La dimensión internacional de la ciberseguridad

Félix Arteaga | Investigador principal de Seguridad y Defensa, Real Instituto Elcano | @rielcano

Dentro de la acción exterior de los Estados, se pueden tener dos enfoques de la dimensión internacional de la ciberseguridad: uno vertical, en el que cada actor proyecta su actuación hacia el ámbito global, y uno transversal, en el que se integran todos los ámbitos verticales antes de proyectarlos hacia el exterior. Adoptando uno u otro enfoque, los gobiernos pueden elegir entre que cada actor público y privado internacionalice su proyección individualmente o coordinar esas proyecciones de forma que añada valor y economía de escala a su acción exterior.

En la Estrategia de Acción Exterior de febrero de 2015, el Ministerio de Asuntos Exteriores y Cooperación no optó por ninguna de los dos enfoques porque no consideró la ciberseguridad como una dimensión de esa acción exterior. Siendo la ciberseguridad una política pública recién llegada a las responsabilidades del Gobierno, no es de extrañar que no se tuviera en cuenta suficientemente su **dimensión transversal sobre la acción exterior** y que se considerara suficiente la designación de un Embajador en Misión Especial para la Ciberseguridad. Por defecto, se entiende que la responsabilidad de coordinar transversalmente la ciberseguridad recae sobre el Comité Especializado de Ciberseguridad, según se reconoce en la Estrategia de Ciberseguridad Nacional de 2013, y con un enfoque transversal ya que se le encomienda la coordinación de las Administraciones públicas y los sectores privados tanto en el ámbito nacional como en el internacional.

La dimensión internacional se orienta a desarrollar la participación española en la coordinación internacional, en las funciones de regulación multilateral, la armonización de estándares técnicos o la cooperación policial y judicial, entre otras, para fomentar un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales. Esos intereses nacionales se definen hasta ahora por varios actores públicos de la Administración, particularmente los que están más implicados en la protección contra los riesgos y amenazas de la ciberseguridad nacional. Pero existen otros intereses asociados con la economía, la industria, la tecnología y el uso social del ciberespacio que afectan a otros actores privados y que se internacionalizan de forma autónoma. No todas las proyecciones públicas y privadas de la ciberseguridad afectan de igual manera a la seguridad nacional o a la acción exterior, por lo que no resulta necesario coordinar todos los procesos de internacionalización. Pero sí que resulta conveniente identificar, coordinar y supervisar transversalmente aquellos procesos de internacionalización relevantes para la sociedad, sean públicos o privados. Una situación que debería revertirse en la próxima estrategia de ciberseguridad nacional.

En Holanda, su Estrategia Internacional de Ciberseguridad de 2017 reconoce que el Estado comparte intereses, riesgos y retos con el sector privado, la comunidad tecnológica, el mundo académico y las organizaciones no gubernamentales, por lo que

su acción internacional debe articularse sobre un modelo consultivo en el que todos los actores mencionados definan conjuntamente la estrategia a seguir. Este enfoque integral lleva la coherencia hasta el extremo de que no se asumen compromisos internacionales sobre los que no exista suficiente consenso interno. La coherencia es comprensible en la medida que los acuerdos internacionales generan costes y obligaciones para los sectores privados que, en contrapartida, deben participar en el sistema de decisiones desde el inicio. Es el mismo enfoque "transparent, bottom-up, consensus-driven processes whereby governments, the private sector, civil society and the technical community all participate on equal footing" que contienen las Recomendaciones al Presidente de la Oficina del Coordinador para Asuntos de Ciberseguridad de los Estados Unidos para proteger los intereses de ciberseguridad estadounidenses a través de la cooperación internacional.

Los **modelos de gobernanza** actuales varían en función de la dimensión internacional de cada país. Entre las grandes potencias, como los Estados Unidos, Rusia o China, la centralización de los grandes coordinadores sectoriales: defensa, seguridad interior o inteligencia se realiza mediante los grandes consejos de seguridad nacional. En las potencias intermedias, donde las obligaciones internacionales no son tan elevadas, la integración precisa una estructura de agencia permanente que ayude a la autoridad nacional de ciberseguridad a garantizar la continuidad entre el nexo externo e interno de la ciberseguridad.

En **España**, aprovechando la necesaria revisión de la Estrategia de Ciberseguridad Nacional, se debería reforzar la coherencia del enfoque integral del Sistema. Por un lado, esa nueva Estrategia deberá reflejar de forma más explícita su dimensión internacional, no como un objetivo o principio genérico, sino como una estrategia bien elaborada en la que se relacionen objetivos, actores y medios. Precisa un plan de actuación que la desarrolle y, sobre todo, una autoridad que vele por su cumplimiento. Hasta ahora, la autoridad rotatoria entre los actores gubernamentales o delegada en el Centro Nacional de Inteligencia ha servido para coordinar transversalmente los aspectos de ciberseguridad asociados al núcleo duro de la seguridad nacional, asegurando la protección de las infraestructuras críticas y servicios esenciales para la sociedad. Sin embargo, ese modelo de coordinación no parece adecuado para afrontar el crecimiento exponencial y disruptivo que se registra en todos los ámbitos de ciberseguridad.

"Mantener el modelo basado en los decisores gubernamentales de seguridad conllevaría el riesgo de primar el enfoque de seguridad sobre el resto de enfoques económicos, políticos y sociales"

Por un lado, se entra en una nueva fase en el que las decisiones sobre actuación, regulación e inversión se alejan de la seguridad nacional para adentrarse en la seguridad económica donde no es preciso un nivel de intervención gubernamental tan elevado porque los intereses a proteger ya no afectan a toda la sociedad. En consecuencia, el **ecosistema no gubernamental** deberá tener más protagonismo e influencia en el nuevo modelo de gobernanza porque es el que mejor conoce el contexto e implicaciones de las decisiones sobre seguridad. Mantener el modelo basado en los decisores gubernamentales de seguridad conllevaría el riesgo de primar el enfoque de seguridad (segurizar) sobre el resto de enfoques económicos, políticos y sociales, por

lo que la participación privada debe superar el estadio opcional actual y convertirse en un actor de pleno derecho.

Aparte del reconocimiento de la naturaleza público-privada de la ciberseguridad, sería conveniente reconocer su carácter transversal designando una autoridad, coordinador o comisionado que no pertenezca a los compartimentos verticales ministeriales o de las agencias actuales. Para desempeñar sus funciones de integración, esa figura (Sr. o Sra. CIBER) debería contar con una estructura permanente de trabajo, lo que en tantos países se denomina como agencia y que aquí debería tener las mismas funciones pero distinta denominación por razones de cultura administrativa. Articulando de este modo el núcleo interior de la ciberseguridad, se podría trasladar a su núcleo externo, europeo y global, los intereses e iniciativas españolas de ciberseguridad, asegurando la coherencia y continuidad entre lo exterior y lo interior y reforzando el papel protagonista en las decisiones (*decision shaper*) frente al de destinatario de las mismas (*decision taker*). El reciente Anteproyecto de Ley para la trasposición de la Directiva NIS atribuye al Departamento de Seguridad Nacional ese papel de "bisagra" entre las dimensiones externas e internas en lo que a la seguridad de las redes y sistemas de información se refiere, pero su implantación plantea reto organizacional para desarrollar tanto esa función como el resto de funciones de coordinación interior-exterior que puedan encomendársele en el futuro. En consecuencia, se debería aprovechar la revisión de la Estrategia para revisar también el Sistema y los procedimientos adecuados para gestionar la creciente dimensión internacional de la ciberseguridad.