¡Es la atribución, estúpido!

Luis Fernández Delgado
Editor
lfernandez@codasic.com

Hace algo más de un año, concretamente el 13 de febrero, el presidente estadounidense Barack Obama dijo durante un discurso en la Universidad de Stanford que "el mundo Ciber es el Salvaje Oeste". En consonancia con los desórdenes, el desmadre legal y el terror que los forajidos e indios de por entonces causaban –a ojos de los conquistadores del Far West, claro–, un senador USA acaba de formular a la Administracion Obama hace escasas semanas una pregunta interesante: ¿Cuál es la definición exacta de un "Acto de guerra" cíber?

La cuestión, nada trivial por cierto, instaba a que cuando desde presidencia se tuviera a bien responderla, la respuesta arrojara luz nítida sobre la manera en que un ciberataque se manifiesta, su alcance significativo, intensidad y duración, y si sus efectos pudieran ser equivalentes a los derivados de un ataque que utilice armas convencionales y provoque destrucción física, daños colaterales y cause bajas.

Mike Rounds –que así se llama el inquiridor– también puntualizó que la legislación debería requerir del ejecutivo que definiera cuáles de estas acciones constituirían un acto de guerra ciber, lo cual permitiría al ejército USA estar en mejor disposición para responder a los ciberataques y detener en etapas tempranas cualesquiera intentos de agresión cibernética.

A finales de febrero Noruega acusó oficialmente a China de haberles robado secretos militares y de que esta información confidencial estaba siendo ahora utilizada por el ejército chino. Respecto a la autoría el teniente general Morten Haga –responsable de la agencia de Inteligencia noruega E-tjenesten– se guardó muy mucho de precisar que fueron "treats actors in China" y no especificó las compañías afectadas ni qué secretos les fueron sustraídos.

A la hora de cierre de esta edición al senador Rounds, miembro del Comité de Servicios Armados del propio Senado y formulador de la espinosa cuestión, aún no se le había respondido.

La verdad es que la pregunta tiene su aquel, mayormente por un tema crucial: el de la **autoría**. Viene aquí a colación la famosa frase gestada y usada en el periodo electoral de la etapa Clinton cuando se utilizó aquello de "Es la economía, estúpido". Trayéndola a nuestro terreno sería "Es la atribución, estúpido".

Abundando en ello precisamente, a finales de febrero Noruega acusó oficialmente a China de haberles robado secretos militares y de que esta información confidencial estaba siendo ahora utilizada por el ejército chino. Con todo, respecto a la autoría el teniente general Morten Haga Lunde –responsable de la agencia de Inteligencia noruega E-tjenesten– se guardó muy mucho de precisar que fueron "treats actors in China" y no especificó las compañías afectadas ni qué secretos les fueron sustraídos.

Y llegamos a España. Con un balance absolutamente satisfactorio concluyeron a finales del mes pasado las II Jornadas de Mando Conjunto de Ciberdefensa, un evento que concitó grandísimo interés por abordar el estado del arte de las operaciones militares en esa nueva quinta dimensión bélica que es el ciberespacio. En el jugoso programa, se incluyó acertadamente una sesión centrada en "El derecho en las operaciones militares en el ciberespacio, Manuales de Tallín y reglas de enfrentamiento".

Sus participantes, gente versada en lo legal y con bagaje en los frentes internacionales, abordaron este crucial tema, evidenciando los distintos avances de los agentes institucionales y privados en cómo poder aplicar las normas existentes en el derecho internacional en casos de conflicto o en guerra cibernética, y poniendo de manifiesto la extrema dificultad de avanzar consensuadamente a la hora de atinar con el "quid" del meollo: la atribución, auténtico quebradero de las cabezas pensantes a la hora de perfilar y sistematizar el proceder y la proporción ante altercados cibernéticos en los que la autoría debería quedar fehacientemente demostrada y, por ende, su eventual respuesta, llevada a cabo en tiempo próximo al real. Colosal empeño parece a la luz de lo que se dijo.

Así, el representante de la OTAN Vincent Roobaert, de la que es asesor legal en la Agencia de Comunicaciones e Información (CNIA), puso foco en los espinosos aspectos legales relacionados con el derecho de uso de la fuerza en relación con ciberataques (*ius ad bellum*) y en los relativos a la conducta de las ciberoperaciones (*ius in bello*).

De especial interés fueron también las aportaciones de Ana Pilar Velázquez, de la Asesoría Jurídica del Cuartel General de la Armada española, quien puntualizó que, hasta el momento, no hay consenso internacional sobre lo que es una violación de la soberanía ni tampoco de cuál es el umbral de daño a partir del cual podría considerarse una acción objetable.

Igualmente, fue de extremo interés saber que Naciones Unidas no puede intervenir en asuntos que se consideran de jurisdicción interna de cada país y que solo existirá responsabilidad del Estado si puede atribuirse de facto a un Estado; de la misma forma, será asimismo atribuida si es realizado por un órgano del Estado.

Con todo, es determinante la comisión de un acto en aparente función oficial, ya que puede haber entidades privadas que cuenten con la autorización de un Estado para actuar, de modo que sus actos serían atribuibles a dicho Estado. De la misma manera, cuando un Estado no tenga recursos ni capacidad para desarrollar las ciberoperaciones, y encomiende dicha tarea a grupos o personas privadas, en tal caso, esa actividad también será atribuida al Estado. Por último, las ciberoperaciones conducidas por un órgano estatal –puesto a disposición de otro– serían asimismo atribuidas a este último y en el caso de que un agente no estatal participase en un conflicto armado, a través de ciberoperaciones, se le aplicaría el Derecho Internacional Humanitario.

Ante este berenjenal de frágiles certezas, no queda otra que seguir hacia adelante echando mano de lo poco que hasta ahora viene funcionando: el consenso y subsiguiente convenio –como ya sucediera en los precedentes ámbitos de lo nuclear, biológico, ecológico…–. Quizá proceda acudir a una de nuestra plumas más sabias, la de aquel que visionariamente plasmó –llevándolo a nuestro terreno– lo de que "(Ciber)caminante no hay camino, se hace (ciber)camino al andar". Sea. ●