Sanciones contra los ciberataques: la UE enseña las uñas

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

El incremento de la cantidad y calidad de los ciberataques amenaza con superar la capacidad defensiva de los actores públicos y privados, por lo que en los últimos años se ha ido abriendo paso la necesidad de contar con instrumentos de ciberdisuasión, para llevar al ánimo de los ciberatacantes la existencia de un riesgo, y de contrataque, para materializar ese riesgo.

"En junio de 2017, la Comisión Europea y sus Estados miembros decidieron poner en marcha un régimen de sanciones diplomáticas disuasorias"

En junio de 2017, la Comisión Europea y sus Estados miembros decidieron poner en marcha un régimen de sanciones diplomáticas disuasorias, el EU Cyber Diplomacy Toolbox, que se ha materializado el 17 de mayo de 2019 con las primeras medidas sancionadoras del Consejo en respuesta a los ciberataques generados fuera de la UE y que puedan tener o tengan un impacto importante sobre la ciberseguridad de la UE (infraestructuras críticas, servicios públicos, elecciones, información clasificada y seguridad interior o exterior) o de Estados y organizaciones internacionales. Las sanciones se enmarcan en la Política Exterior y de Seguridad Común de la UE (artículos 21 y 30 del TUE) y consisten en la prohibición de viajar o la congelación de bienes, entre otras, a quienes realizan o coadyuban a la realización de ciberataques, incluso en grado de tentativa.

La ciberseguridad no cuenta todavía con una regulación específica en el derecho internacional, por lo que la UE trabaja para el desarrollo progresivo de normas voluntarias tanto en Naciones Unidas como en otros foros que permitan trabar su gobernanza en el futuro, como el G20 o el Llamamiento de París para la Confianza y Seguridad en el Ciberespacio. Pero, mientras se trata de llegar a acuerdos vinculantes, los Estados intentan ponerse de acuerdo con otros Estados mediante acuerdos bilaterales o disuadirlos aprobando regímenes sancionadores como el que acaba de adoptar la UE. El Consejo comenzó a muñir sus instrumentos diplomáticos en febrero de 2015, solicitando a las instituciones y Estados miembros en sus "Conclusiones sobre Ciberdiplomacia" que reflexionaran sobre la necesidad de incluir en su acción exterior medidas relacionadas con la regulación internacional del ciberespacio, la protección de los derechos y libertades o la cooperación internacional.

El Consejo no recomendó en aquel momento el desarrollo de medidas sancionadoras, pero esa reflexión inicial condujo a 2017, cuando la Comisión y el Servicio Europeo de Acción Exterior presentaron al Consejo para su aprobación su inventario de medidas diplomáticas de respuesta a ciberataques (Cyber Diplomacy Toolbox). El Consejo, siguiendo el dictamen del Grupo de Expertos Gubernamentales de 2015, consideró

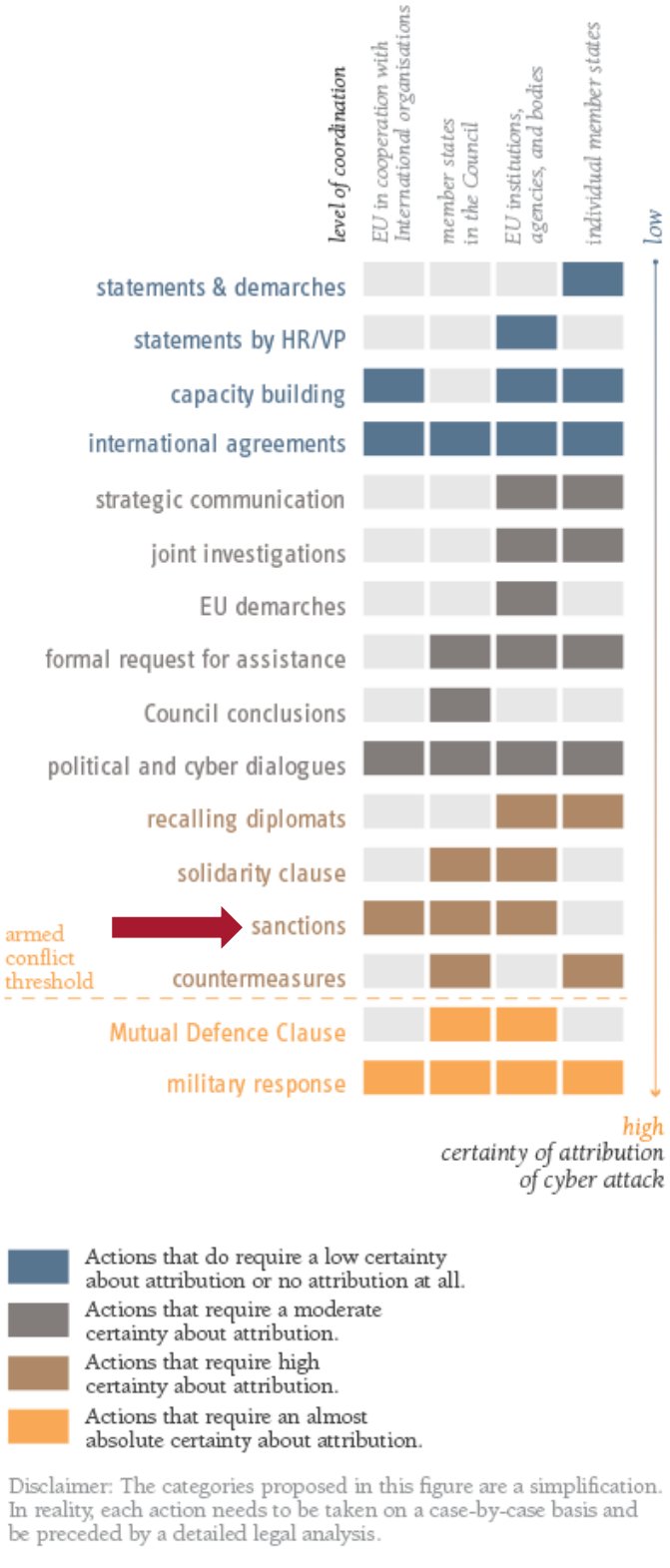
necesario adoptar medidas diplomáticas disuasorias, incluidas sanciones, contra los Estados que llevaran a cabo ciberataques contra la UE desde sus territorios o que consintieran su realización desde los mismos por actores no estatales El Consejo se mostró dispuesto a encajar estas medidas en el derecho internacional aplicable a la ciberseguridad y aplicarlas con todas las cautelas y proporcionalidad posible, pero evitó vincular su aplicación a la atribución previa, ya que algunas medidas diplomáticas no precisaban contar con la certeza absoluta de la atribución para ser disuasorias.

Mientras se desarrollaba este mandato, arreciaron los ciberataques como los del WannaCry o del NotPetya, por lo que el Consejo de Asuntos Exteriores de abril de 2018 condenó su proliferación y reiteró la necesidad de buscar respuestas disuasorias dentro de la PESC, incluyendo sanciones. Los Consejos Europeos de junio y octubre de 2018 reiteraron la necesidad de desarrollar las capacidades disuasorias de la UE para responder a los ciberataques, apelaciones que precedieron a las medidas adoptadas en abril de 2019.

“Los Consejos Europeos de junio y octubre de 2018 reiteraron la necesidad de desarrollar las capacidades disuasorias de la UE para responder a los ciberataques”

Las medidas aprobadas ahora pueden complementarse en el futuro con otras medidas, diplomáticas o no, de la UE o de sus Estados miembros. Esa combinación depende del nivel de atribución que sea posible, porque, cuanta más certeza exista sobre la autoría, más fácil será adoptar medidas de mayor rigor. En la Figura 1 aparece un hipotético inventario en el que se recogen todas las medidas de respuesta posibles frente a los ciberataques, tanto de la UE como de sus Estados miembros, solos o en colaboración con terceros y ordenadas por el nivel de atribución.

Figura 1. Inventario de posibles medidas en respuesta a los ciberataques



Las respuestas en azul son más fáciles de adoptar, porque apenas necesitan atribución. La certeza en la atribución tiene que ser mayor en las respuestas más contundentes (en gris y en marrón) y, sobre todo, para adoptar las medidas que pueden activar las cláusulas de solidaridad y de defensa colectiva de la UE (naranja).

El nivel de las sanciones adoptadas ahora se indica en la Figura con la flecha de color rojo.

Fuente: EU Institute of Security Studies, julio de 2017, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf.

La previsión de estas medidas es necesaria porque las medidas defensivas no bastan para contener la progresión de los ciberataques: se hace necesario que los Estados miembros de la UE adopten, individual o colectivamente, medidas disuasorias que desincentiven la agresión y mitiguen la impunidad con la que se atacan bienes, personas, libertades y derechos a través del ciberespacio. No serían necesarias si existiera una verdadera voluntad de cooperación internacional, pero es difícil que esa cooperación cristalice mientras las grandes potencias del ciberespacio no se vean amenazadas por las mismas capacidades y amenazas avanzadas persistentes que ellos mismos han creado o consentido. Cuanto mejor funcionen estas medidas disuasorias, más difícil será subir por la peligrosa escalera de las medidas de represalia (defensa activa), pero tal y como están las cosas en la ciberseguridad, parece inevitable incluirlas en el inventario de respuesta, tal y como acaba de hacer la nueva Estrategia francesa de ciberdefensa o como lo acaba de anunciar la Estrategia Nacional de Ciberseguridad.