



Anuario Mexicano de Asuntos Globales
2025

ENSAYOS

Diplomacia digital, ciberdiplomacia y el uso de la inteligencia artificial

Eduardo Roldán¹

Fecha de recepción: lunes, 13 de abril de 2026

Fecha de aprobación: viernes, 4 de septiembre de 2026

DOI: <https://doi.org/10.59673/amag.v4i1.137>

Resumen

El objetivo de este ensayo es analizar y entender las decisiones tomadas por los actores internacionales involucrados en los procesos del mundo digital, el uso de la inteligencia artificial (IA), en la diplomacia digital y en la diplomacia cibernética o ciberdiplomacia en pleno siglo XXI. Esto en virtud del impacto que han tenido en la formulación de políticas públicas tanto nacionales como internacionales, en los sectores de la política, la economía, el comercio, la cultura, la mercadotecnia, la justicia, la comunicación, la educación y la salud, entre otros sectores clave, pues vivimos en un mundo global.

Palabras clave: Diplomacia digital, ciberdiplomacia, inteligencia artificial, ciberseguridad diplomática, diplomacia cibernética

Abstract

This essay analyzes the decisions made by international actors involved in digital processes; in the use of artificial intelligence (AI), digital diplomacy, and cyber diplomacy in the 21st century. This is due to the impact these decisions have had on the decision-making process of national and international public policies in the political, economic, trade, cultural, marketing, justice, communication, educational, and health sectors, among other key areas, as we live in a globalized world.

Keywords: Digital diplomacy, cyberdiplomacy, artificial intelligence, diplomatic cybersecurity, cyber diplomacy

¹ El Emb. Eduardo Roldán fue presidente de la Asociación del Servicio Exterior Mexicano (ASEM), presidente de la Asociación Mexicana de Estudios Internacionales (AMEI), miembro del Consejo de Honor de la AMEI, Embajador de México en Argelia, Libia, Mauritania y Túnez; Jefe de Cancillería en la Embajada de México en Corea del Sur y Cónsul General Alterno de México en Hong Kong. Doctor en Ciencias Políticas y Sociales, UNAM. Catedrático del posgrado en la Universidad Intercontinental. Autor de 10 libros. Correo electrónico: eroldana21@gmail.com

Introducción: la inteligencia artificial

Hoy en día es un imperativo estratégico entender la relevancia de la Inteligencia Artificial (IA). En simples términos, la IA es la capacidad de una máquina para imitar el comportamiento humano. La IA se basa en algoritmos. Un algoritmo es un conjunto ordenado y finito de operaciones que permiten encontrar la solución de un problema por medio de una secuencia de pasos que arrojan un resultado de acuerdo con ciertas condiciones variables. La IA aprende todo tipo de información, la sistematiza, identifica patrones y así toma decisiones autónomas.

La Organización Mundial de Propiedad Intelectual (OMPI) la define como “el conjunto de sistemas automatizados diseñados para realizar tareas típicamente asociadas con la inteligencia humana o funciones cognitivas” (Roldán, 2025, p. 266). La IA hace juicios probabilísticos basados en patrones y tendencias. Los sistemas de IA, a través de sus mismas operaciones, están en constante flujo e instantáneamente analizan nuevos datos y buscan mejorarse con base en sus análisis. Este proceso desarrollado por la IA genera una habilidad previamente reservada a los humanos. Hace juicios estratégicos sobre el futuro, algunos basados en información recibida y acumulada a través de códigos.

Lo anterior es un marco de referencia para entender que, hoy en día, vivimos en un dilema: existen desafíos, pugnas y disputas geopolíticas y geoeconómicas que se dan entre países y empresas en la fabricación de chips que son la base para la utilización en la IA. Sectores privados y públicos han utilizado la IA para informar o desinformar y divulgar mensajes verídicos o falsos. Otro dilema es que, mediante los algoritmos, la sociedad puede ser víctima de sesgos sociales, raciales y étnicos, cuyo resultado es el refuerzo de la discriminación institucional, pública, privada o policial hacia las minorías por el simple hecho de existir. En este entorno necesitamos entender que:

Evolucionar y adaptarnos a los cambios han sido una de nuestras ventajas competitivas como especie. Hoy nos enfrentamos a un nuevo momento de adaptación. El mundo digital ha irrumpido en nuestra vida a mucha velocidad y se prevén cambios importantes en los próximos años, a los cuales debemos adaptarnos. Una vez más, necesitamos esa adaptación, como ya hemos hecho en innumerables ocasiones, a lo largo de la historia de la humanidad. Todos los días vemos en las noticias, en los medios de comunicación, informaciones a propósito de la transformación digital, de la robótica, de la inteligencia artificial y de los efectos -positivos y negativos- para la humanidad (Briones, 2020, p.60).

La inteligencia artificial no podría existir sin chips, sin semiconductores (Roldán, 2023, p. 68). Y por ello, estamos en medio de una lucha por la nueva hegemonía en este mundo global. De acuerdo con la información proporcionada por Statista, el valor de la IA, a precios del mercado, representa más de 300 mil millones de dólares. Lo antes analizado nos lleva a entender las consecuencias de las decisiones tomadas por los actores

internacionales involucrados en estos procesos.

Los actores nacionales e internacionales emplean *chatbots* impulsados por IA para difundir sus acciones o manipular la opinión pública a su favor y desarrollan *deepfakes* para difundir información errónea e incluso utilizan el aprendizaje automático para optimizar sus resultados. “La IA puede ser una fuerza para el bien, pero también puede ser una herramienta para los malvados. Estas redes, además de desinformar, impulsadas por la IA pueden manipular los mercados” (Roldán, 2025, p. 268). Al respecto, Paolo Benanti (2024) analiza nítidamente la comunicación veraz y fiable y las *fake news* y su influencia en la sociedad contemporánea.

Ese es el desafío que tenemos frente a la IA. El objetivo esencial debiera ser siempre buscar el beneficio de la humanidad para combatir la desinformación. Esta última es uno de los cinco mayores riesgos globales que enfrenta el mundo contemporáneo (World Economic Forum, 2025). Al respecto, concuerdo con el siguiente planteamiento:

La IA generativa, particularmente los grandes modelos de lenguaje (LLM) y los sistemas de generación de imágenes y vídeos, constituyen probablemente la tecnología con mayor potencial disruptivo más inmediato... La IA generativa ofrece capacidades de producción de contenido que habrían parecido imposibles hace una década (Lakomy, 2023).

Esto es, la IA generativa puede alterar la diplomacia utilizando *chatbots* multilingües con adaptación cultural, realizando análisis predictivo de opinión pública en tiempo real, o simulando escenarios de posibles negociaciones. Lo anterior se visualiza en la siguiente gráfica que muestra diferentes acciones como investigación, transmisión de lenguajes, identificación de identidades, promoción de ideas, de imágenes, ataque de *phishing*, *vishing*, *smishing*, *pharming*, *spoofing*, *watering* automatizados, traducción de idiomas, *deepfakes*, traducción de identidad sintética, escaneo de código abierto, reconocimiento, investigación, automatización de *bots*, suplantación de dominio, generación y depuración de código, desarrollo de herramientas, generación de *malware*, ofuscación o mutación de cargas útiles de malware, inyección de mensajes integrados, servicios de encubrimiento, negociaciones de *ransomware*, identificación de credenciales sensibles y movimiento lateral, etc., que pueden ser utilizadas mediante el uso de la IA en el mundo de hoy.

Neologismos: definición de conceptos

El *phishing* es el uso de métodos de engaño a través de los correos electrónicos para conseguir información personal o financiera del usuario. El término *vishing* es una combinación de las palabras voice (voz) y phishing, por lo que también se denomina en ocasiones *voice phishing*. El *vishing* usa la tecnología VoIP (voz sobre IP). El *smishing* es el uso de métodos de engaño a través de los SMS o mensajes de texto del celular para conseguir información personal o financiera del usuario. El *pharming* envía al usuario a un sitio web falso para

robarle información personal o financiera. El *spoofing* consiste en usurpar una identidad electrónica para ocultar la propia identidad. En el *watering hole* (abrevadero digital) los *hackers* esperan a que sus víctimas visiten un sitio web bancario e instalan el software malicioso en las computadoras del usuario. Los *deepfakes* son vídeos, imágenes o audios generados o manipulados mediante IA que imitan la apariencia y la voz de una persona real de manera hiperrealista. Los *bots* son programas informáticos automatizados que operan en internet para realizar tareas repetitivas a alta velocidad.

Todo ello se da en virtud de que:

La IA facilita la traducción automática y la adaptación cultural: un mensaje puede publicarse simultáneamente en todos los idiomas posibles, cada uno ajustado a los modismos locales para mejorar su eficacia. O en el caso de las informaciones falsas o *deepfakes* éstas pueden añadir una dimensión particularmente perversa pues pueden fabricar evidencia visual de eventos que nunca ocurrieron (Torres, 2026, p.6).

Asimismo, los *chatbots* conversacionales desempeñan un papel relevante pues pueden validar o invalidar posiciones políticas o ideologías diplomáticas. En suma, la IA no es una panacea. Es una herramienta, y como toda tecnología, su impacto depende de cómo se use, quién la use y en qué contexto (Torres, 2026, p. 18). Sin embargo, estas son decisiones que definen el tipo de sociedad que queremos ser. El horizonte 2035 no está tan lejos. Las tecnologías que definirán ese futuro ya existen y se están desarrollando frenéticamente (Torres, 2026, p. 19). Es evidente que el futuro nos alcanzó.

Es en ese contexto donde el uso de la IA ha modificado de una manera sustancial y profunda la diplomacia tradicional, pues las nuevas tecnologías de comunicación abrieron el abanico de acciones y posibilidades, mismas que se han incrementado exponencialmente. El Sistema Económico Latinoamericano y del Caribe lo resume de la siguiente manera:

En el actual mundo de la era digital, el ciberespacio se ha convertido en uno de los principales campos de acción para los gobiernos, instituciones públicas, empresas, sociedad civil y ciudadanos. Las grandes compañías tecnológicas, fundamentalmente norteamericanas y chinas, han liderado y gobiernan la era digital. El poderío económico derivado del uso de la inteligencia artificial para producir bienes y servicios conlleva implicaciones geopolíticas, siendo la principal, transformar a estas grandes compañías en los actores globales en el sistema internacional. La Inteligencia Artificial está generando un impacto en sectores como el transporte, banca y finanzas, educación y salud por mencionar algunos. Por tanto, modifica los sistemas económicos, financieros y comerciales tradicionales, pero no solo. También influye y afecta los sistemas políticos de los países. Las campañas de información y desinformación, la alteración de los procesos electorales, las acciones que llevan al cambio o derrocamiento de gobiernos, todo ello gestionado con la Inteligencia Artificial lo grafica. (SELA, 2024, p. 10)

Consecuentemente, esta realidad nos permite analizar y entender las nuevas acciones

digitales en el ámbito político y económico que se están instrumentando en el mundo diplomático del siglo XXI.

Las nuevas categorías analíticas: la diplomacia digital y la ciberdiplomacia

La diplomacia clásica se puede definir como el arte de conducir los asuntos entre naciones, basado en la buena fe, la prudencia y la búsqueda de acuerdos, alejándose de la improvisación. En síntesis, la diplomacia se sustenta en cuatro principios fundamentales: la negociación, la comunicación, la construcción de relaciones y la promoción de intereses (Nicolson, 1994). Es decir, ella enfatiza el uso de medios pacíficos, la representación y el diálogo. El diálogo, la paciencia y la precisión han sido su esencia. La diplomacia es una actividad pacífica, pero puede involucrarse en guerras o en actos de violencia particulares.

A la diplomacia no se le debe juzgar tanto por lo que obtiene, sino por lo que previene. En múltiples ocasiones se hacen y se dicen las cosas más desagradables en la forma más agradable.

Tenemos ante nosotros diferentes trayectorias tecnológicas, decisiones político-económicas estatales y dinámicas sociales y empresariales que nos conducen a realidades radicalmente distintas. “Explorar esos escenarios nos permite anticipar no solo las oportunidades, sino también las amenazas, y, sobre todo, prepararnos para una serie de futuros inciertos” (Torres, 2026, p. 3).

Adolfo Gracia (2022) destaca el papel de la comunicación en diversos ámbitos de la vida cotidiana, su relación con las herramientas sociotécnicas, así como los cambios que estas últimas han traído consigo en las maneras en las que nos comunicamos y, por lo tanto, en la forma en la que abordamos la vida cotidiana. En pocas palabras:

En el panorama de las relaciones internacionales, en constante evolución, la diplomacia digital se ha consolidado como una de las fuerzas más transformadoras de la gobernanza global. Al combinar las prácticas diplomáticas tradicionales con tecnologías de vanguardia, la diplomacia digital está redefiniendo la manera en que las naciones se comunican, colaboran y negocian en el siglo XXI. A medida que avanzamos, las herramientas digitales —desde las plataformas de redes sociales hasta la inteligencia artificial (IA)— se vuelven cada vez más esenciales para que los países proyecten su poder, promuevan sus intereses nacionales e interactúen entre sí en el escenario mundial. (Diplomat Today, 2025).

Los Estados, los organismos internacionales o las ONG están utilizando la IA predictiva tomando en cuenta la información de los macrodatos a los que tienen acceso. Con base en dicha información, los actores la procesan mediante algoritmos para modificar la imagen de la sociedad nacional o internacional en la que operan. En este sentido, las tecnologías de reconocimiento facial o de reconocimiento biométrico, voz, análisis del movimiento,

identificación vocal y otros marcadores biométricos han alcanzado niveles de precisión. La propaganda diplomática o también denominada diplomacia pública, y dentro de ella la diplomacia cultural, es el ejemplo paradigmático (Torres, 2026, pp. 9, 11, 16).

En pocas palabras, las nuevas tecnologías han revolucionado al mundo y la diplomacia clásica se ha tenido que adecuar a esas nuevas realidades. En este entorno analítico, la Diplo Foundation (2026) enmarca en tres grandes bloques el análisis de la diplomacia:

La diplomacia y la geopolítica. En este marco analítico se ve el impacto de la tecnología en las cadenas de suministro, la economía global y la distribución del poder que conforma el entorno en el que opera la diplomacia. Por tanto, aquí se ubica la diplomacia basada en la Inteligencia Artificial, la diplomacia por cable, la diplomacia de los chips, la diplomacia de datos, la diplomacia satelital, la diplomacia científica, la diplomacia de los semiconductores, la diplomacia espacial, la diplomacia tecnológica, la diplomacia telegráfica y la diplomacia telefónica. En la diplomacia temática los diplomáticos debaten en foros internacionales, bilaterales y regionales sobre asuntos que incluyen la ciberseguridad, la seguridad de los datos, la IA y el comercio electrónico. Por ello, en este rango se ubican la diplomacia basada en la Inteligencia Artificial, la diplomacia por cable, la diplomacia de los chips, la diplomacia de datos, la diplomacia criptográfica, la diplomacia cibernética, la diplomacia de las TIC, la diplomacia en línea, la diplomacia cuántica, la diplomacia satelital, la diplomacia científica, la diplomacia de los semiconductores, la diplomacia espacial, la diplomacia tecnológica, la diplomacia telegráfica y la diplomacia telefónica. En otro marco analítico, se toman en cuenta los métodos y herramientas diplomáticas, donde los diplomáticos utilizan herramientas digitales como las redes sociales, la inteligencia artificial, el análisis de datos y las videoconferencias. Aquí se ubica a la diplomacia basada en la Inteligencia Artificial, la diplomacia del blockchain (basada en el uso de la tecnología de registro distribuido descentralizado para mejorar la confianza, transparencia y seguridad en las relaciones internacionales y acuerdos diplomáticos, la seguridad, autenticidad y transparencia), la diplomacia por cable, la diplomacia criptográfica, la diplomacia basada en el Facebook, la diplomacia basada en Instagram, la diplomacia basada en Internet, la diplomacia del metaverso, la diplomacia en línea, la diplomacia cuántica, la diplomacia en tiempo real, la diplomacia científica, la diplomacia tecnológica, la diplomacia telegráfica, la diplomacia telefónica, la diplomacia basada en el Twitter (X), la diplomacia virtual, la diplomacia del blog (utiliza internet y redes sociales para que gobiernos e instituciones ejerzan la política exterior, promuevan intereses y gestionen relaciones internacionales de manera directa con audiencias globales) (Diplo Foundation, 2026).

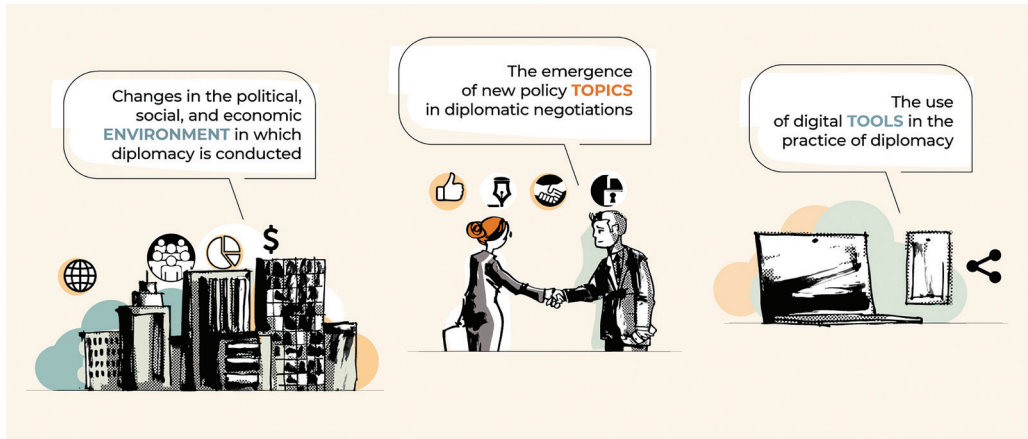
Todo lo descrito anteriormente sobre la transformación digital de la diplomacia se visualiza en el siguiente esquema publicado por la Fundación Diplo.

Figura 1.

Transformación digital de la diplomacia

Digital transformation of diplomacy

happens in three main areas:

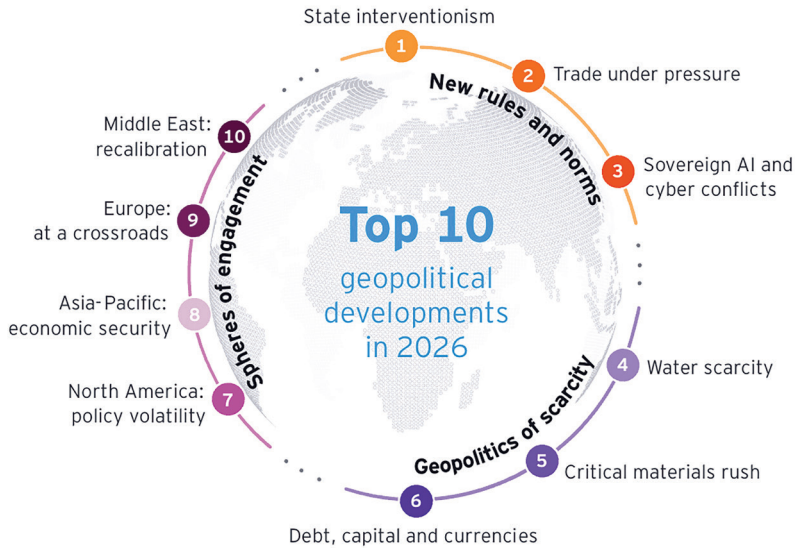


Fuente: Diplo Foundation, 2026.

La diplomacia en la era digital es la transformación de las acciones diplomáticas surgidas a raíz de los avances tecnológicos. Dichas acciones toman en cuenta la información disponible y se instrumentan por medio de la comunicación. El sistema internacional prevaleciente después del año 2000 se caracteriza por la impugnación de las normas internacionales, el regionalismo, el debilitamiento del multilateralismo y por la lucha por una nueva hegemonía mundial. El entorno geopolítico y geoeconómico se visualiza en la siguiente gráfica donde entre los principales acontecimientos geopolíticos en 2026 sobresalen la intervención estatal, la presión sobre el comercio, la IA soberana y los conflictos cibernéticos, la escasez de agua, la escasez de materiales críticos, la deuda, el capital y las divisas, la volatilidad de las políticas en Norteamérica, la seguridad económica en Asia-Pacífico, Europa en su encrucijada, el reajuste en Oriente Medio. Lo anterior se aprecia en la siguiente gráfica:

Figura 2.

Top 10 geopolitical developments in 2026



Fuente: World Economic Forum, 2025.

Es claro que la diplomacia juega un papel fundamental en la difusión, prevención, concientización y en el trabajo activo para ejecutar acciones de manera dinámica y proactiva. Por ello, considero que los tres bloques analíticos que la Diplo Foundation propone, yo los integro en dos categorías analíticas: la diplomacia digital y la ciberdiplomacia.

El objetivo de la diplomacia digital es influir en la opinión pública y en los actores internacionales. Las ideas se difunden a través de declaraciones políticas, iniciativas, negociación, instrucciones, intercambios bilaterales o multilaterales, reuniones presenciales o virtuales y enlaces con ONG.

En este contexto me sirvo de estas dos categorías analíticas para analizar las acciones diplomáticas que se emprenden cuando se utilizan las herramientas digitales en el campo digital y cibernético del mundo contemporáneo. Así pues, la diplomacia digital es “el uso de herramientas digitales para conseguir fines diplomáticos”. La ciberdiplomacia es “el uso de herramientas diplomáticas para resolver asuntos relativos al ciberespacio”. Es decir:

La diplomacia digital se refiere al uso de plataformas digitales, redes sociales y tecnología para llevar a cabo actividades diplomáticas, promover los objetivos de la política exterior de una nación e interactuar con audiencias globales. Durante la última década, el auge de plataformas como Twitter(X), Facebook, Instagram, TikTok, LinkedIn, etc. ha cambiado la forma tradicional en que los gobiernos se comunican. En lugar de depender únicamente de discursos oficiales, comunicados de prensa y reuniones presenciales,

las naciones ahora aprovechan el poder de las herramientas digitales para interactuar directamente con el público extranjero, los responsables políticos y los actores globales. (Diplomat Today, 2025).

Y es así que, por medio de estas herramientas tecnológicas, se realiza la diplomacia pública, la diplomacia cultural, la paradiplomacia, etc. Una de las acciones de difusión económica, política o de difusión de la cultura se genera a través de la diplomacia digital, utilizando Facebook, X, otrora Twitter, TikTok, WhatsApp, etc.

A manera de ejemplo, resalto en las siguientes cuatro fotografías, las acciones artístico-culturales de la diplomacia digital realizadas por México, a nivel mundial, con motivo de la celebración del centenario de la Revolución Mexicana y del bicentenario de la Independencia de México, como se aprecia en el libro publicado por la Secretaría de Relaciones Exteriores.

Figura 3.

Portada de la obra 2010. Celebraciones de México en el Mundo



Fuente: SRE, 2011.

Figura 4.

Mosaico fotográfico de celebraciones mexicanas alrededor del mundo



Fuente: SRE, 2011.

Figura 5.

Cartel de una exposición de gráfica mexicana contemporánea celebrada en Abu Dabi, Emiratos Árabes Unidos



Fuente: SRE, 2009.

Figura 6.

Cartel de una actividad de diplomacia cultural mexicana celebrada en 2010



Fuente: SRE, 2011.

En relación con el uso de la diplomacia digital en el ámbito político, Juan Clark (2021), Rodrigo Perera y Gerardo Dorantes (2023) abundan sobre el uso de los medios de transmisión o el exceso de la utilización del Twitter (X) desde el poder, como se visualiza en el texto y los dos gráficos siguientes.

A través de su red social favorita, Truth Social, Donald Trump mostró mensajes de texto que recibió del presidente de Francia, Emmanuel Macron, y del secretario general de la Organización del Tratado del Atlántico Norte, Mark Rutte, sobre la cuestión de Groenlandia.

EMMANUEL MACRON:

Mi amigo,

Estamos totalmente de acuerdo con lo de Siria, Podemos hacer grandes cosas en Irán. No entiendo qué estás haciendo en Groenlandia. Intentemos construir grandes cosas:

1) Puedo organizar una reunión del G7 después de Davos en París el jueves por la tarde. Puedo invitar a los ucranianos, daneses, sirios y rusos en los márgenes. 2) Cenemos juntos en París el jueves antes de que regreses a Estados Unidos.

MARK RUTTE:

Señor presidente, querido Donald, lo que ha logrado hoy en Siria es increíble. Aprovecharé

mis intervenciones en los medios de comunicación en Davos para destacar su labor allí, en Gaza y en Ucrania.

Me comprometo a encontrar una solución para Groenlandia. ¡Qué ganas de verte!”

Esto es, Twitter(X) e Instagram se han convertido en la cara visible de muchas iniciativas diplomáticas, donde jefes de Estado, ministros de Asuntos Exteriores y embajadores comparten actualizaciones, declaraciones oficiales y participan en debates en tiempo real con el público. Las redes sociales han democratizado la diplomacia, permitiendo a los gobiernos comunicarse directamente con sus ciudadanos y la comunidad internacional, sin necesidad de intermediarios mediáticos tradicionales. Líderes como el presidente de Estados Unidos, el presidente de Francia, E. Macron, el primer ministro de la India, Narendra Modi, y el presidente de los Emiratos Árabes Unidos, el jeque Mohamed bin Zayed Al Nahyan, utilizan plataformas como Twitter(X) no solo para asuntos internos, sino también para expresar sus posturas sobre temas globales como el cambio climático, el comercio internacional y las tensiones geopolíticas. Las redes sociales también facilitan la gestión de crisis en tiempo real, permitiendo a los funcionarios ofrecer actualizaciones y responder a los acontecimientos a medida que se desarrollan, como se ha visto durante emergencias sanitarias mundiales y desastres naturales. Si bien las redes sociales dominan los aspectos públicos de la diplomacia digital, innovaciones más internas están transformando la forma en que los gobiernos llevan a cabo la diplomacia. La inteligencia artificial (IA) y el análisis de datos se han convertido en herramientas poderosas para analizar tendencias globales, la opinión pública y las interacciones diplomáticas.

(Diplomat Today, 2025).

David Cuenca *et al.* (2023) analizan *in extenso* las estrategias de comunicación digital en las redes sociales. Para tal efecto, las funciones del personal diplomático y los sistemas de comunicaciones se han ampliado. Con ello se busca maximizar logros o minimizar daños colaterales. Mercedes Medina (2016) plantea las acciones técnicas digitales utilizadas para ejercer el poder político sobre un mundo cada vez más globalizado.

Otro ejemplo de la diplomacia digital es el uso del denominado pasaporte biométrico, electrónico o digitalizado. Es un instrumento con 45 medidas de seguridad. México está entre las 15 de naciones que emiten un pasaporte de alta seguridad. Fue uno de los primeros cinco en emitirlo a nivel mundial a partir del año 2000, cuando yo era el director general de Delegaciones de la Secretaría de Relaciones Exteriores de México y responsable de dichas tareas.

El documento de identidad permite mostrar al mundo un país que protege la identidad de sus ciudadanos ante el crecimiento de actividades de falsificación de documentos de identidad y viaje. De esta forma se evitan posibilidades de fraude y de falta de seguridad y se da una adaptación a las medidas emitidas por la Organización de Aviación Civil Internacional (OACI).

Con dichas acciones se obtuvo el Premio Nacional Innova 2002 y a nivel mundial

la imagen de México mejoró de manera extraordinaria. El pasaporte mexicano permite viajar a 156 países y territorios sin necesidad de una visa convencional. En 2026, se estima el acceso libre o mediante autorizaciones electrónicas/visa incluyendo la zona Schengen en Europa, a gran parte de América y varios países de Asia. El Índice de Pasaportes Henley es la clasificación original y autorizada de todos los pasaportes del mundo según el número de destinos a los que sus titulares pueden acceder sin necesidad de un visado previo. Según el Henley Passport Index 2026, México ocupa el lugar 20 de 199 países de destino sin necesidad de visa. De ellos, solo 193 son miembros de la ONU. Esto es, el pasaporte mexicano se ubica entre los 20 más poderosos, lo que facilita la movilidad en 156 países y fortalece la imagen de México como socio confiable. El pasaporte mexicano es considerado entre los más fuertes del mundo, lo que facilita el turismo y los negocios sin complicaciones burocráticas previas.

Por todas esas razones, como se muestra en la siguiente gráfica, el pasaporte mexicano de un total de 193 países miembros de la ONU es considerado altamente seguro y se le vincula con la confiabilidad en cuanto a que el portador tiene alto poder adquisitivo en particular relacionado con el turismo internacional.

Ranking global de cada uno de los siguientes pasaportes

1. Singapur – Acceso sin visa a 192 países.
2. Japón, Corea del Sur y EAU. – 187
3. Suecia – 186
4. Dinamarca, Luxemburgo, España, Bélgica, Finlandia, Francia, Alemania, Irlanda, Italia, Países Bajos, Noruega, Suiza – 185
5. Austria, Grecia, Malta, Portugal – 184
6. Hungría, Malasia, Polonia, Reino Unido – 183
7. Australia, Canadá, República Checa, Letonia, Nueva Zelanda, Eslovaquia, Eslovenia – 182
8. Croacia, Estonia – 181
9. Liechtenstein, Lituania – 180
10. Islandia, Estados Unidos – 179
11. Bulgaria, Rumanía – 177
12. Mónaco – 176
13. Chile, Chipre, Hong Kong – 174

14. Andorra – 169
15. Argentina, Brasil – 168
16. Israel, San Marino – 166
17. Barbados, Brunéi – 163
18. Bahamas – 158
19. San Kitts y Nevis, San Vicente y las Granadinas – 157
20. México – 156

Fuente: Henley & Partners, 2026.

Además de que México ocupe un lugar privilegiado en cuanto a su poder de no necesitar visas en 156 países existe una relación directa con el poder adquisitivo de su portador, como se aprecia en la siguiente gráfica. A esto se le denomina riqueza y poder del pasaporte.

Figura 7.

Relación entre riqueza y poder del pasaporte



Fuente: NMás, 2025.

Considerando todo el entorno descrito anteriormente se debe tener en mente que:

Las plataformas con IA pueden analizar millones de tuits, artículos de noticias y publicaciones en línea para brindar a los diplomáticos información crucial sobre el estado de la opinión pública, las tendencias de la política exterior y los indicadores económicos. Los gobiernos utilizan cada vez más el análisis predictivo y el aprendizaje automático para anticipar cambios geopolíticos, monitorear conflictos regionales y medir la efectividad de sus estrategias diplomáticas. Por ejemplo, las embajadas utilizan chatbots con IA para brindar información y asistencia a ciudadanos extranjeros en tiempo real, al tiempo que recopilan datos para mejorar los servicios consulares. (Diplomat Today, 2025).

Concuerdo completamente con la apreciación de la publicación Diplomat Today (2025), según la cual “de cara al futuro, es probable que la diplomacia digital integre aún más las tecnologías virtuales y la inteligencia artificial en los procesos diplomáticos”.

Con el auge de las tecnologías del metaverso, los diplomáticos pronto podrían asistir con mayor frecuencia a cumbres virtuales, participar en intercambios culturales inmersivos o negociar acuerdos en entornos virtuales. El concepto de “embajada digital” podría evolucionar, permitiendo a los diplomáticos operar plenamente en espacios virtuales o aumentados. (Diplomat Today, 2025).

Por otro lado, está la ciberdiplomacia, la ciberseguridad diplomática o diplomacia cibernética. Esta es la cooperación internacional en el ámbito de los asuntos cibernéticos. Comprende el análisis de la problemática en el ámbito del ciberespacio (Serrano, 2025). La categoría analítica de ciberseguridad diplomática engloba la cooperación internacional para la prevención, detección y respuesta frente a amenazas, riesgos y ataques generados en el ciberespacio.

Con el auge de la diplomacia digital surge un tema crucial: la ciberseguridad. A medida que las comunicaciones diplomáticas se trasladan al entorno digital, los gobiernos deben ser más vigilantes que nunca para proteger la información sensible de los ciberataques. El pirateo de servidores de correo electrónico, la filtración de cables diplomáticos y el ciberespionaje se han convertido en riesgos frecuentes para las embajadas y las organizaciones internacionales. (Diplomat Today, 2025).

Lo anterior implica que la interacción multidimensional entre la diplomacia, la ciberseguridad y los actores se da en diferentes niveles: en el centro está la intersección de la ciberseguridad y la ciberdiplomacia, la diplomacia pública, la diplomacia corporativa, rodeadas de los ciudadanos, los gobiernos y sus administraciones, las instituciones de defensa, el mundo académico y los centros de pensamiento, las industrias de las TIC, la seguridad privada, las empresas privadas, los medios de comunicación y las organizaciones internacionales.

Las cancillerías han ampliado las secciones de información y encriptación existentes para fortalecer la cooperación ciber diplomática internacional. El objetivo es contrarrestar

el crimen transnacional y así defender y fortalecer la economía, la política, el comercio y la defensa de los Estados ante hechos tales como el robo de identidad, fraudes cibernéticos, tensiones geopolíticas y geoeconómicas, la carrera armamentística cibernética, uso de tecnologías supersónicas, etc. Sin duda, “la tecnología ha amplificado el lado oscuro del ser humano y ha visibilizado de una manera mucho más universal su ambición de poder” (Franco y Ramírez, 2022). Esto es, “la cooperación entre naciones en materia de ciberseguridad, ciberdiplomacia para combatir a la ciberdelincuencia” y “la prevención de pirateo informático y la guerra de la información se ha convertido en una prioridad en los esfuerzos de la diplomacia digital, con acuerdos que se negocian a través de organizaciones multilaterales como las Naciones Unidas y el G20” (Diplomat Today, 2025).

Por ello se requiere la cooperación internacional en este campo para enfrentar los desafíos, como se ilustra en los tres siguientes diagramas: La cooperación internacional es fundamental, por ello, se encuentra en la intersección de la ciberseguridad para la diplomacia, la ciberseguridad en la diplomacia, y la diplomacia para la ciberseguridad.

Estos países sufrieron más ciber amenazas entre enero y junio de 2025: EE. UU. 24.8%, Reino Unido 5.6%, Israel 3.5%, Alemania 3.3%, Ucrania 2.8%, Canadá 2.6%, Japón 2.6%, India 2.3%, Emiratos Árabes Unidos 2.0%, Australia 1.8%.

Los sectores más afectados en cuanto a ciberataques realizados por la ciberdelincuencia son: los de tecnología de la información TI 25%, la investigación y la academia 14%, gubernamental 12%, centros de pensamiento y organismos no gubernamentales 7%, sector del consumo 7%, sector manufacturero 6%, etc.; de transporte, de comunicaciones, financiero, salud, defensa y energético.

A lo anterior habría que agregar que existen Estados disfrazados. El Estado disfrazado se distancia de un evento, asunto, conflicto o individuo mediante el uso de terceras entidades como ONG, portavoces u otros actores para efectuar acciones cibernéticas. En esta línea de pensamiento, Danna Álvarez (2022, p. 291) resalta que los avances tecnológicos sobre la actividad diplomática pueden traer efectos contrarios en el uso de los canales digitales “por parte de los representantes de los Estados para esparcir información y propaganda de beneficio particular, la cual no en todos los casos es producida a nombre propio”. El propósito es el de influir financiera o ideológicamente en eventos, así pues, crean rumores, mismos que a base de repetirlos se convierten en verdades. Ya que,

A medida que las naciones dependen cada vez más de las plataformas digitales, existe el riesgo de desinformación, información errónea e injerencia cibernética en los esfuerzos diplomáticos. Los *deepfakes*, la desinformación generada por *bots* y las campañas cibernéticas patrocinadas por Estados son nuevas amenazas que requerirán cooperación global y soluciones innovadoras. (Diplomat Today, 2025).

Aquí señalo algunos actos ilegales cibernéticos donde los delincuentes roban

información, hostigan y chantajean política y financieramente en todo el mundo.

Algunos casos clásicos de la delincuencia cibernética realizados

- Banco de Bangladesh (2016 y 2018) 81 millones de dólares.
- Banco Cosmos de India (ago.-oct. 2018) 13 millones de dólares.
- Banco de la Reserva Federal de EE. UU. (2020) mil millones de dólares.
- Bancos en Brasil, Turquía, Malasia, Vietnam, Filipinas, Polonia, Rusia, República Checa, Venezuela, Uruguay, Banco del Austro en Ecuador, la Rizal Commercial Banking Corp, con sede en Manila Filipinas, bancos en Hong Kong, Bank of China, etc.
- BancoEstado de Argentina (2020).
- Departamento de Estado (2020).
- Departamento de Defensa (2020).
- Departamento del Tesoro (2020).
- Autoridad Regulatoria Financiera de Polonia (2020).
- Ciberataque al oleoducto “Colonial pipeline”, el 9 de mayo de 2021.
- Sistema de salud de Irlanda fue hackeado el 14 de mayo de 2021.
- Lotería Nacional de México fue hackeada el 16 de junio de 2021. 800 archivos robados.
- Empresa noruega de comestibles COOP fue hackeada el 3 y 4 de julio de 2021.

Cabe destacar que en el caso de México, prevalecen riesgos graves en el sector de la ciberseguridad como se aprecia en la siguiente tabla.

Fragilidad del sistema en México

Un informe de la OEA reveló que el 43% de las 240 grandes entidades financieras de México han sufrido ataques cibernéticos por hackers nacionales e internacionales.

El costo total de respuesta y recuperación ante incidentes de seguridad digital oscila entre los 2.3 millones de dólares al año para las entidades grandes y los 317 mil dólares para las pequeñas.

El 56% de las entidades financieras no reportan los ataques sufridos ante una autoridad de procuración de justicia en México. México no es un entorno seguro en términos de ciberseguridad.

Falta cultura de la prevención. 9 de cada 10 delitos se cometen a través de tecnologías de la información (OEA, 2020; SSPC, 2020; Banxico, 2021).

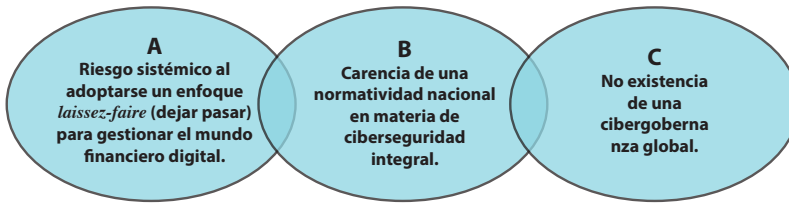
En efecto, en el mundo de hoy, nadie se escapa a dichas acciones. Las mismas naciones, agencias de la ONU y ONG han sido objeto de fraudes internacionales y de ciberataques utilizando logotipos y formatos en intentos para vincular el sitio web de la ONU o de sus organismos con fines políticos. En relación con la IA, Henry Kissinger (2018) resalta que “la tecnología está avanzando más rápido que la capacidad humana para formular los principios que la gobiernen”.

Como consecuencia del análisis anterior se podrían diseñar tres escenarios plausibles: Estos nos permiten orientar las decisiones estratégicas. Nos ayudan a elegir la estrategia más idónea para acometer el proyecto o la acción deseada. De esta forma, ante la problemática presentada en cada uno de ellos, ponemos énfasis en reforzar los entornos de seguridad e implementar bases sólidas para hacer frente a las amenazas y riesgos que se puedan presentar en el futuro cercano y distante con una arquitectura de entornos tecnológicos seguros. Para tal propósito —como afirma Baena (2015)— se identifican los riesgos, las amenazas y oportunidades que afectan la probabilidad de ocurrencia y los retos y objetivos estratégicos y la elaboración de las recomendaciones. Los escenarios propuestos son lo más cercano a lo deseable y superior a lo posible, pero aún factibles. Estos futuribles son el futuro deseable y posible aprovechando un pasado y un presente conocidos con relativa suficiencia. (Miklos y Arroyo, 2008, p. 22). En pocas palabras se toman en cuenta futuros posibles (futuribles) y deseables (futurables) y se anteponen acciones frente a la incertidumbre y el azar con el propósito de prever obstáculos y reducir el riesgo. Es decir, se visualiza la perspectiva de los cambios posibles y deseables.

Veamos qué implicaría cada uno de los siguientes tres escenarios:

- a. Riesgo sistémico al adoptarse un enfoque *laissez-faire* (dejar pasar) para gestionar el mundo digital. Este podríamos llamarlo tendencial pues es la extrapolación basada en las estructuras del presente.
- b. Carencia de una normatividad nacional en materia de ciberseguridad integral y la imperiosa necesidad de establecerla. Este escenario podríamos denominarlo deseable con estructuras potencialmente diferentes a las actuales.
- c. No existencia de una cibergobernanza global y el plausible caos en el espacio cibernético. A este escenario podríamos señalarlo como catastrófico pues sería lo indeseable; se ubicaría en el extremo de lo temible. (Roldán, 2023, pp. 212-214)

Figura 8.

Escenarios de la ciberseguridad

Fuente: Elaboración propia del autor.

El escenario A engendraría un riesgo sistémico al adoptarse un enfoque *laissez-faire* (dejar pasar) para gestionar el mundo digital. De ahí la necesidad de tomar acciones drásticas para evitar el riesgo sistémico prevaleciente. Las instituciones que continúen con una visibilidad completa de todos los puntos de entrada y salida de su red estarían poniendo toda su infraestructura en riesgo. Por tanto, se generaría y profundizaría un desorden o anarquía global.

El escenario B contempla la carencia de una normatividad en materia de ciberseguridad holística nacional integral y la imperiosa necesidad de establecerla. Dicha carencia ha permitido a la ciberdelincuencia seguir horadando la confianza y las finanzas de las instituciones bancarias, gubernamentales y privadas. Hoy en día, cada institución hace lo que puede y como puede. Falta coordinación vertical y transversal entre instituciones públicas y privadas. De seguir así se llegaría a un descontrol absoluto en la materia. La ciberdelincuencia lo sabe y se ha aprovechado de esos vacíos legales inexistentes.

El escenario C es la no existencia de una cibergobernanza global, misma que nos podría llevar a un plausible caos en el espacio cibernético a nivel mundial. A este escenario podríamos señalarlo como catastrófico pues sería lo indeseable. Actualmente en la era de la hiperconectividad se vive la globalización del desorden del espacio cibernético. Cada quien hace lo que quiere como puede y cuando quiere. Vivimos en la globalización del desorden. No hay una normatividad global. El mundo caería en el caos cibernético. Se agudizaría el caos en el ciberespacio donde todos seríamos perdedores. De seguirse socavando la confianza en las cadenas de suministro mundiales de ciberseguridad se profundizaría la guerra cibernética o guerra en la red, como la denominan Richard Clarke y Robert Knake (2011), con consecuencias catastróficas a nivel mundial.

Se requieren normas claras en torno al uso del ciberespacio y una importante actualización de la gobernanza de Internet con protocolos de seguridad a nivel mundial. Godet y Durance (2010) destacan que —entre otras acciones— se debe formar una coalición de todos los países, industrias y grupos de la sociedad civil con mentalidad afín para impulsar un modelo que garantice, como mínimo, protecciones para las infraestructuras

críticas y la implementación de una cibergobernanza global.

Los esfuerzos actuales claramente han sido insuficientes en una era digital. Países como Estados Unidos, China y Rusia han estado estableciendo doctrinas para el uso del ciberespacio y la ciberdefensa, lo que conduce al posible surgimiento de reglas de participación de facto. Sin embargo, los riesgos de un error de cálculo catastrófico también están creciendo.

Considerando los tres escenarios planteados en este ensayo se deben establecer políticas públicas nacionales e internacionales para afrontar el problema, y así mantener la ciberseguridad de la conectividad que se tiene actualmente. La historia mundial está plagada de conflictos. El mundo de hoy es muy frágil; en él, los ciberdelincuentes persiguen la información y el dinero y, cada vez más, buscan socavar la integridad de las naciones y de sus instituciones que, en el corto y mediano plazo, pueden producir ciberguerras y generar mayor inestabilidad en el mundo contemporáneo. Si no se instrumentan esas acciones el mundo pasará a ser el mundo de las cuatro i (ies): irrelevante, inconsistente, incompetente e ineficiente. En pocas palabras, negligente. Es una tarea a la que estamos convocados todos: los proveedores de servicios, los consumidores y todos los que proveen algún tipo de bien a través del ciberespacio. Tomando en cuenta los tres escenarios planteados en este ensayo se deben orientar las estrategias hacia el establecimiento de instrumentos a nivel normativo, estratégico y operativo para afrontar el problema, y así preservar la condición de ciberseguridad.

Tenemos que pensar y actuar global y localmente. No es una cuestión de carácter local sino un reto que estamos enfrentando todos los países, todas las instituciones públicas o privadas y todos los seres humanos en su conjunto.

Por ello, para evitar esos riesgos debe establecerse una cibergobernanza global: La ciberseguridad diplomática es un problema de orden transversal y de seguridad multidimensional pública nacional e internacional. La Cámara de diputados y de senadores de México, en 2021, propuso la suscripción de un convenio latinoamericano de ciberseguridad y la adhesión de México al *Convenio sobre la ciberdelincuencia* o *Convenio de Budapest* respectivamente.

Las Naciones Unidas han estado facilitando discusiones sobre ciber normas desde 2004. En esa tesitura, el CyberPeace Institute presentó una iniciativa para mejorar la estabilidad del ciberespacio con el respaldo de Microsoft, Mastercard, la Fundación Hewlett y otros patrocinadores corporativos. Tenemos que adaptarnos a la nueva realidad internacional en un entorno de ciberseguridad internacional ante la problemática que se da en el ciberespacio, como se muestra en las siguientes tres fotografías. En ellas destacan los 4.4 millones de dólares como costo promedio mundial por la filtración de datos y que

el 69% de las organizaciones que pagaron un rescate fueron atacadas más de una vez.

No hay un tratado global sobre la IA, aunque sí cooperación técnica en foros multilaterales para intercambiar mejores prácticas. El informe de la ONU 2023 *Algorithms and Terrorism* destaca el escenario de enjambres de micro drones autónomos con reconocimiento facial, que seleccionan a las víctimas con el uso de la IA. Y en tal sentido se busca la cooperación internacional para combatir el crimen organizado.

Asimismo, en el tercer informe del GEG de la ONU, por primera vez, los 20 países que lo integran entre ellos, EE. UU., China y Rusia, acordaron la creación de un código de conducta responsable en el ámbito de ciberseguridad, pero de una manera sistémica y libre de confrontación. En dicho informe se indica que las recomendaciones son de carácter voluntario y no obligatorio.

Cuando la comunidad internacional haya madurado y se dé cuenta de la gran importancia que representa la ciberseguridad para todos, esas normas podrían adquirir un carácter jurídicamente vinculante. Estos son los barruntos en búsqueda de una gobernanza internacional en la materia.

La Declaración Bletchley busca cumplir los objetivos clave de la cumbre europea al establecer un acuerdo y una responsabilidad compartidos sobre los riesgos, las oportunidades y un proceso de avance para la colaboración internacional en la investigación y la seguridad de la IA. Todo lo anterior, y a pesar de la Declaración Bletchley generada en el marco de la Cumbre de Seguridad de la Inteligencia Artificial, ha generado una serie de acciones en las empresas digitales.

En 2025, Europol puso en marcha el Grupo Operativo Grimm. Reunió a agencias de ocho Estados europeos para combatir las plataformas delictivas. Es evidente que:

Existen desafíos importantes, especialmente en lo que respecta a la ciberseguridad y los riesgos de la desinformación, las oportunidades para una diplomacia más directa, eficiente y transparente son inmensas. A medida que las naciones continúan adaptándose a este nuevo mundo digital, serán aquellas que adopten la tecnología e innoven en sus esfuerzos diplomáticos las que prosperarán y moldearán el futuro de las relaciones globales. (Diplomat Today, 2025).

Cada país lidia con el problema según sus capacidades: las naciones avanzadas tecnológicamente mantienen a raya la mayoría de las amenazas, mientras que las regiones más inestables sufren en mayor medida la brecha tecnológica (Torres, 2026, p. 17). Esto en virtud de que “hoy vivimos luchas geopolíticas y geoeconómicas, pero sobre todo estas son las luchas por las conquistas de nichos de mercados” (Roldán, 2023, p. 63). Uno de los ejemplos es la Agencia de Seguridad Cibernética y de Infraestructura (Cybersecurity and Infrastructure Security Agency) de EE. UU. o CISA encargada de la ciberseguridad

nacional y protección de infraestructuras (CISA, 2023-2024). Es el mismo caso de la Agencia de Ciberseguridad de la Unión Europea que, entre otras cuestiones, ha propuesto la Ley sobre IA (ENISA, 2023). Asimismo, la Organización del Tratado del Atlántico Norte (2024), en una reunión sostenida en julio de 2024, adoptó medidas para adaptarse a los desafíos cibernéticos, amenazas híbridas, la IA y la cooperación en la ciberdefensa, entre otras cuestiones.

No obstante, en los países de América Latina y el Caribe, el debate sobre la cooperación ciberdiplomática entre los proveedores de inteligencia artificial y las autoridades de justicia penal en la identificación de actividades delictivas está ganando relevancia. Tanto la Ley Modelo Regional sobre Inteligencia Artificial y Delincuencia de EL PACCTO 2.0 como la Ley Marco Regional sobre Inteligencia Artificial y Delincuencia ofrecen marcos alternativos para que los países puedan regular las áreas identificadas.

En síntesis, hay avances al respecto por parte de instituciones internacionales y nacionales de prestigio que han estado haciendo análisis rigurosos sobre la temática central de este ensayo, tales como el SELA sobre *Inteligencia Artificial y Diplomacia: Las relaciones internacionales en la era de las tecnologías disruptivas* (2024), la Diplo Foundation sobre *Digital diplomacy in 2026: Geopolitics, new topics & tools*, EE.UU. con su *United States International Cyberspace & Digital Policy Strategy* (2021-2026). Además, se han estado desarrollando operaciones exitosas de ciberatribución por parte del Grupo Operativo Grimm de Europol (2025), la Open-Ended Working Group (OEWG) de la ONU en ciberseguridad (2025), la International Counter Ransomware Initiative (CRI) de EE.UU. y la cooperación UE-LAC. No obstante, se requiere agilizar y profundizar la cooperación internacional aún más en estos temas en los que el mundo convulso de hoy está inmerso.

Conclusiones

Las nuevas tecnologías, y la IA dentro de ellas, están desempeñando un papel crucial en el desarrollo de las naciones. La IA debe centrarse en mejorar las capacidades humanas, en la empatía, en la ética, en la seguridad y en la confianza. La IA debe utilizarse para el beneficio de la supervivencia y la prosperidad de la humanidad. No para su destrucción. Algunos sectores privados y públicos han utilizado la IA, ya sea para informar o desinformar y divulgar mensajes verdaderos o falsos.

Ese es el desafío que tenemos frente a ella. El objetivo esencial debiera ser siempre buscar el beneficio de la humanidad para su bienestar. Es indispensable avanzar en la regulación y en el comportamiento responsable de los Estados en el ciberespacio, pues sólo si la comunidad internacional entiende la relación entre la IA y los conflictos en el ciberespacio, como un

fenómeno global, se podrá avanzar realmente hacia una regulación significativa. El objetivo es lograr estabilidad, certidumbre y gobernabilidad internacional duradera.

Para lograr estabilidad, certidumbre y gobernabilidad duradera en el ciberespacio, los gobiernos deben decidir si les conviene aceptar límites a la forma en que despliegan capacidades cibernéticas ofensivas en pos de objetivos políticos y estratégicos.

Insisto: para lograr esto, los gobiernos, las organizaciones internacionales, las empresas, las ONG y los ciudadanos comunes deberían trabajar juntos para crear conciencia sobre los riesgos que la explotación maliciosa de Internet representa para la vida y los medios de vida de las personas.

Todo lo antes escrito nos obliga a reflexionar sobre la importancia de la IA, la diplomacia digital y la ciberdiplomacia, sus beneficios, su uso múltiple en el mundo global de hoy, y los desafíos a los que nos enfrentamos.

En estos tiempos de retos geopolíticos y geoeconómicos, el rápido desarrollo de tecnologías disruptivas tiene un efecto transformador en la política y en las economías de las sociedades. La ciberdiplomacia de los Estados es un elemento vital para garantizar la buena gobernanza global del ciberespacio.

Hemos explicado la intersección entre inteligencia artificial (IA), diplomacia digital y ciberdiplomacia en el contexto geopolítico y geoeconómico del siglo XXI. Asimismo, hemos planteado la distinción analítica entre diplomacia digital (uso de herramientas digitales para fines diplomáticos) y ciberdiplomacia (uso de herramientas diplomáticas para resolver asuntos del ciberespacio internacional), hemos expuesto el énfasis en sus riesgos éticos y la llamada a una gobernanza global responsable con elementos sólidos y coherentes.

Es evidente que sobre la temática analizada resulta imposible predecir el futuro. Pero es posible identificar lo que es probable y descartar lo que es altamente improbable. Lo cierto es que los escenarios representativos se han basado en un análisis detallado de megatendencias.

Consecuentemente, las prioridades deben ser: En primer lugar, participar estratégicamente en todos los foros multilaterales pertinentes y salvaguardar el modelo multilateral de gobernanza del internet. En segundo lugar, robustecer la diplomacia digital para configurar una conectividad internacional segura y fiable.

Pero para que la diplomacia digital, de cualquier país, sea realmente efectiva debe haber una correspondencia entre lo que se difunde y el quehacer doméstico. El país debe fortalecer su Estado de derecho, su transparencia y su sistema de justicia, de rendición de cuentas y de seguridad pública e interna; combatir la corrupción, la impunidad y la

delincuencia; promover la democracia y los derechos humanos; fortalecer la sociedad civil y las libertades de prensa y de expresión; robustecer su economía, las oportunidades económicas y su sector productivo; profundizar la equidad y su sustentabilidad; reducir sus vulnerabilidades frente al exterior; desempeñar un papel activo y responsable en el mundo y diversificar sus nexos diplomáticos y su comercio internacional.

Por todo lo anterior, propongo la adhesión plena de México al *Convenio de Budapest*, la creación de una Unidad de Ciberdiplomacia en la Secretaría de Relaciones Exteriores de México y su participación en el IGF 2026. 🌐

Referencias

- Álvarez, D. (2022). La diplomacia en la era digital: Un diálogo sobre los procesos de transformación diplomática surgidos a raíz de los avances tecnológicos. *Relaciones Internacionales*, (48), 173–193.
- Baena, G. (Coord.). (2015). *Planeación prospectiva estratégica: Teorías, metodologías y buenas prácticas en América Latina*. Universidad Nacional Autónoma de México, Facultad de Ciencias Políticas y Sociales.
- Benanti, P. (2024). *La era digital: Teoría del cambio de época*. Ediciones Encuentro.
- Briones, J. (2020). *La humanización de la era digital*. Catarata.
- Cybersecurity and Infrastructure Security Agency. (2023). *Roadmap for artificial intelligence*. U.S. Department of Homeland Security. <https://www.cisa.gov/ai>
- Clark, J., et al. (2021). *Comunicaciones digitales*. Ariel.
- Clarke, R. A., & Knake, R. K. (2011). *Guerra en la red: Los nuevos campos de batalla*. Ariel.
- Cuenca Orozco, D., et al. (2023). *Tecnologías digitales en la comunicación política del gobierno de la 4T: Internet, redes sociodigitales, streaming y videojuegos*. Universidad Nacional Autónoma de México.
- DiploFoundation. (2026). *Digital diplomacy in 2026: Geopolitics, new topics & tools*. <https://www.diplomacy.edu/topics/digital-diplomacy/>
- Diplomat Today. (23 de diciembre de 2025). The new age of digital diplomacy: Transforming global relations in 2025. <https://diplomattoday.com/the-new-age-of-digital-diplomacy-transforming-global-relations-in-2025/>
- Agencia de la Unión Europea para la Ciberseguridad. (2023). *Informe sobre ciberseguridad de la IA*.
- Franco, P., & Ramírez, A. (2022). *Era digital: Enemiga o aliada*. SER Editorial.
- Gracia, A., et al. (2022). *Comunicación y vida cotidiana en la era digital*. Universidad Nacional Autónoma de México.
- Henley & Partners. (2026). *Global passport ranking*. Henley Passport Index. <https://www.>

henleyglobal.com/passport-index

- Kissinger, H. (Junio de 2018). *How the Enlightenment ends*. The Atlantic. <https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/>
- Lakomy, M. (2023). Artificial intelligence as a terrorism enabler? Understanding the potential impact of chatbots and image generators on online terrorist activities. *Studies in Conflict & Terrorism*. <https://www.tandfonline.com/doi/full/10.1080/1057610X.2023.2259195>
- Medina, M. (2016). *La comunicación y su estructura en la era digital*. Centro de Estudios Financieros.
- Miklos, T., & Arroyo, M. (2008). *Prospectiva y escenarios para el cambio social*. Universidad Nacional Autónoma de México.
- NMás. [@n.mas]. (13 de noviembre de 2025). ¿Existe una relación entre la riqueza y el poder del pasaporte? [Publicación de Instagram]. Instagram. <https://www.instagram.com/p/DRBIcrAk21R/>
- Nicolson, H. (1994). *La diplomacia* (3.ª ed.). Fondo de Cultura Económica.
- Organización del Tratado del Atlántico Norte. (9–11 de julio de 2024). Cumbre de la OTAN en Washington, D. C., 9-11 de julio de 2024. <https://es.washington.org/meeting/nato-summit-2024>
- Perera, R., & Dorantes, G. (2023). *Tuiteando desde el poder: Nuevas tecnologías, viejas estrategias*. Universidad Nacional Autónoma de México.
- Roldán, E. (2023). Prospectiva de la seguridad financiera hacia el 2030. En J. Ávalos (Coord.), *Brújula Hemisférica: Desarrollo de capacidades prospectivas y estudios de futuros para las decisiones en seguridad de América Latina*. Centro de Estudios Superiores Navales; Instituto de Investigaciones Estratégicas de la Armada de México.
- Roldán, E. (2024). La lucha por la nueva hegemonía mundial, los semiconductores y la relocalización. *Anuario Mexicano de Asuntos Globales*, 2(2), 61–84. <https://doi.org/10.59673/amag.v2i2.67>
- Roldán, E. (2025). La inteligencia artificial y el mundo global. *Anuario Mexicano de Asuntos Globales*, 3(3), 15–38. <https://doi.org/10.59673/amag.v3i3.82>
- Secretaría de Relaciones Exteriores. (2011). 2010. *Celebraciones de México en el mundo*. Acervo Histórico Diplomático.
- Sistema Económico Latinoamericano y del Caribe. (2024). *Inteligencia artificial y diplomacia: Las relaciones internacionales en la era de las tecnologías disruptivas*. <https://www.sela.org/publicaciones/inteligencia-artificial-y-diplomacia-las-relaciones-internacionales-en-la-era-de-las-tecnologias-disruptivas/>
- Serrano, B. (2025). *Ciberdiplomacia y diplomacia corporativa: Claves para la ciberseguridad*. Barcelona Supercomputing Center. <https://www.bsc.es/>

- Torres, M. (2026). *El impacto transformador de la inteligencia artificial en el terrorismo: Horizonte 2035* (Documento Marco IEEE N.º 01/2026). Instituto Español de Estudios Estratégicos. <https://www.defensa.gob.es/ceseden/-/ieeee/ia-terrorismo-horizonte-2035>
- World Economic Forum. (2025). *The global risks report 2025*. <https://www.weforum.org/reports/global-risks-report-2025/>