Ciberseguridad: llegan las acciones ofensivas

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

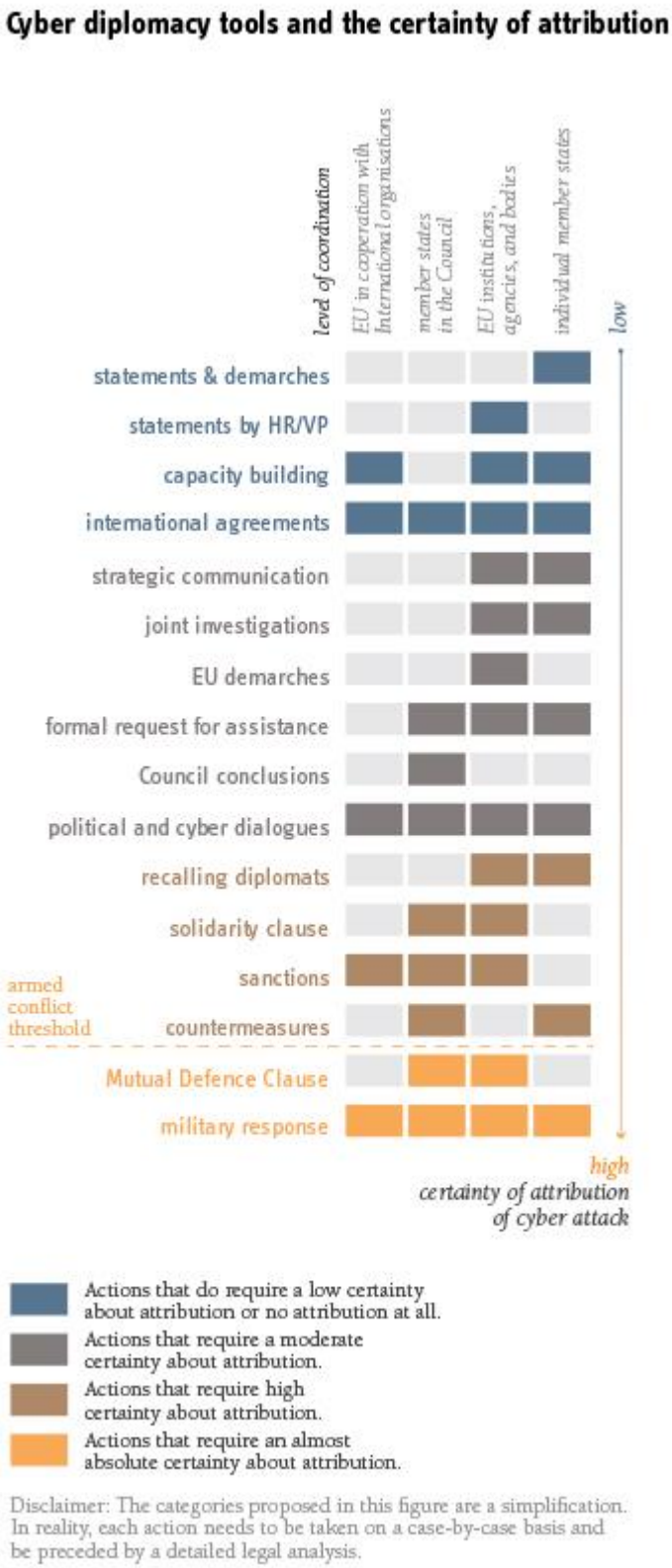
Al principio fueron los virus y los antivirus. Con el desarrollo de Internet llegaron los ataques sobre el tráfico de correos y datos, y aparecieron los sistemas de detección de intrusos (IDS) para detectarlos y los parches informáticos para prevenir las intrusiones. Luego, los ciberataques se aprovecharon de las vulnerabilidades de las *Webs* y de las descargas imprudentes para llevar sus códigos maliciosos a los usuarios. Entonces aparecieron nuevos métodos de defensa contra el *malware* y las corporaciones, públicas o privadas, recurrieron a soluciones integrales y unificadas corporativas o en la nube para protegerse de ataques masivos, rápidos e inteligentes.

"(…) los informes sobre ciberataques muestran que siguen creciendo en calidad y en cantidad, por lo que las medidas defensivas no pueden seguir siendo la única forma de respuesta".

Pese a lo anterior, los informes sobre ciberataques muestran que siguen creciendo en calidad y en cantidad, por lo que las medidas defensivas no pueden seguir siendo la única forma de respuesta. No se trata de ya sólo de prevenir perturbaciones o interrupciones de los servicios públicos o privados que se prestan o de evitar el robo de datos, sino de asegurar la soberanía de los Estados (seguridad nacional) y la continuidad de negocio de sus empresas (seguridad económica). El ciberespacio se ha convertido en un escenario de conflicto y competencia por motivos políticos o económicos. Los ciberataques responden a estrategias de poder, coacción e influencia deliberadas. Se han convertido en las nuevas armas de destrucción masiva o de primer uso que se utilizan como instrumentos de poder estatal o empresarial. Y los responsables ya no son los hackers gamberros o activistas del principio o los grupos criminales que los siguieron, sino actores estatales y no estatales que utilizan los ciberataques para conseguir sus objetivos estratégicos.

Hasta ahora, se han descartado medidas de carácter ofensivo por la dificultad de identificar a los atacantes, la falta de regulación del derecho a la legítima ciberdefensa o los riesgos de la devolución de ataques (*hacking-back*). Pero los estados y las empresas no pueden seguir invirtiendo en medidas reactivas cuando se acumulan las evidencias de que Estados como Rusia, China, Irán o Corea del Norte (por no mencionar al "fuego amigo") utilizan los ciberataques para minar la estabilidad política de sus rivales y competir con ventaja sobre sus competidores. Entidades tan poco agresivas como la Unión Europea han visto cómo Rusia ha utilizado grupos afines para atacar infraestructuras críticas o lanzar campañas de desinformación para alterar el resultado o la normalidad de las elecciones, lo que llevó a incluir en su Diplomacia Digital un conjunto de herramientas para prevenir la impunidad (Cyber Diplomacy Toolkit, CDT). Siendo conjuntas las respuestas, la UE desea contar con un conjunto de medidas que le permitan escalar en ellas desde las declaraciones oficiales hasta la respuesta militar si fuera preciso, pasando por un amplio abanico de medidas que se recogen en la figura 1.

Figura 1. Instrumentos de respuesta ciberdiplomática de la UE en función de la seguridad de la atribución y el nivel de coordinación entre sus Estados miembros



Fuente: Moret, E. & PawlakThe, P. (2017), 'EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?', *Brief Issue 24*, European Union Institute for Security Studies (EUISS).

En el CIBER Elcano de octubre se recogen algunos de los documentos recientes que marcan un cambio desde la postura reactiva y defensiva de Estados y empresas hacia una más proactiva y ofensiva. Destaca la Estrategia de Ciberseguridad de Estados Unidos que reconoce que la disuasión no puede seguir siendo el elemento central de respuesta y es necesario contar con medidas ofensivas. Se pasa de mitigar riesgos y controlar la escalada a aceptar el riesgo de un enfrentamiento para evitar que una postura exclusivamente defensiva incentive los ciberataques. Autorizando las operaciones ofensivas en el ciberespacio y llevándolas al terreno del agresor, Estados Unidos aumenta su capacidad de disuasión, complica el cálculo del riesgo-beneficio del ciberatacante. También se mencionan las denuncias de Reino Unido y Holanda de actividades cibernéticas desarrolladas por Rusia en sus territorios. Una denuncia ante los Ministros de Defensa de la OTAN reunidos en Bruselas el pasado 4 de octubre, que ha llevado al Secretario de Defensa, Jim Mattis, a reiterar su colaboración de asistencia (ahora en "modo" ofensivo).

"Las acciones ofensivas también han llegado al ámbito empresarial porque el coste de la defensa contra los ciberataques no cesa de aumentar, al igual que no dejan de hacerlo las obligaciones de protección que les imponen los gobiernos".

Las acciones ofensivas también han llegado al ámbito empresarial porque el coste de la defensa contra los ciberataques no cesa de aumentar, al igual que no dejan de hacerlo las obligaciones de protección que les imponen los gobiernos. En su informe sobre "Raising the Consequences of Hacking American Companies", el Center for Strategic and International Studies (CSIS) de Washington D.C. reconoce que las empresas privadas no pueden seguir defendiéndose por sí mismas como hasta ahora y que pronto, las capacidades ofensivas de los ciberatacantes acabarán desbordando las medidas defensivas actuales. En consecuencia, se le pide al Gobierno que haga lo que sea necesario para disuadir a Estados como China o Rusia de seguir apoyando ciberataques contra las empresas estadounidenses. En el mismo sentido, el Carnegie Endowment for International Peace revela en el documento "Protecting Financial Institutions Against Cyber Threats: A National Security Issue" la intensidad de los ciberataques que está sufriendo el sistema financiero de los Estados Unidos, el más castigado de todos los que forman parte de las infraestructuras críticas y el más expuesto a un fallo sistémico.

En este contexto de transición desde el delito a la agresión, desde el hackeo ético a las *cyber weapons* y desde los garajes privados a las unidades de ciberinteligencia, la futura Estrategia de Ciberseguridad no puede seguir confiando la protección a la carta única de la defensa. Las actuales líneas de acción de la Estrategia de Seguridad Nacional de 2017 se deben complementar con otras dedicadas que doten de capacidades ofensivas a la respuesta del Estado. El Estado tiene la obligación de hacerlo porque ostenta el monopolio de la fuerza para proteger la seguridad y la prosperidad nacional. Puede hacerlo en colaboración con otros Estados y con el sector privado, pero no puede delegar en ellos su competencia. A pesar de las dificultades y reservas legales, tecnológicas y éticas señaladas, el Estado no puede ignorar que el ciberespacio se encuentra en estado de guerra y que las primeras víctimas en los conflictos cibernéticos son los Estados y las empresas más débiles.