

Panorama tecnológico actual

*Una mirada a este entorno, por parte de la entrevistada
Mónica Flórez Cáceres.*

DOI: 10.29236/sistemas.n180a3

Desde la vista de relaciones internacionales y los conflictos actuales ¿cómo ha cambiado la dinámica de los conflictos en el contexto del ciberespacio?

Las dinámicas de los conflictos han cambiado profundamente desde la aparición de nuevas tecnologías, basta con observar las reflexiones de Mary Kaldor hacia finales del siglo XX, para observar cómo los conflictos se transformaban por la erosión de los Estados y el surgimiento de actores asimétricos, así como por la aparición de nuevas herramientas y “espacios” que dieron lugar a lo que en su momento la

politóloga denominó guerras virtuales y del ciberespacio.

Así, la consolidación del ciberespacio como quinto dominio de la guerra en la doctrina militar estadounidense y de la OTAN¹, primordialmente, ha permitido analizar este escenario desde dos perspectivas: como uno de los ejes transversales de apoyo a los otros dominios (tierra, mar, aire y ciberespacio) y como un

¹ Véase: Fuente, I. (2022). La OTAN y el Ciberespacio: Un nuevo dominio para las operaciones. En: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/LaOTAN_ciberespacio.pdf

dominio en sí mismo que desafía la triada de Clausewitz referente a la letalidad, la instrumentalización y el objeto político que caracterizan a una guerra tradicional.

No obstante, lo que sí es indiscutible es que ha dado sentido a la hibridez como la descripción exacta del desarrollo de los conflictos actuales, que no solo se valen de medios tradicionales para desestabilizar al oponente, sino que potencian su actuar con métodos que se tornan contundentes con la mediación de la tecnología, la inexistencia de fronteras en el mundo cibernético, el anonimato de la actuación, la rapidez de los efectos y la masificación de sus efectos.

Siempre traigo a colación el ejemplo del ciberataque a las gasolineras iraníes en diciembre de 2023, el 70% de las gasolineras del país quedaron paralizadas. Así pregunté siempre al público ¿qué sucedería si una sola tarde en su ciudad se dejara de suministrar combustible? Creería que las imágenes apocalípticas han embargado siempre las mentes de mis interlocutores. Ahora bien, al reflexionar sobre las probabilidades de caos total, ha de resaltarse que para ello no hubo necesidad de movilizar tropas, lanzar misiles, volar helicópteros, solo bastó un clic... un solo clic.

Esa es la dinámica que ha cambiado, tal vez ahora no ha sido tan evidente la letalidad de un ciberataque, pero lo que si es cierto es que

puede desestabilizar a un país entero si se afecta la infraestructura crítica cibernética, por demás desprotegida en países que no han priorizado la temática dentro de su agenda de seguridad y defensa nacionales.

Adicionalmente, desde el estudio de la geopolítica crítica² hay un aspecto relevante para el análisis de los conflictos internacionales actuales y es la construcción y masificación de discursos. Es decir, cada acción en el marco de un conflicto va acompañado de la construcción de una narrativa que se masifica gracias a la existencia de las redes sociales, siendo un canal directo para la influencia en la opinión pública, aquella que tanto importa en los procesos electorales y en la legitimación del actuar de los gobiernos o de los tomadores de decisiones.

Las palabras importan, aún más cuando hacen parte de estrategias de “soft power”³ que moldean las voluntades y los intereses de una audiencia inmersa en un mar de sobreinformación, posverdad, y apasionamientos que polarizan, segmentan y generan fracturas que perpetúan y profundizan las diná-

² Véase: Cabrera Toledo, Lester. (2020). Geopolítica crítica: alcances, límites y aportes para los estudios internacionales en Sudamérica. *Foro internacional*, 60(1), 61-95. Epub 15 de abril de 2020. <https://doi.org/10.24201/fi.v60i1.2574>

³ Véase: Ahmed, Shahla. (2025). El poder blando en la era digital. Rn: <https://saisreview.sais.jhu.edu/the-role-of-soft-power-in-the-digital-age/>

micas conflictuales. Así, podría concluirse, sin ánimo de ser generalistas (porque el debate es profundo, largo y complejo) que el ciberespacio como medio, como fin y como escenario, transforma día a día las dinámicas conflictuales, añadiendo herramientas poderosas que pueden equilibrar la balanza entre actores que tienen diversas capacidades militares y económicas, rediseñándose así el panorama de las guerras y conflictos actuales.

Obsérvese el caso de la guerra ruso-ucraniana, ello ha moderado, incluso, las voces analistas que solían predecir el desenlace de las historias: si bien hay un sinnúmero de factores, indiscutiblemente la mediación de tecnología ha dado un margen de ventaja a la que se consideraba un actor que caería rápida y estrepitosamente ante el poder militar y económico ruso. Hasta la dinámica analítica de ellos conflictos ha cambiado, la perspectiva es tal vez hoy una de las tareas más difíciles de completar.

¿Cómo se observan las tensiones internacionales alrededor de la tecnología? ¿como habilitadores de nuevos conflictos o como aceleradores del desarrollo de armas más avanzadas?

Definitivamente como ambas. Tal y como se planteaba en la respuesta anterior, el ciberespacio puede ser analizado como medio, como fin o como herramienta. Así, bajo las circunstancias planteadas, la faci-

dad de acceso, el anonimato y el gran alcance de los ciberataques, la desinformación y otras tantas acciones llevadas a cabo en el entorno digital, facilita la escalada de los conflictos a estadios más complejos, violentos y difíciles de desescalar.

A su vez, el perfeccionamiento de ataques que pueden, por ejemplo, amenazar el abastecimiento de energía eléctrica de una ciudad y el funcionamiento de las plantas de suplencia, podría generar caos, inestabilidad e incluso muertes numerosas, pensando, por ejemplo, en el caso de hospitales que tengan pacientes dependientes de maquinaria que pueda verse afectada por este tipo de acciones, incluso, terroristas.

Así mismo, en escenarios de amenaza la innovación se activa, ello se puede constatar en asuntos como la invención del radar o el avance de la aviación que se dio en contextos de guerra, por mencionar algunos ejemplos. En este sentido, la posibilidad de ser atacados y, la clásica paradoja de Relaciones Internacionales del “Dilema de Seguridad”⁴, conlleva a que los Estados, en primera medida, y los actores en confrontación, hallen formas de blindarse y superar en poder militar al oponente.

⁴ Véase: Jordán, Javier. (2020). El dilema de seguridad en las relaciones internacionales. En: <https://global-strategy.org/dilema-seguridad/>

Por ello, desde la posibilidad de defenderse y atacar con drones, de realizar ciber espionaje, operaciones cognitivas, ataques a la infraestructura crítica cibernética entre otras, se abre la posibilidad al desarrollo de nuevas armas o su fortalecimiento para adquirir o acumular más poder, en especial en un contexto en el que proliferan los conflictos asimétricos y los actores de diferente estatus al estatal, buscan desestabilizar por diversos medios.

¿Cómo se puede entender estas tensiones de la geopolítica digital en el contexto de Colombia? ¿Estamos poniendo atención a las dinámicas internacionales en estos temas?

Se debe revisar desde la óptica de quien hay atención o no. Es decir, desde la academia y, particularmente, desde el estudio de los conflictos en programas de educación superior, hay un apetito creciente por entender cuáles son las dinámicas conflictivas actuales.

En los anaqueles de las bibliotecas de las universidades del país reposan numerosas investigaciones sobre la temática, pero sin que ello refleje un apetito similar a nivel de la agenda política.

Si bien ha sido creciente el interés de los tomadores de decisiones de diversos sectores sobre la geopolítica actual (tanto en el plano tradicional, como en el ciberespacio), no podría afirmarse que existe un lugar prioritario en la agenda. Las

relaciones con socios tradicionales y las actividades, también tradicionales, en la interacción con el sector externo, siguen siendo la prioridad.

De hecho, ha sido objeto de análisis constante el nivel de conciencia geopolítica de los tomadores de decisiones en el país y, particularmente, de quienes han dirigido la política exterior colombiana desde inicios de la vida republicana, no solo por una realidad cambiante y compleja que por largos periodos se ha observado desde la óptica de grandes aliados, sino por el reconocimiento de lo que somos como país.

Por otro lado, para el sector privado existe una preocupación creciente por la ciberseguridad, pero no necesariamente por la geopolítica asociada a las dinámicas conflictivas que derivan en los incidentes de seguridad que vulneran los negocios, probablemente menos del 1% de los encargados de ciberseguridad de las empresas privadas en el país podrían afirmar que la conexión de Hezbollah con algunas redes criminales en Iberoamérica pueden constituirse en una amenaza para la continuidad de su negocio, lo que revela la desconexión entre hechos y causas inmediatas, y contextos algo más profundos y complejos.

Del mismo modo, para el público en general, el tema sigue siendo aún muy desconocido. Si bien la mayo-

ría puede conocer que hay un conflicto entre Palestina e Israel, o entre Rusia o Ucrania, no hay un conocimiento profundo sobre el contexto geopolítico tras aquellos casos, y tras la veintena de conflictos de diversa intensidad que actualmente se documentan en instituciones especializadas como la International Crisis Group.

El conflicto interno y la diversidad de retos que se afrontan como país hacen que la observancia de asuntos internacionales se limite a ciertos sectores, incluso en la academia. Es natural ante un escenario que ya brinda de por sí suficientes elementos para estudiar y, por supuesto, para procesar y sobrevivir.

Frente al aumento de ciberataques en diferentes regiones del mundo, y la incorporación de la IA como herramienta dual (defensa y ataque) ¿qué reflexiones se plantean frente a un escalamiento del ciberconflicto que se tiene en la zona gris de las tensiones internacionales?

Podría hacerse un análisis similar al realizado en la post Segunda Guerra Mundial y la consolidación de las armas nucleares como referente de poder militar. Si bien ningún ciberataque ha alcanzado el nivel de destrucción de “Little Boy” y “Fat Man”, si se plantearon en su momento serios cuestionamientos sobre la racionalidad de los actores en un escenario de confrontación, sabiendo que es eminente el poder de destrucción total.

Así, retomando la reflexión sobre el dilema de seguridad como un asunto clásico en el estudio de Relaciones Internacionales, el surgimiento de nuevas armas, tácticas y escenarios, remiten a la pregunta sobre qué tan lejos puede ir un actor racional, sin conocer a ciencia cierta cuál podría ser la respuesta de su adversario, precisamente sabiendo que la IA y las nuevas tecnologías son duales.

Por ello una escalada significativa no habría de esperarse si se sigue la lógica del actor racional. Ahora bien, en un complejo tablero geoestratégico, puede haber un error de cálculo que termine en un caos sin precedentes, guiados además por la mera intuición, pues una vez más se reitera: el anonimato en la actuación en el ciberespacio hace casi imposible la atribución a un actor particular de un hecho que pueda abrir el camino a una escalada.

Eventualmente denominaron al orden internacional como un orden del terror, por la posibilidad de una guerra nuclear, infortunadamente se siguen sumando elementos que refuerzan este rotulo y que hacen que la tarea de prospectiva sea un imposible, ante la mutación acelerada de la manera en la que se desarrollan los conflictos.

¿Qué recomendaciones se podría ofrecer a la región latinoamericana frente las operaciones cibernéticas encubiertas y abiertas que los estados desarrollados están desple-

gando en zonas de conflicto en la actualidad?

La primera recomendación es que desde la agenda política y la doctrina militar se aprehenda los conceptos asociados al ciberespacio como amenazas a la supervivencia física y digital del Estado. Si bien la preocupación es creciente, la toma de medidas específicas no permite que la brecha digital se cierre, quedando a merced de la disponibilidad de recursos e información de los aliados estratégicos tradicionales.

Si bien la postura latinoamericana nunca ha sido de ataque, si es necesario entender cómo todas las dinámicas conflictivas globales se interconectan e impactan en un mundo altamente interdependiente. Si bien han sido crecientes los debates sobre la globalización, si es cierto que siguen estando abiertos los canales de intercambio de información, bienes, personas, capitales, etc., lo que de por sí es natural, pero que resulta preocupante cuando hace parte de la estrategia de forta-

lecimiento del terrorismo internacional y el crimen transnacional, solo por mencionar dos aspectos.

Es menester tener consciencia geopolítica sobre las propias condiciones físicas y ciberespaciales, así como de la vulnerabilidad ante las realidades que cada vez se acercan más al ámbito latinoamericano, entendiendo que hacemos parte de lo que hace unos párrafos recordé como el tablero geoestratégico, en el que podemos quedar en medio de un fuego cruzado o, de unos clics cruzados.

De fondo, la educación y, de manera más avanzada, la voluntad política, podrán priorizar la atención al ciberespacio, no solo desde una mirada meramente exploratoria, para poder entender lo que sucede y cómo podría afectarnos, más que para responder críticamente a favor o en contra de actores extrarregionales, sino para blindarnos frente a los actos y actores que, solo por un efecto colateral, podrían vulnerarnos. 🌐