Por qué necesitamos diplomáticos en el ciberespacio

Shaun Riordan

Un hombre pasa al lado de un anuncio de 5G en Seul, Corea del Sur, abril 2019. JUNG YEON-JE/AFP/Getty Images

No podemos dejar el ciberespacio en manos de los técnicos, porque en este dominio están en juego cuestiones políticas y geopolíticas como la gobernanza de Internet, la ciberseguridad e incluso el ciberconflicto.

El francés Georges Clemenceau dijo una vez que la guerra es demasiado seria como para dejársela a los generales. De igual modo, el ciberespacio es demasiado serio como para dejárselo a los técnicos. Y, sin embargo, eso es lo que estamos haciendo. Se ha puesto de manifiesto con el actual revuelo causado por Huawei y el 5G. A las reuniones en las que se iban a tratar los nuevos estándares industriales para la telefonía 5G asistieron expertos técnicos de gobiernos y empresas occidentales. Y estos no repararon en la relevancia del repentino aumento del tamaño de las delegaciones chinas en estas reuniones. Tampoco entendieron las implicaciones en materia de seguridad y geopolítica de que Huawei se asegurara una posición dominante en el establecimiento de los estándares industriales de la segunda fase del 5G, aquella relacionada con el denominado *Internet de las cosas.* Para cuando el gobierno de Estados Unidos se dio cuenta de lo que había sucedido, el problema había pasado a ser el de recuperar el terreno perdido. Lo que puede acabar siendo demasiado tarde.

Los diplomáticos y los políticos han dejado el ciberespacio en manos de los técnicos: si estos crearon el ciberespacio, que sean ellos los que resuelvan sus problemas. Mientras tanto, los diplomáticos se han obsesionado con el uso de las redes sociales para promocionar la imagen de sus países (con poco éxito). Pero, cada vez con más frecuencia, los problemas que suscita

el ciberespacio no son técnicos y no tienen soluciones técnicas. Son asuntos políticos y geopolíticos que van desde la gobernanza de Internet hasta la ciberseguridad, e incluso el ciberconflicto. Estos no son problemas que los técnicos puedan resolver. Surgen en todos los ámbitos del ciberespacio, desde las redes físicas de cables y estaciones de conmutación hasta el nivel social de los humanos que interactúan a través de Internet y la red informática mundial. Se extiende el debate sobre cómo debe regularse la Red y proteger los datos. Los submarinos se entregan a su *ballet* alrededor de los cables submarinos, ya sea para interceptarlos, cortarlos o protegerlos. Surgen actores malintencionados que utilizan las plataformas de redes sociales para difundir desinformación. Ninguno de estos son problemas técnicos.

En muchos aspectos, la naturaleza y la estructura de los problemas que se registran en el ciberespacio son un reflejo de los del espacio físico. La distinción entre la agenda de la gobernanza de Internet y la de la ciberseguridad refleja la distinción entre la agenda de las cuestiones globales y la de la geopolítica en el ámbito físico. Del mismo modo que las agendas geopolíticas más tradicionales amenazan con distraer la atención de los gobiernos de la agenda de cuestiones globales y debilitar los esfuerzos para resolver sus dilemas, los problemas de ciberseguridad amenazan la gobernanza de Internet. Tanto en el espacio físico como en el ciberespacio, una amplia variedad de actores estatales y no estatales participan ahora activamente en los asuntos internacionales, ofreciendo diferentes visiones, en ocasiones en conflicto, de cómo podrían resolverse distintas cuestiones. En algunos casos, los actores, estatales y no estatales, pueden ser el problema, aunque también parte de la solución. A medida que la relativa hegemonía de Estados Unidos disminuye y surgen puntos de vista divergentes sobre la gobernanza global, las reglas que rigen las relaciones políticas y económicas internacionales se fragmentan. El impacto de esta transición hacia un mundo multipolar se siente con tanta intensidad en el ciberespacio —donde está representado por los desacuerdos entre los países de Internet libre y los defensores de la soberanía cibernética— como en el ámbito físico.

La construcción de la gobernanza internacional del siglo XXI, ya sea en el ciberespacio o en el mundo físico, deberá tener en cuenta estos cambios. En lugar de acuerdos intergubernamentales que conduzcan a nuevas organizaciones internacionales que impongan marcos regulatorios de arriba hacia abajo es más probable que la nueva gobernanza tanto en el espacio físico como en el ciberespacio se construya de abajo a arriba a través de debates en red entre todo el abanico de actores estatales y no estatales. Estos debates reguladores se producirán a su vez tanto en el espacio físico como en el ciberespacio. Es probable que el modelo sea el de los debates en red de actores estatales y no estatales que en última instancia condujeron a los Acuerdos de París sobre el cambio climático, en los que se formaron coaliciones heterogéneas en torno a unos objetivos comunes: los resultados que se consideraban preferidos. Es probable que los nuevos debates normativos clave se centren en nuevas tecnologías como la inteligencia artificial, el aprendizaje automático y la manipulación genética, y las aplicaciones que se consideran aceptables o inaceptables de todas ellas. La diplomacia entre múltiples partes interesadas que todo esto exigirá será la misma que para la gobernanza de Internet. Escindir esta de los otros debates regulatorios no solo tendría poco sentido, sino que podría pasar por alto las compensaciones entre diferentes dominios reguladores.

El enfoque diplomático del ciberespacio se basa en la idea de una comunidad internacional de

diplomáticos y en el proceso de socialización de los actores internacionales dentro de ella. En el contexto del ciberespacio, la idea es construir una comunidad internacional de diplomáticos dentro del ciberespacio. Una pregunta clave para el siglo XXI, tanto en el ciberespacio como en el ámbito físico, es si los nuevos actores no estatales socializarán dentro de la comunidad diplomática, y, en caso de no hacerlo, qué significará eso para el futuro de la gobernanza internacional y la estabilidad. ¿El papel cada vez más importante de las ONG, que ven el mundo en términos de blanco o negro y que insisten en aferrarse al hallazgo de soluciones óptimas, dificultará la negociación de acuerdos mínimos de gobernanza? ¿El creciente papel de las compañías y los ejecutivos empresariales llevará a centrarse excesivamente en los factores económicos? En resumen, ¿la creciente multiplicidad de actores no estatales hace que la gobernanza de Internet sea más fácil o más difícil de lograr?

Los diplomáticos deben comenzar a interactuar de manera más efectiva con las principales compañías de Internet. Este no es un caso más de entablar contactos con una empresa comercial cualquiera. Estas grandes compañías no solo proporcionan servicios o plataformas para sus clientes, dan forma al ciberespacio y a cómo funciona. Los algoritmos y los motores de búsqueda facilitan la difusión de información errónea y posibilitan la guerra de información, a la vez que complican y minan los esfuerzos para combatirla. Las propias empresas de Internet necesitan entender mejor cómo funcionan en el ciberespacio y aceptar sus responsabilidades. Los diplomáticos deben tratarlos como actores geopolíticos por derecho propio, y no siempre con actitudes amistosas o cooperativas.

El papel fundamental del Estado es proteger la seguridad de su territorio y sus ciudadanos. El sobrestimado declive de la relevancia del Estado se puso en contexto en el espacio físico con el 11-S y el subsiguiente papel clave del Estado a la hora de proteger a sus ciudadanos contra el terrorismo internacional. Del mismo modo, en el ciberespacio, a pesar de la gran cantidad de actores no estatales y su importancia, la agenda de ciberseguridad garantiza la continua relevancia e importancia del Estado. Solo los Estados, o los grupos respaldados por estos, tienen los recursos técnicos y financieros necesarios para penetrar en objetivos bien protegidos o para defender infraestructuras críticas contra los ciberataques. Solo ellos tienen la legitimidad para penetrar en sistemas informáticos extranjeros con el fin de verificar sus capacidades y motivaciones. Comprender las intenciones de otros Estados sigue siendo un problema importante para la ciberseguridad. En el ciberespacio es difícil distinguir entre ataque y defensa. Una penetración defensiva en los sistemas informáticos de otro país para comprobar sus capacidades y motivaciones puede parecer lo mismo que una penetración ofensiva en preparación para un gran ataque cibernético. La evaluación efectiva de las intenciones, y la capacidad de entender cómo pueden ser interpretadas las acciones propias, se vuelven esenciales para evitar la escalada de los conflictos cibernéticos. Algunos estudios recientes

enfatizan la importancia de los encuentros regulares cara a cara para la correcta comprensión de las intenciones y el desarrollo de la empatía. Los diplomáticos que se relacionan en el espacio físico, y mantienen un contacto frecuente entre sí, siguen siendo clave para la estabilidad en el ciberespacio.

El problema de evaluar intenciones, combinado con las dificultades para determinar la autoría de los ataques cibernéticos, la probabilidad de que las acciones de represalia causen daños limitados y la percepción de efectos colaterales cinéticos (daños en el espacio físico) también limitados pueden reducir el umbral para la guerra cibernética. En un sistema internacional en el que se vive una tensión creciente pero donde las armas nucleares limitan las opciones de que se desencadene una gran guerra entre países, el conflicto cibernético puede parecer una opción de bajo riesgo. A diferencia del espacio físico, donde la guerra está limitada por la Ley de Conflictos Armados, en la actualidad hay pocas, o ninguna, norma de comportamiento acordada para la ciberguerra. Incluso una cuestión que resulta tan esencial como si un Estado puede responder a un ataque cibernético con represalias cinéticas sigue sin resolverse.

Abordar las cuestiones de la ciberseguridad y de la gobernanza de Internet exigirá un cambio por parte de los ministerios de Exteriores y de los diplomáticos. Los ministerios de Relaciones Exteriores deberán ser menos jerárquicos y estar más interconectados. Tendrán que integrar a

los diplomáticos que se encuentran en el extranjero en los procesos de toma de decisiones, al mismo tiempo que les delegan más autonomía y autoridad. El ciberespacio rara vez da tiempo para consultas y tomas de decisiones jerárquicas. Los ministerios de Relaciones Exteriores tendrán que desarrollar intercambios con la industria tecnológica para identificar nuevas tecnologías y el impacto que estas tendrán en las relaciones internacionales. Los diplomáticos deberán formarse en nuevas áreas, incluyendo algoritmos, técnicas de optimización de motores de búsqueda (SEO) y ciertos niveles de codificación. Pero estos son ámbitos en los que todos van a necesitar capacitación y las nuevas generaciones probablemente puedan aprender en el colegio junto con la lectura y las matemáticas.

El mayor desafío tanto para los ministerios de Exteriores como para los diplomáticos puede ser el desarrollo de una diplomacia que tenga en cuenta a múltiples partes interesadas de manera efectiva para interactuar con todo el abanico de actores estatales y no estatales. Los diplomáticos tienen que mejorar su capacidad de identificar toda la variedad de actores no estatales. Los ministerios de Relaciones Exteriores deben comprender las tensiones y dificultades de los diplomáticos y de aquellas misiones que tratan simultáneamente con actores estatales y no estatales. Sobre todo, los diplomáticos deben reconocer que no todos los actores no estatales querrán hablar o colaborar con ellos. Necesitan pensar en cómo pueden utilizar técnicas innovadoras de diplomacia pública y digital o intermediarios para llegar a estos actores no estatales más reacios a involucrarse con el fin de poder tratar con ellos en los debates clave.

La diplomacia de múltiples partes interesadas no es la única área donde los diplomáticos del siglo XXI tienen que ser polifacéticos, tanto en el ciberespacio como en el espacio físico. Deberán tratar con el espacio físico y el ciberespacio al mismo tiempo, integrando ambos campos dentro de políticas exteriores y estrategias diplomáticas coherentes. En ambos dominios, también tendrán que lidiar simultáneamente con los problemas globales y las agendas geopolíticas (en el ciberespacio con la gobernanza de Internet y las agendas de ciberseguridad). No deben permitir que las agendas geopolíticas distraigan la atención y el esfuerzo de aquellas de temas globales. Pero tampoco deben permitir que su participación en las agendas de problemas globales socave su capacidad para responder con firmeza y eficacia a los retos geopolíticos. El desafío clave de la política exterior del siglo XXI será el desarrollo de una capacidad híbrida de gobernar (combinando el enfoque diplomático con herramientas militares y económicas) que incorpore el espacio físico y el cibernético, implique a múltiples actores estatales y no estatales y gestione los problemas globales y las agendas geopolíticas. La diplomacia es una parte necesaria, aunque no suficiente, de este arte del buen gobierno.

Este artículo está basado en el libro *Cyberdiplomacy: Managing Security and Governance Online,* Polity Press, 2019.

Fecha de creación

22 abril, 2019