuestra vida desarrollada en el dominio del ciberespacio. Solo de esta manera, seremos capaces de poner las cosas más difíciles a todos aquellos actores que intenten aprovecharse de nuestras vulnerabilidades, tanto individuales como colectivas.

Acciones políticas determinantes que mejoren nuestras capacidades como sociedad que se desarrolla, cada vez más, en el dominio del ciberespacio. Por supuesto asignando recursos, tanto de talento como económicos, suficientes para poder enfrentar todos los riesgos señalados y mitigar, en la medida de lo posible, el posible impacto de las amenazas.

Todas estas medidas han de ser puestas en práctica con urgencia. Sin miedo a equivocarse o a no resultar eficientes porque, lo que en realidad necesitamos, como sociedad, es que sean eficaces. Y que lo sean como proyecto transgeneracional.

Pero no olvidemos nuestra responsabilidad individual dentro de un colectivo como es la sociedad en la que desarrollamos nuestro modelo de vida. Tenemos que invertir. Nuestro tiempo, nuestros recursos y nuestro talento, con el fin de conseguir que, entre todos, mujeres y hombres, nos desarrollemos, de forma sana, como sociedad avanzada. No podemos hacer dejación de nuestra responsabilidad como ciudadanos en esta materia. El Estado no tiene los recursos suficientes para asegurar, por sí solo, este desarrollo ordenado y generador de riqueza para toda la sociedad.

Cada uno de nosotros, personas físicas y jurídicas, somos responsables de nuestra parcela en materia de ciberseguridad.

No podemos ver como un gasto esta asignación de recursos sino como una inversión. Una importante inversión de futuro.

Como hemos mencionado antes, un proyecto transgeneracional. Hemos olvidado lo que esto significa, pero es importante. Y podemos recordarlo. Hace no tanto tiempo construíamos catedrales… Y ello significaba que una sociedad tenía un proyecto común a largo plazo. El ciberespacio nos brinda, de nuevo, la posibilidad de trabajar en el sentido antedicho. ¡Aprovechémoslo! ■