Analisis de la actualidad internacional:

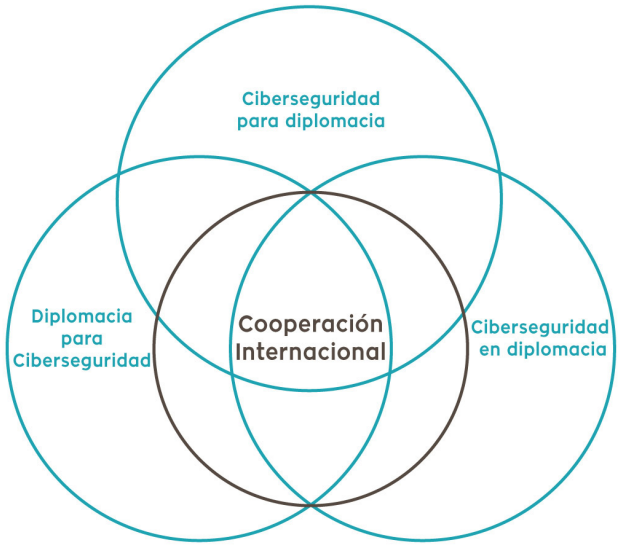
Ciberdiplomacia y diplomacia corporativa: claves para la ciberseguridad

AUTOR: Beatriz Serrano Casas. Analista y consultora en relaciones internacionales. Business Analyst (Ford Credit Europe).

La ciberseguridad es una disciplina de creciente interés debido a la relevancia que ha cobrado Internet y el mundo digital en nuestra vida diaria. El concepto de ciberseguridad engloba la prevención, detección, y respuesta frente a amenazas y ataques. Sin embargo, existe una amplia diferencia en la concienciación y el nivel de conocimiento que se tiene en distintos países sobre las consecuencias de una buena ciberseguridad, la sensibilidad sobre sus impactos en la seguridad nacional o en la vida diaria de sus habitantes.

Es necesario el uso de una gran variedad de medios para que las políticas de ciberseguridad nacional sean efectivas. En este sentido, la diplomacia juega un papel fundamental en la prevención, concienciación y trabajo activo para una ciberseguridad proactiva.

Relaciones entre ciberseguridad y diplomacia



Ciberdiplomacia

Con el progreso del dominio cibernético, se acuñaron términos que en ocasiones se utilizan indistintamente y producen equívocos, lo que dificulta la existencia de una base común que sea útil para la puesta en marcha de las medidas adecuadas. Shaun Riordan, ex diplomático británico y profesor asociado de London School of Economics (LSE), distingue de una forma muy pedagógica entre Diplomacia Digital y Ciberdiplomacia. Cuando hablamos de diplomacia digital, nos referimos al "uso de herramientas digitales para conseguir fines diplomáticos". La ciberdiplomacia, en cambio, es "el uso de herramientas diplomáticas para resolver asuntos relativos al ciberespacio".

La ciberdiplomacia se ha desarrollado en gran parte gracias a la necesidad de ciberseguridad y resulta vital para garantizarla. El propio carácter del ciberespacio, con fronteras difusas y actores que operan en dominios jurídicos que a menudo se solapan o no están definidos, hace que el uso de la diplomacia sea especialmente crítico. Franz-Stefan Gady (investigador de East West Institute, editor principal en Diplomat APAC) y Greg Austin (profesor en Australian Centre for Cyber Security, UNSW y miembro de East West Institute) recogen la necesidad de utilizar estrategias diplomáticas proporcionales a las amenazas, si bien reconocen que no muchos gobiernos

lo han implantado suficientemente. Además, destacan que los esfuerzos diplomáticos en ese sentido no son capaces de alinearse con los intereses de seguridad nacional. El mundo actual no puede funcionar adecuadamente si la ciberconectividad es atacada con éxito.

Avances en ciberdiplomacia mundial de los últimos años incluyen, por ejemplo, el acuerdo entre el gobierno estadounidense y el chino para luchar contra el ciberespionaje, que implicaba intercambio de información, evitar el apoyo de actividades que vayan en contra de los intereses de alguno de los dos países y promocionar el buen uso del ciberespacio. Pero, como afirma Enrique Fojón, subdirector de THIBER, este tipo de pactos debería ir más allá de los acuerdos de mínimos.

Como ejemplo, el proyecto de ley sobre Ciberdiplomacia de Estados Unidos reinstaura y eleva el puesto de cibercoordinador dentro de la Office of Cyber Issues (Oficina de Asuntos Cibernéticos) que dependería del Departamento de Estado y se encargaría de liderar la labor ciberdiplomática del Departamento de Estado en asuntos que van desde la ciberseguridad a la economía digital y asuntos de internet.

Por su parte, la Unión Europea, en medio del debate sobre la soberanía, las legislaciones nacionales e internacionales en el ciberespacio, decidió aprobar la creación de un marco de trabajo para la ciberdiplomacia, The EU Cyber Diplomacy Toolbox. Esta "caja de herramientas" pretende dotar a la UE y a sus países miembros de la capacidad de señalización y reacción para influir en el comportamiento de potenciales agresores. Actualmente las acciones de la UE se centran, principalmente, en sanciones. Erica Moret (investigadora principal del Centro de Gobernanza Global de The Graduate Institute Geneva) y Patryk Pawlak (oficial ejecutivo del Instituto de Estudios de Seguridad de la Unión Europea en Bruselas) recomiendan, entre otros, la integración de las sanciones dentro de la estrategia de política exterior de la UE combinadas con diplomacia, negociaciones comerciales, inteligencia, leyes, colaboración con otros países e instituciones multilaterales y cooperación con el sector privado.

Diplomacia corporativa

Parece evidente que el papel de la empresa privada en la ciberseguridad es clave, no sólo para la protección de intereses económicos, sino para la seguridad ciudadana, defensa de puntos estratégicos como infraestructura, gobierno y administración, salud, etc. Además, la iniciativa privada es fuente de innovación, recursos y talento. En la actualidad, es tal la relevancia de la empresa privada, incluso como interlocutor a escala nacional (diálogo empresa-país) y supranacional (diálogo empresa-organización internacional, UE, etc.), que países e instituciones internacionales están formalizando cada vez más los canales de interacción con la empresa privada. Especialmente llamativo es el ejemplo de las grandes empresas tecnológicas, que sirven de plataforma para formadores de opinión, tienen una valoración bursátil mayor que el PIB de algunos países y juegan un papel primordial en cuestiones políticas de alcance internacional. Acontecimientos como la Primavera Árabe, influencia en elecciones de otros países, la radicalización a través de Internet y ejemplos similares, han llevado a los actores internacionales tradicionales a ser conscientes de que el escenario internacional ha cambiado y, con el cambio, han llegado nuevos actores y nuevas formas de relacionarse.

> **"las grandes empresas utilizan técnicas políticas frente al aumento de los riesgos globales"**
>
> Juan Luis Manfredi, periodista y profesor de la Universidad de Castilla-La Mancha

Por parte de la iniciativa empresarial, la diplomacia corporativa crece en importancia debido a la incertidumbre a la que hacen frente las grandes corporaciones que operan a escala internacional. Juan Luis Manfredi, periodista y profesor de la Universidad de Castilla-La Mancha, destaca cómo "las grandes empresas utilizan técnicas políticas frente al aumento de los riesgos globales" mediante la diplomacia corporativa, para impulsar la estrategia de relaciones internacionales entre poderes públicos y privados de una forma activa.

En el lado de la diplomacia nacional, tenemos el ejemplo de Dinamarca que, el pasado año, nombró al primer embajador tecnológico y digital de Dinamarca, con el mundo digital como ámbito de actuación y como interlocutores las grandes empresas tecnológicas. Como explicó el ministro de exteriores danés, "Compañías como Google, Apple o Microsoft se han convertido en una especie de nuevas naciones y debemos reaccionar de alguna manera".

Aunque tradicionalmente empresas y gobiernos han mantenido relaciones institucionales, el nombramiento de embajadores frente a grandes empresas, o el uso de técnicas políticas para hacer frente a los riesgos globales suponen llevar las relaciones estados-empresas a un nuevo nivel. Según Corneliu Bjola, profesor asociado de Estudios Diplomáticos en la Universidad de Oxford, otros gobiernos están siguiendo con interés el caso de Dinamarca y, si siguen su ejemplo, el surgimiento de actores internacionales no estatales con capacidades diplomáticas estaría a la vuelta de la esquina.

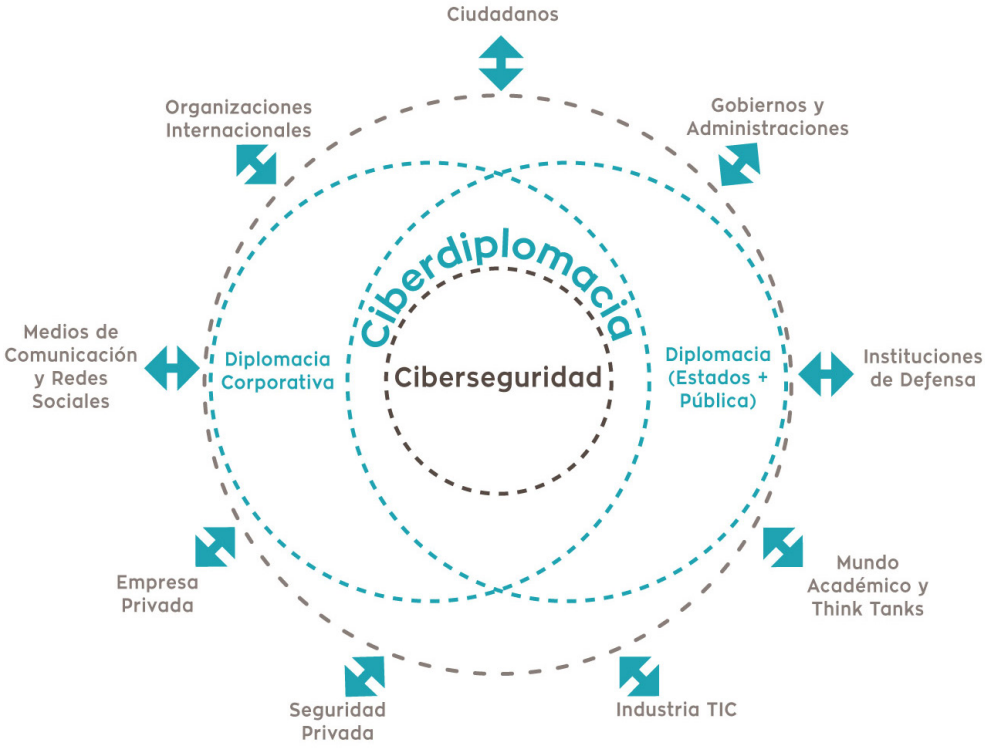
Ciberseguridad

El complejo escenario internacional, profundamente disruptivo y con métodos híbridos que afectan a actores de diferentes niveles, desde supranacionales a individuales, con un carácter asimétrico, transversal e íntimamente interconectado, demuestra la necesidad de una red de medidas de seguridad que tengan las mismas características: carácter disruptivo, ágil, multidisciplinar, hibrido multinivel y nodular. Para ello, se están dando varios pasos que son importantes pero que carecen de la cohesión que les haga ser realmente efectivos en el ciberespacio. Resultan especialmente significativos el reconocimiento del ciberespacio como dominio de operaciones de defensa de la OTAN, el desarrollo de una estrategia de ciberdefensa por parte de varios países, o la firma de acuerdos público-privados de colaboración para la mejora de la ciberseguridad.

Por lo tanto, la ciberseguridad debe formar parte de la agenda de este nuevo escenario diplomático en el que interactúan actores a distintos niveles, con diferentes ámbitos de actuación e intereses pero cuya colaboración es esencial para garantizar la seguridad de ciudadanos, estados y empresas.

Relaciones entre Ciberseguridad, Diplomacia y actores en diferentes niveles.

Nota: el grafico representa relaciones multidimensionales, en ningún caso pretende ser exhaustivo o establecer niveles de importancia.



Beatriz Serrano
@Beatriz_Sercas

Fuente: Elaboración propia

Esta ciberdiplomacia debe incluir las siguientes acciones:

1. Presencia creciente de la ciberseguridad tanto en la agenda diplomática de países como en la diplomacia corporativa.
2. Control efectivo del cibercrimen financiero.
3. Colaboración efectiva público-privada (PPP) basada en confianza y transparencia.
4. Búsqueda de consenso entre entidades públicas y privadas en la definición de ciberseguridad y cómo garantizarla.
5. Promoción de sistemas que faciliten la difusión de información en tiempo real.
6. Desarrollo de legislación uniforme que facilite la cooperación entre países y con el sector privado.
7. Debate enriquecedor entre sectores público y privado para aclarar diferencias en la definición de ciberseguridad.
8. Fomento del sector de ciberseguridad con claro énfasis en la innovación y la investigación.
9. Coordinación para un uso más eficiente de los fondos centrado en demanda de soluciones de ciberseguridad
10. Acciones de diplomacia pública encaminadas a hacer visible la industria de la ciberseguridad, su necesidad y el papel de los diferentes actores.

Fuente: www.pexels.com

En resumen, la ciberdiplomacia, empleada por estados dentro de su agenda diplomática y por la iniciativa privada a través de la diplomacia corporativa, es un elemento vital para garantizar la ciberseguridad y como potenciador de innovación dentro de este campo. Es necesario que todos los niveles diplomáticos tomen conciencia y se doten de medios para conseguir estos objetivos, y fundamental para lograr una concienciación a todos los niveles, indispensable para una ciberseguridad activa y eficaz.