

Capítulo 7

La guerra y el liderazgo estratégico en la era de la computación cuántica*

DOI: <https://doi.org/10.25062/9786287602861.07>

Camilo Bolaños Jiménez

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: En el presente capítulo se realiza un breve análisis de la computación cuántica como tecnología disruptiva y emergente en el marco del liderazgo estratégico, teniendo en cuenta las guerras de quinta generación. En el capítulo se hace un recorrido histórico y una explicación de conceptos en torno a este extraordinario avance científico-tecnológico. Posteriormente, se aborda el impacto que tiene en la ciberseguridad y la ciberdefensa, respecto a lo cual se argumenta que la tecnología cuántica tiene una especial importancia para los estudios estratégicos, particularmente por la inestabilidad y la complejidad de la geopolítica frente a la seguridad y la defensa nacionales. Finalmente, se describe la posición de la Organización del Tratado del Atlántico Norte al respecto y se desarrolla la teoría de la comunicación humana, enfocada en la prevención de nuevos vectores de ataque que ponen en riesgo las políticas y las estrategias de protección en el ciberespacio.

Palabras clave: ciberdefensa; ciberseguridad; computación cuántica; liderazgo estratégico.

* Capítulo de libro resultado del proyecto de investigación "Conceptualización de los estudios estratégicos contemporáneos", de los grupos de investigación "Centro de Gravedad", categorizado en A por Minciencias, "Masa Crítica" (A1) y "Memoria Histórica, Construcción de Paz, Derechos Humanos, DICA y Justicia" (A), de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Camilo Bolaños Jiménez

Teniente Coronel (R) de la Policía Nacional de Colombia. Especialista en Seguridad del Centro de Estudios Superiores de la Policía Nacional de Colombia. Profesional en Criminalística, Escuela de Cadetes "General Santander", Colombia. Doctorando en Estudios Estratégicos, Seguridad y Defensa, y magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto, Colombia. Consultor en Ciberseguridad.

<https://orcid.org/0009-0005-8847-8491> - Contacto: camilo.bolanos@esdeg.edu.co

Citación APA: Bolaños Jiménez, C. (2024). La guerra y el liderazgo estratégico en la era de la computación cuántica. En S. Uribe-Cáceres & D. López Niño (Eds.), *Guerra, estrategia y liderazgo: cómo los líderes forjan la historia* (pp. 155-184). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602861.07>

GUERRA, ESTRATEGIA Y LIDERAZGO: CÓMO LOS LÍDERES FORJAN LA HISTORIA

ISBN impreso: 978-628-7602-85-4

ISBN digital: 978-628-7602-86-1

DOI: <https://doi.org/10.25062/9786287602861>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes prieto"

Bogotá D.C., Colombia

2024



Introducción

Los extraordinarios avances tecnológicos de las últimas décadas han influido de diferentes formas en los intentos por solucionar los innumerables problemas que aquejan a la humanidad. Sin embargo, también originan nuevos riesgos que amplían los vectores de ataque, como el incremento ostensible de delitos informáticos, las violaciones a los sistemas informáticos o los ciberataques en una sociedad cada vez más hiperconectada, donde la comunicación es una condición *sine qua non* de la vida humana y el orden social.

Este documento, basado en la teoría de la comunicación humana y en estudios estratégicos, examina cómo las amenazas asimétricas, impulsadas por la computación cuántica, evolucionan en el ciberespacio. Estas innovaciones permiten a organizaciones de cibercrimen transnacional desarrollar armas sofisticadas que desafían la seguridad nacional. En tal contexto, el liderazgo en la defensa cibernética es crucial porque estas amenazas ponen en riesgo las infraestructuras críticas y, por ende, pueden afectar el suministro de bienes y servicios esenciales, así como, en última instancia, comprometer la democracia y el bienestar de los ciudadanos en tiempos de guerra.

Justamente, el objetivo del capítulo es contribuir al fomento de una conciencia nacional de defensa. En particular se resalta que la computación cuántica, como herramienta poco convencional, incidirá en los resultados de las denominadas guerras de quinta generación, en las cuales la evolución de los conceptos de *información* y *tecnología* es determinante. Asimismo, estos avances tecnológicos tienen gran variedad de recursos que son valiosos para respaldar las políticas y las estrategias de ciberseguridad y ciberdefensa, con el objetivo de disminuir el impacto de los vectores de ataque existentes en los diferentes entornos digitales.

La tesis planteada en el presente capítulo enfatiza en la necesidad de comprender la importancia que tiene la computación cuántica como eje central de la

problemática alrededor de las nuevas amenazas contra la seguridad y la defensa de las naciones. Por consiguiente, se requieren teorías que coadyuven a su entendimiento y líderes estratégicos con visión proactiva que guíen el camino para abordar y enfrentar con conciencia situacional esta era de revolución digital. Se subraya entonces el peso de la academia en los saberes concernientes a la seguridad, la defensa, la prevención de ciberconflictos, las ciencias sociales, la ciberseguridad, la ciberdefensa, la ética y la guerra.

La teoría de la comunicación humana planteada por Watzlawick et al., (1991) establece que la comunicación está presente desde la génesis de la existencia humana, por lo tanto, a medida que la sociedad avanza, elementos subyacentes y nuevos conceptos de intercambio de información se van adaptando. Así pues, los principios de esta teoría constituyen un factor clave en los diversos modelos de intercambio de datos en el ciberespacio, pues contribuyen a determinar los riesgos asociados a un mundo digitalizado en el cual la relación emisor-receptor es vital.

Adicionalmente, la acelerada globalización ha conducido a que las naciones realicen continuos procesos de comercialización más eficientes para fortalecer sus sectores económicos, sociales, políticos y militares. Dado que el ciberespacio ha dispuesto un camino sin fronteras que facilita esas negociaciones, es importante que la academia contribuya a debatir y analizar en profundidad esos complejos cambios, de tal manera que provea elementos para entender los modernos procesos tecnológicos que se están desarrollando actualmente y aportar así a la formación de una sociedad digital más segura.

Específicamente, en este capítulo se aborda la computación cuántica como eje para comprender y asimilar las nociones de las diferentes áreas de aplicación del pensamiento crítico cibernético dirigido a la seguridad y la defensa. Con este propósito, también se analiza el tipo de liderazgo estratégico que exige la era de la computación cuántica en la guerra, teniendo en cuenta que en la actualidad no se concibe la composición de un Estado y una sociedad sin el uso de sistemas y redes informáticas conectados permanentemente a internet, con los riesgos inherentes que conlleva el uso del ciberespacio, denominado el quinto dominio, junto con el mar, la tierra, el aire y el espacio.

Aproximación histórica y conceptual de la computación cuántica

En los últimos 200 años, la tecnología y las formas de comunicación han experimentado transformaciones radicales y rápidas. Desde las cartas y el telégrafo hasta el teléfono fijo, y posteriormente el celular y las redes sociales, cada avance

ha marcado un hito en la historia de la comunicación humana. Impulsada por el internet, esta evolución ha sido constante y cada nueva invención se considera un avance definitivo, pero la experiencia ha demostrado que poco después será superada por otra innovación. Hoy en día, la comunicación se encuentra en la era de la electrónica, la ciencia computacional, la inteligencia artificial, el hardware, el software y la computación cuántica (Barreno et al., 2016).

La comunidad académica del Doctorado en Estudios Estratégicos en Seguridad y Defensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto" está impulsando la investigación, la contextualización y la socialización de las amenazas cibernéticas contemporáneas, pues considera imprescindible generar conciencia sobre aquellas que surgen a medida que se exploran las enormes y diversas posibilidades en el ciberespacio. La preparación y el análisis del escenario futuro, donde convergen los principales aspectos de la sociedad para enfrentar los próximos riesgos poco convencionales, determinará el resultado en cuanto al aprovechamiento de las tecnologías dispuestas para la seguridad y la defensa de los Estados.

Si bien la computación cuántica se ha desarrollado gracias al aporte de connotadas personalidades del campo científico, en este capítulo se destaca a tres investigadores cuya contribución fue absolutamente relevante. En primer lugar se encuentra Alan Turing y su máquina universal, pues estableció los fundamentos con los que funcionan las computadoras de hoy en día. Además, en el campo de las ciencias militares, se debe mencionar el increíble aporte que hizo a la historia de la humanidad cuando descifró el código de la máquina criptográfica Enigma, con la cual el ejército de la Alemania de Hitler intercambiaba mensajes secretos en la Segunda Guerra Mundial, pues esto permitió salvar muchas vidas y acelerar el determinante triunfo de los Aliados en contra de las potencias del eje.

En segundo lugar, se debe señalar que la idea de la computación cuántica fue introducida por primera vez en 1982 por el premio Nobel de Física Richard Feynman. El aporte de este científico fue significativo porque propuso la simulación de sistemas basados en los principios de la mecánica cuántica por otros sistemas cuánticos. En tercer lugar, otro avance esencial lo hizo en 1985 David Deutsch, de la Universidad de Oxford, cuando describió una computadora cuántica universal apoyado en los diseños de la máquina universal que hizo Alan Turing a mediados de los años treinta (Saniz, 2001).

Con base en estos aportes, la informática se desarrolló con el propósito de realizar cálculos cada vez más sofisticados, precisos y más eficientes sobre grandes volúmenes de datos. A partir de este punto y por primera vez en la historia, el campo de la computación se ramificó con la aparición de los ordenadores cuánticos, que son capaces de hacer cálculos prácticamente imposibles para los ordenadores convencionales (Bravyi et al., 2022).

Aprovechando la teoría pura de la mecánica y la física cuántica, los científicos informáticos se encaminaron a la siguiente era de la computación. “En los últimos años se ha producido en todo el mundo un aumento espectacular de la investigación científica, así como en la inversión financiera para desarrollar un ordenador cuántico” (Metcalf & Chow, 2018). El imparable raciocinio humano lo ha llevado a crear mecanismos que las personas van acoplando al estilo de vida individual y colectivo, de manera que los adelantos tecnológicos incorporados a la sociedad han influido notablemente en la articulación de los procesos sociales del comportamiento humano.

En este escenario, los estudios estratégicos fomentan el debate necesario para confrontar y analizar los nuevos factores que pueden afectar la seguridad, al tiempo que estudian las estrategias y doctrinas que ayuden a garantizarla. En este sentido, se considera que debe ser un compromiso global transmitir estos avances tecnológicos para crear un nuevo concepto de seguridad y defensa que los incorpore mediante estudios sociológicos. De esta manera, será posible plantear una defensa general en el marco de un modelo y unos valores comunes para elevar el nivel de la cultura de seguridad y defensa en los integrantes de una sociedad altamente tecnológica (Centro Superior de Estudios de la Defensa Nacional [CESEDEN], 2023).

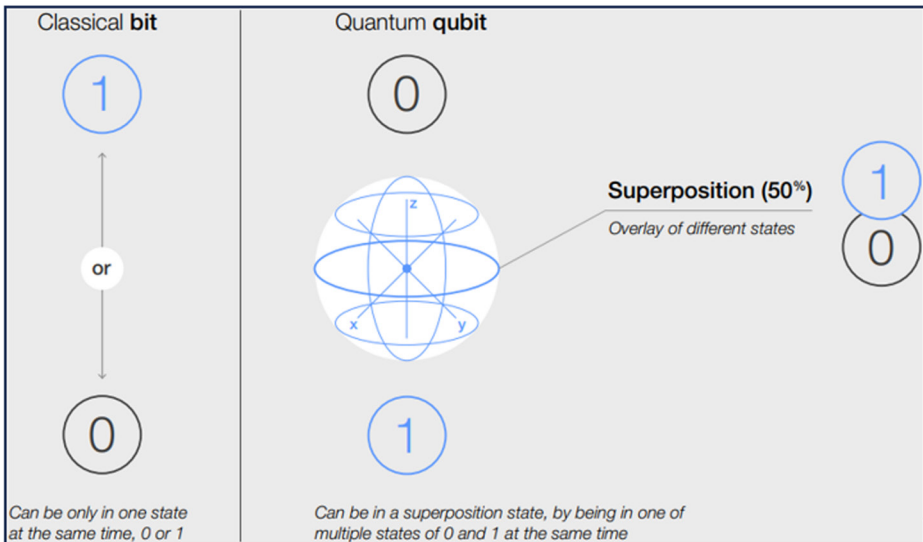
En una época marcada por la acelerada transformación digital y el surgimiento de tecnologías disruptivas como la inteligencia artificial, el *blockchain*, el metaverso y la computación cuántica, es fundamental que los Estados prioricen la seguridad y la defensa de sus ciudadanos. Cuando una nación logra establecer altos estándares de protección, su sociedad goza de mayores oportunidades para prosperar en diversos ámbitos sociales dentro de un sistema democrático sólido.

Por consiguiente, los conocimientos tecnológicos, que impactan directamente en el bienestar y el desarrollo de la población se vuelven cruciales en un contexto virtual, donde, por momentos, se pierde la noción entre la realidad y la ficción. Así, la inversión en seguridad y defensa no solo salvaguarda a la ciudadanía, sino que además sienta las bases para un crecimiento integral y sostenible en una época marcada por la innovación y la transformación digital.

Por ello, y a efectos de una comprensión significativa, se debe acotar que la computación cuántica es un área en desarrollo de la ciencia de la computación que busca explotar los descubrimientos realizados por la física cuántica para resolver problemas mucho más complejos que los que pueden analizar los ordenadores tradicionales y, por ende, de una manera más rápida y eficiente (Cobelli et al., 2022).

Como se observa en la figura 1, mientras la computación clásica trabaja con bits como unidad básica de información, la computación cuántica lo hace con qubits, es decir, bits cuánticos. Una de las principales diferencias entre los bits y los qubits es la unidad de información: en un computador tradicional se codifica en 0 o 1, en tanto que en la computación cuántica, debido a la naturaleza del principio de superposición de la materia establecido por la mecánica cuántica, el qubit puede estar codificado en diversos estados al mismo tiempo, es decir, de forma simultánea, lo cual facilita y agiliza el procesamiento de datos para la solución de cálculos complejos y de mayor envergadura (Vanegas, 2016).

Figura 1. Superposición de estados, diferencia entre bit clásico y bit cuántico (qubit).



Fuente: World Economic Forum (2022).

Esta poderosa tecnología ha surgido en un momento en el cual el auge de internet y su masificación permiten el ser humano interactuar a diario con un ecosistema digital integrado por tecnologías emergentes y disruptivas accesibles para casi cualquier persona. En tal sentido, la computación cuántica constituye un desafío significativo que obliga a la humanidad, en especial a aquellos responsables de la innovación, a adaptarse y prepararse para los profundos cambios que vienen e implican a esta tecnología. Por lo tanto, el capítulo busca proporcionar un

conocimiento tecnológico derivado del campo ciber a los estudios estratégicos para contribuir a la comprensión de estos avances.

En este contexto, la preparación para enfrentar la creciente inseguridad cibernética es una responsabilidad compartida que debe tomarse muy en serio. A medida que avanza el desarrollo de la computación cuántica, es probable que esta tecnología supere a la computación clásica, alcanzando lo que los científicos y expertos denominan *supremacía cuántica*, un término "acuñado por el físico teórico estadounidense John Preskill en 2011 que denota el supuesto poder superior de cálculo, en términos de complejidad computacional, que tendría un ordenador cuántico frente a uno clásico" (Ruiz, 2021, p. 19).

Ahora bien, la ilustración de la figura 1 sobre la composición y el funcionamiento de la computación cuántica también permite vislumbrar su potencial impacto en diversos problemas contemporáneos. En particular, los principios de esta tecnología emergente tendrán un papel crucial en áreas como la detección temprana de enfermedades, la corrección de errores en las cadenas de suministro y la optimización de procesos industriales y manufactureros, entre otros.

Sin embargo, su relevancia es aún más crítica en el contexto de la seguridad cibernética, especialmente durante la escalada de los conflictos y en las denominadas *guerras de quinta generación*. En este nuevo paradigma bélico, donde la información y la tecnología son armas esenciales, la computación cuántica podría ofrecer soluciones avanzadas para proteger las infraestructuras críticas cibernéticas, garantizar la integridad de los datos y contrarrestar amenazas informáticas de manera más efectiva, redefiniendo así las estrategias de seguridad y defensa en un entorno de guerra tradicional y guerra cibernética cada vez más complejo y dinámico.

La computación cuántica en las guerras de quinta generación

De acuerdo con Hassan y Jassim (2023), el concepto de guerras de quinta generación (en adelante 5GW, por su sigla en inglés) se refiere a guerras implosivas o guerras híbridas, pues son una ramificación de las guerras asimétricas. Consiste en un tipo de enfrentamiento en el cual se utilizan todos los métodos de guerra convencionales y no comunes, al tiempo que incorpora temas políticos, religiosos y sociales. Asimismo, durante su desarrollo se crean con frecuencia redes de cooperación entre Estados y grupos armados no estatales, pero con alguna especie de interés

común, de manera que se considera una guerra sin restricciones en la que se emplean todas las herramientas existentes y disponibles para las partes en conflicto.

En consonancia con el coronel en retiro Thomas X. Hammes (2007), del USMC United States Marine Corps, se puede afirmar que ha habido grandes cambios políticos en quién lucha en las guerras. La tendencia ya no refleja que los Estados-nación utilicen enormes ejércitos uniformados contra pequeños grupos de personas que escuetamente deciden luchar. Actualmente resulta imposible distinguir a los combatientes de simples elementos criminales y se emplea la estrategia del manejo de la información en distintos modelos sociales como un arma fundamental para lograr la victoria. Además, se usan las comunicaciones móviles y el internet para reclutar, adiestrar y efectuar el control de nuevos miembros, al tiempo que la movilización masiva se convierte en movilización individual selectiva (Hammes, 2007).

Según argumenta Qureshi (2019), en las 5GW la percepción es forjada por los algoritmos que utilizan los sistemas informáticos en el ciberespacio, los cuales la transforman en datos y, por ende, en información, de manera que perfectamente podrían convertirse en un arma letal. El papel de los medios de comunicación, el incremento ostensible de tecnología disruptiva en el ciberespacio y el auge de las redes sociales son un factor esencial para la construcción de identidades y para poder adaptar las voluntades del contrario. Todo puede ser utilizado como táctica de engaño para generar impresiones erróneas de la realidad, dado que la estrategia de proliferación, propagación y difusión de la información inclinaría la balanza de la victoria en esta especie de guerras no convencionales.

Además de los conceptos expuestos sobre las 5GW y la aparición e incorporación de modelos tecnológicos vanguardistas, se debe señalar que el carácter de la guerra es permeado con frecuencia por elementos inexplorados e indeterminados. El desconocimiento, por parte de los líderes políticos y militares, de la activa y cambiante dinámica digital debilita a los ejércitos en la demanda por mantener el control y el poder de la fuerza militar, lo cual podría conducir a un error en las operaciones militares en el ciberespacio. Por esta razón, es importante analizar un conjunto de problemas que gravitan en torno a las posibilidades del adversario, pues si este se anticipa en la comprensión de las tecnologías emergentes y disruptivas, posiblemente superaría las capacidades militares del contrario.

Lo dicho hasta aquí supone que, dadas las posibilidades digitales actuales, es factible que ocurra una ciberguerra y el campo de batalla se extienda hacia objetivos virtuales. En este escenario concreto, las ciberoperaciones se deben dirigir a las redes informáticas y a todo tipo de tecnologías de la información, enfocar los

ciberataques en la destrucción del software o hardware, el ciberespionaje y la defensa de la red. Es importante tener en cuenta que en la cuarta revolución industrial, una ciber guerra se podría librar con todo tipo de innovaciones tecnológicas, entre las cuales se destacan: “el *machine learning*, el *blockchain*, el internet de las cosas, la ciencia de datos e incluso la computación cuántica” (Gayozzo, 2021, p. 31).

Ahora bien, con el objeto de adaptar la tecnología cuántica para la defensa en una 5GW, es preciso señalar que “la primera revolución cuántica tuvo y sigue teniendo un profundo impacto en todos los aspectos de la sociedad, desde el ámbito militar y la seguridad internacional, hasta el desarrollo de armas atómicas, chips, ordenadores y navegación precisa” (Krelina & Důbravčík, 2023, s. p.). Si bien la tecnología cuántica es una disciplina con más de cien años de investigación y desarrollo, actualmente el mundo está enfrentando la *Revolución Cuántica 2.0*, o *QT*, fase en la cual se está aprovechando aún más todo el espectro de la física cuántica en el desarrollo potencial de instrumentos de guerra.

La evolución que ha tenido el proceso escalonado de la ciencia se refleja ahora en la creciente dependencia de los seres humanos en redes informáticas que influyen en las decisiones y tendencias de millones de personas. El hecho de que información sensible en diferentes ámbitos, tanto pública como privada, se exponga constantemente en internet tiene incidencia en un contexto geopolítico complejo. Esta situación plantea la posibilidad de que ocurra una guerra mundial híbrida, impulsada por los avances en la computación cuántica, cuyas consecuencias podrían ser devastadoras y llevar a la humanidad a buscar una mayor profundización filosófica para comprender y superar los desafíos que se presenten. Así, la interconexión entre tecnología y filosofía se vuelve crucial en un mundo cada vez más interdependiente.

Por ello, el manejo de la información en relación con los conceptos tecnológicos resulta esencial para el análisis filosófico de la ciencia cibernética, sobre todo si se tiene en cuenta que después de la Segunda Guerra Mundial el ser humano sufrió marcados y complejos efectos sobre el discernimiento de sí mismo. En este sentido, el poder que tiene controlar la información ha sido y será sumamente significativo, pues ha llevado a la humanidad hacia un desarrollo científico y tecnológico asombroso. La cibernética, por lo tanto, no solo surgió como “una nueva epistemología, sino que también ofreció una visión totalmente nueva del funcionamiento de los complejos sistemas interactuantes que encontramos en biología, psicología, sociología, economía y otros campos” (Watzlawick et al., 1991, p. 15).

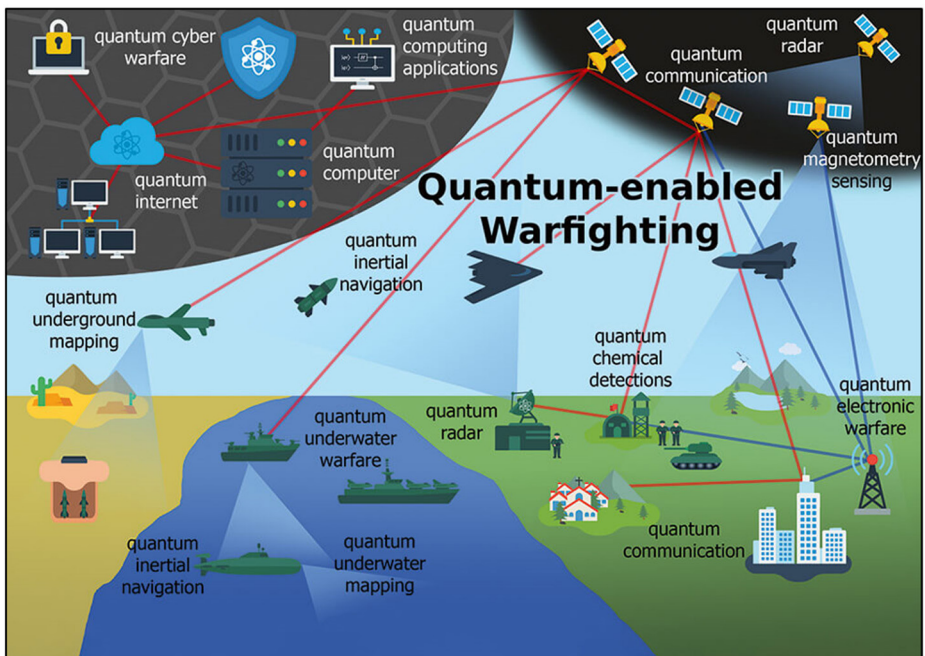
Visto desde otra perspectiva, ese juicio induce a buscar la sabiduría en teorías que fundamenten la anticipación a las amenazas, la ciberresiliencia y el

ciberespacio. En este sentido, es apenas natural considerar que la razón abordada desde las perspectivas filosóficas, estratégicas, ontológicas y tecnológicas coadyuve a prevenir vectores de ataque sofisticados que ponen en riesgo y vulneran la seguridad y la defensa nacionales.

No obstante, aunque los estudios estratégicos enfocados en la defensa pueden fundamentar esta visión proactiva para visualizar y minimizar las ciberamenazas, se debe señalar que para tener una comprensión más profunda del escenario cibercriminal es necesario ejecutar ejercicios de entrenamiento y simulación, como los que efectúa la Organización del Tratado del Atlántico Norte (OTAN), cuyas características permiten un aprendizaje efectivo. Además, es importante tener en cuenta que la cooperación internacional y las alianzas público-privadas pueden moldear el análisis de los riesgos para alcanzar una mejor resiliencia en concordancia con la comunicación humana responsable y segura (Fernández, 2023).

De esta manera se evidencia que los conceptos cuánticos son fundamentales para concebir las futuras herramientas de combate en el campo de batalla, como se muestra en la figura 2.

Figura 2. *Conceptos de guerra con sistemas quantum-enabled warfighting.*



Fuente: Krelina y Dúbravčík (2023).

Es pertinente remarcar que en la *Revolución Cuántica 2.0* se aprovecha el comportamiento de sistemas cuánticos individuales como el electrón, el átomo, el núcleo, la molécula o las cuasipartículas. Aunque la mayoría de los desarrollos y las aplicaciones cuánticas para la defensa siguen su camino investigativo, tienen gran relevancia para los Estados-Nación desde el punto de vista militar. Así lo demuestra el hecho de que las tecnologías cuánticas estén siendo ejecutadas con rigor en las agendas de los planes de defensa de naciones avanzadas, como es el caso de Estados Unidos, China, Reino Unido, Australia, India, Rusia, Canadá, entre otros. Precisamente, en el año 2021 los ministros de defensa de la OTAN aprobaron la Estrategia de Tecnologías Emergentes y Disruptivas (EDT), en la cual acordaron que la tecnología cuántica sería una de las nueve áreas tecnológicas elegidas para impulsar su investigación y aplicación (Krelina & Dúbravčí, 2023).

Other international actors are aggressively pursuing QTs. For example, the Chinese People's Liberation Army has recognized the strategic value and potential decisive advantage of QT, while the European Union has marked QT as an 'emerging technology of global strategic importance' and noted that it will be used 'for sensitive applications in the area of security, and in dual-use applications. As such, it is clear that QTs are set to play a major role in the defence strategies of nations across the world. (Krelina & Dúbravčí, 2023, p. 40)

Hecha esta salvedad, no se puede dejar de mencionar la situación militar en el panorama mundial actual, que resulta desconcertante y expectante porque están en pleno desarrollo dos guerras. Por un lado, en Europa, debido a la ocupación de Rusia en Ucrania, y, por otro, en Asia, con el ataque terrorista de Hamás a Israel y la intensa reacción operativa militar de este último. Por su puesto, estos actos bélicos impactan en todo el mundo, no solo en aspectos netamente operacionales, sino también en asuntos diplomáticos, económicos, sociales, geopolíticos, entre otros, en los cuales el ciberespacio tiene un papel preponderante.

En este sentido, en los ciberanálisis se deben considerar teóricamente las connotaciones geopolíticas que han permitido el escalamiento del conflicto y las variables geoestratégicas que otorgan una ventaja táctica. Asimismo, conviene recordar las persistentes maniobras militares que generan acumulación de tensiones constantes entre China y Taiwán, donde Estados Unidos ha permanecido sumamente vigilante. Evidentemente, todo este tipo de conflictos causan máximas alertas, razón por la cual es fundamental incluir estos temas en la agenda de

seguridad cibernética regional y mundial, admitiendo como una realidad que nos encontramos *ad portas* de un camino que conduce hacia la era militar cuántica.

Contexto militar relacionado con la computación cuántica y las guerras de quinta generación

Este apartado destaca la importancia de considerar la computación cuántica en el contexto de futuras guerras, subrayando su relevancia para los estudios estratégicos y la seguridad y la defensa de los Estados. Se enfatiza la necesidad de realizar investigaciones académicas que aborden la ciberseguridad y la ciberdefensa, dada la influencia de la computación cuántica en la seguridad nacional y en las guerras de quinta generación.

De acuerdo con López de Mesa (2022), desde tiempos remotos el ser humano ha desarrollado tecnologías para la guerra, y en la actualidad la lucha por la carrera armamentística basada en los adelantos de la ciencia ha cobrado más fuerza que nunca. En particular, se observan diversas características de guerras geoeconómicas entre Estados Unidos y China, por una parte, y entre Estados Unidos y Rusia, por otra.

Ahora bien, con los recientes acontecimientos en Ucrania por la invasión rusa y la incursión armada a Israel ejecutada por la organización política y paramilitar palestina Hamas, la ciencia y la tecnología han demostrado ser un factor definitorio en la conducción y el carácter de la guerra. Se han registrado diversas operaciones militares, incluidas ciberoperaciones, que evidencian la presencia de una guerra invisible que marca su huella hegemónica en el liderazgo militar del ciberespacio, lo que podría marcar el camino hacia la era militar de la computación cuántica.

Para situar la necesidad de la innovación tecnológica militar mundial cabe enfatizar que la OTAN ha percibido la importancia del ecosistema de tecnología-seguridad-defensa, con la puesta en marcha de la Aceleradora de Innovación de Defensa para el Atlántico Norte (DIANA), la cual tiene como objetivo convertir a la tecnología en una prioridad (Ricart, 2023). Por otra parte, uno de los trascendentales asuntos tratados en la cumbre de la OTAN llevada a cabo el 29 de junio de 2022 en Madrid, España, tuvo que ver con la aprobación de un Nuevo Concepto Estratégico, el cual asegura que la Alianza se prepare para enfrentar el futuro y cuente con los recursos financieros necesarios en procura de asumir su tarea con mayor fundamento técnico.

El informe de la OTAN sobre *Tendencias en Ciencia y Tecnología 2020–2040* hace referencia a las tecnologías que madurarán previsiblemente en el período 2020-2040 y para las cuales cabe esperar que sus efectos no terminen perjudicando las funciones de defensa y seguridad. La notoria preocupación alrededor de los avances y desarrollos científicos tiene impactos en los principales representantes de la seguridad mundial. Específicamente, la OTAN define nueve prioridades, entre las cuales se resaltan las tecnologías de base cuántica, las cuales a su vez se subdividen por áreas, destacándose la criptografía cuántica, los radares cuánticos y la comunicación cuántica, cuya evolución debe evaluarse periódicamente (Ricart, 2023).

El nuevo concepto estratégico de la OTAN muestra la firmeza y determinación en que tiene para proteger a los más de mil millones de ciudadanos que forman parte de su jurisdicción, para defender el territorio y salvaguardar la libertad y la democracia. Asimismo, evidencia el firme compromiso para con la defensa mutua frente a todas las amenazas, independientemente de su procedencia, insistiendo en la importancia del desarrollo e innovación tecnológica. Con respecto a las tecnologías emergentes y disruptivas, en el punto número 24 de ese documento, la OTAN expresa:

Aceleraremos nuestra transformación digital, adaptaremos la Estructura de Mandos de la OTAN a la era de la información y mejoraremos nuestra ciberdefensa, redes e infraestructuras. Promoveremos la innovación y aumentaremos nuestras inversiones en tecnologías emergentes y disruptivas para preservar nuestra interoperabilidad y nuestra ventaja militar. Trabajaremos juntos para adoptar e integrar nuevas tecnologías, cooperar con el sector privado, proteger nuestros ecosistemas de innovación, elaborar normas y comprometernos con los principios de uso responsable que reflejen nuestros valores democráticos y los derechos humanos. (Oficina de Comunicación del Ministerio de Defensa, 2022, p. 10)

Por otra parte, en el ámbito de la política pública, el gobierno de Estados Unidos de América publicó un suplemento del presidente a la solicitud de presupuesto 2023, el cual sirve como Informe Anual de la Iniciativa Cuántica Nacional, que fue requerido por la Ley de la Iniciativa Cuántica Nacional (NQI Act; P.L. 115-368; codified at 15 U.S.C. §§8801 et seq.), que el Congreso aprobó y el presidente promulgó en diciembre de 2018. En concreto, se destaca la relevancia y el apoyo económico hacia la referida iniciativa con el objeto de “acelerar la investigación y desarrollo (I+D) cuánticos para la seguridad económica y nacional de Estados Unidos y

garantizar el liderazgo continuado en la ciencia de la información cuántica y sus aplicaciones tecnológicas" (Congressional Research Service, 2023, p. 1).

De acuerdo con la United States Government Accountability Office (Oficina de Rendición de Cuentas del Gobierno de Estados Unidos), las comunicaciones cuánticas podrían mejorar la seguridad, la detección y la informática. Esto permitiría contar con protocolos de comunicaciones cuánticas seguras, fortalecer este aspecto en empresas y administraciones públicas de diversos sectores, como la seguridad nacional, las elecciones, las finanzas, el suministro energético y los servicios sanitarios. Por ejemplo, los protocolos de seguridad de las comunicaciones cuánticas podrían robustecer la seguridad de la infraestructura crítica cibernética protegiendo los datos enviados entre centros de control y los usuarios, lo cual evidentemente fortalece la ciberdefensa del país (United States Government Accountability Office, 2021).

El ejemplo de los Estados Unidos demuestra que los democráticos deben asumir con compromiso el estudio y la implementación de tecnologías cuánticas para la defensa y la seguridad nacionales, considerando que el ciberespacio es ahora un campo de batalla donde la información y la desinformación pueden provocar conflictos sociales, culturales y militares.

En este sentido, se debe tener en cuenta que la teoría de la comunicación humana ha considerado a los individuos en su nexos social y su interacción con otros sujetos, es decir, el vehículo de esa interacción es la comunicación. Hoy en día, más que nunca, la información emitida y recibida está en constante riesgo, no solo por falta de comprensión del mensaje, sino de violación a los principios de confidencialidad, disponibilidad e integridad. "De cualquier manera, parece evidente que la concepción del hombre solo como un 'animal social' no logra explicar al hombre en su nexos existencial, del cual la participación social es solo un aspecto, aunque muy importante" (Watzlawick, et al., 1991, p. 171).

Así las cosas, el mensaje de la teoría es comprender y fortalecer significativamente la comunicación entre individuos para limitar y por ende disminuir los elementos vulnerables que podrían conllevar a ejercer puntos de inflexión cuando se está inmerso en la escalada del conflicto o dentro de una guerra de quinta generación. Dicha comunicación debe ser protegida con severidad, ya que el uso equivocado o alterado, sumado a la negligencia y la falta de protección de la información sensible, genera el rompimiento de los principios de la teoría de la comunicación humana.

En este punto conviene mencionar algunos eventos en los que la información ha sido parte sustancial de una guerra de quinta generación. Según *The New York Times*, el grupo terrorista Hamas también utiliza estrategias de guerra psicológica usando el ciberespacio en el conflicto armado que protagoniza en Oriente Medio. La nueva táctica de guerra digital es utilizar las cuentas de redes sociales como Facebook, Instagram y WhatsApp, pertenecientes a israelíes que secuestraron para sembrar el terror, retransmitir en directo atentados, difundir mensajes de odio y lanzar amenazas de muerte (Frenkel & Minsberg, 2023). Por ende, la tecnología debe abordarse desde la profunda comprensión del ser en razón de las múltiples implicaciones en las mentes de los integrantes de la cibersociedad actual.

España, por ejemplo, es uno de los países que se ha preocupado por propiciar el desarrollo de la tecnología transformacional. Se observa particularmente que estos avances se han orientado a actualizar sus capacidades militares, lo cual implica afrontar importantes retos tecnológicos, entre los cuales está la computación cuántica, para guiar los enfoques de I+D+i en la defensa.

Este direccionamiento consiste en obtener beneficios tácticos y operacionales para enfrentar el riesgo que trae el uso de la tecnología por parte de grupos terroristas, una de las mayores amenazas a la seguridad mundial. Con este propósito, el gobierno español trazó una estrategia para el período 2021-2027, la cual consiste en incrementar las prestaciones de los sistemas y equipos que sustentan las capacidades militares para mantener la libertad de acción de sus Fuerzas Armadas, campo en el que otorgan gran relevancia a la computación cuántica (Ministerio de Defensa de España, 2020).

En un mundo hiperconectado y geopolíticamente inestable, la mitigación, la medición y la tolerancia al riesgo son aspectos que se deben problematizar. Ahora es común que diariamente haya nuevos descubrimientos, como la computación cuántica, y que muy rápido pasen a formar parte de la vida de los seres humanos. Esto crea desconocidas y sofisticadas amenazas que se suman a las existentes para aumentar los riesgos a que está expuesta la sociedad, lo cual desafía a los gobiernos y, particularmente, a los representantes de la seguridad y la defensa, que son quienes tienen la responsabilidad de enfrentarlas.

En relación con los riesgos asociados a la computación cuántica, se debe señalar que, por ejemplo, el gobierno de los Estados Unidos tiene una visión clara para anticipar y comprender las amenazas desconocidas en función de priorizar la protección de los intereses de seguridad nacional:

Some quantum computing technologies may pose risks to national security if they were to be obtained by adversaries of the United States and other malign actors. For example, using quantum algorithms, a practical quantum computer could potentially compromise the cryptography currently used to protect sensitive data communications among government agencies, financial institutions, health service providers, and others. (Congressional Research Service, 2023, p. 14)

El uso de tecnologías en los conflictos armados de la llamada revolución digital es un componente indispensable que ha modificado las guerras actuales y ha generado todo tipo de conjeturas sobre cómo se verán afectadas las guerras futuras. Es claro que concurrirían fenómenos fundamentales en el carácter de la guerra con la llegada de la digitalización a las innovaciones militares. En este sentido, se subraya la importancia evidente que tienen los teatros de operaciones cibernéticas para valorar el impacto de las nuevas tecnologías y su influencia en el desarrollo del conflicto (Fojón, 2022).

En estas circunstancias, el mundo atraviesa una era tensa donde el ajedrez geopolítico se mueve según las alianzas de los países hegemónicos, de tal manera que la naturaleza de la guerra puede cambiar rápidamente, en semanas o meses. Resulta crucial entonces analizar los hechos militares históricos para anticipar futuros conflictos, ya que a menudo son preludios de guerras anunciadas o reflejan la complejidad de los desafíos venideros.

Ahora bien, para proseguir el análisis es oportuno traer a colación una investigación publicada en 2013 que encuadra con precisión en el carácter de las guerras actuales: *El valor de la ciencia está en la capacidad de prever lo que sucederá o podría suceder en el futuro*, escrita por el General Valery Gerasimov, jefe del Estado Mayor General de las Fuerzas Armadas de la Federación Rusa.

En este manuscrito, conocido como la doctrina Gerasimov, el General argumenta que las acciones militares se han ido desnaturalizando y son cada vez más dinámicas, activas y fructíferas. Además, subraya la inclusión en el campo bélico de nuevas tecnologías de información que han permitido complementar significativamente algunas carencias de estrategias no militares. Advierte que los nuevos desafíos exigen considerar nuevas formas y métodos de llevar a cabo las operaciones de combate y, por consiguiente, la inclinación de la balanza en los resultados finales (Gerasimov, 2016).

La percepción rusa de la transformación de la guerra describe en forma detallada las fases que conducen a la evolución del conflicto y la correlación de las

medidas no militares y militares. En esta, se destaca el liderazgo político militar en concordancia con las amenazas militares dirigidas, la búsqueda de métodos para regular un conflicto y las medidas militares de disuasión estratégica, en las cuales el uso de la tecnología establece componentes clave de la ciencia militar actual y donde la participación de la sociedad en su conjunto es inevitable y en algunos casos necesaria.

Como lo menciona Fernández (2023), las sociedades en menor o mayor medida son cibercombatientes, aunque no lo sepan. La falta de identificación, individualización y judicialización de los cibercriminales es un gran problema para mejorar los procesos de ciberseguridad y ciberdefensa, así como para optimizar la respuesta de las autoridades judiciales. Esto complica también el campo militar de las operaciones en el ciberespacio, donde cada vez más aumentan los usuarios y, por lo tanto, los actores de amenaza se pueden camuflar entre ellos.

Así las cosas, la proyección que tiene actualmente la tecnología cuántica indica que tendrá una gran influencia en el panorama geopolítico, donde las opiniones, posiciones e inclinaciones políticas que circulan en el ciberespacio tienen gran importancia en un mundo digital cada vez más desintegrado. En este sentido, es clave comprobar la legitimidad que tienen dichas posturas, en un contexto en el que la saturación del ciberespacio con información no confiable es la única certeza. Precisamente, la computación cuántica no solo servirá para detectar y comprobar la información no confiable, sino que también guiará la prevención de ataques cibernéticos contra objetivos críticos por parte de otros agentes estatales y piratas informáticos criminales a su servicio.

Implicaciones de la computación cuántica en la ciberseguridad y ciberdefensa

Los conceptos de la ciberseguridad y ciberdefensa están cada vez más compenetrados en la gobernanza digital debido a la dinámica cibercriminal y los retos que enfrentan todo tipo de organizaciones en cualquier rincón del planeta. Por un lado, los elementos que forman parte del ecosistema digital personal o empresarial deben contar con efectivas políticas de ciberseguridad, mientras que los sistemas y las redes informáticas que interconectan las infraestructuras críticas cibernéticas prestadoras de servicios básicos y fundamentales deben respaldar su protección en los fundamentos aplicados por la ciberdefensa con el fin de llevar a cabo un marco operacional.

La aparición permanente de vulnerabilidades cibernéticas exige también nuevos estándares de conocimientos preventivos y reactivos para evitar, manejar y mitigar el riesgo, así como para responder eficazmente a las amenazas. En este sentido, la ciberseguridad contribuye a consolidar una normalización digital que responda al funcionamiento de la cibernación. Por su parte, el enfoque de la ciberdefensa se encamina específicamente a la capacidad de respuesta militar ante ciberataques y la posibilidad de llevar a cabo una ciberoperación como respuesta ofensiva. La ciberseguridad y la ciberdefensa cuentan con grandes perspectivas de estrategias y procedimientos en concordancia con las necesidades del campo de aplicación y requieren un alto grado de coordinación (Pontijas, 2023).

Dicho esto, el imparable desarrollo de las tecnologías emergentes aún está en una incipiente etapa de la cuarta revolución industrial, aunque los avances ya impactan todas las áreas, especialmente la seguridad. Los asuntos militares presentan componentes digitales de diversas características y formas antes inimaginables. La inteligencia artificial, los drones aéreos y marítimos no tripulados, las armas cada vez más autónomas y, por supuesto, la computación cuántica hacen necesario considerar marcos éticos y modificaciones en las operaciones y ciberoperaciones, la cadena logística y la organización del poder militar. "Mirando en el horizonte hacia 2040, la computación cuántica es una buena ilustración de por qué el mundo puede estar solo en la primera fase de la revolución tecnológica" (Manning, 2020, p. 11). Al respecto, Grobman (2020) señala:

[...] como toda tecnología, en las manos equivocadas, la computación cuántica puede ser una herramienta peligrosa. En el campo de la ciberseguridad, por ejemplo, los Estados-nación podrán utilizar la tecnología cuántica para romper los sistemas criptográficos públicos que protegen y nos permiten confiar en gran parte de nuestro mundo digital, incluido el tráfico web, correos electrónicos e innumerables cargas y descargas de todo tipo, desde archivos confidenciales a actualizaciones de software. (p. 53)

Los argumentos expuestos hasta este punto evidencian que es necesario adaptar el concepto de la defensa nacional y robustecer el entorno operacional en el ciberespacio para apropiarse de las dinámicas digitales, con el fin de ejercer dominio y protección, tanto de los ciudadanos, como de las infraestructuras críticas a su servicio. Los ataques cibernéticos a base de tecnología cuántica perpetrados por actores estatales y no estatales podrían resquebrajar fácilmente la gobernabilidad, la salud pública o la economía de un país. Por tal motivo, la seguridad y la

defensa nacionales en el ciberespacio deben ser una política pública para fortalecer el nuevo escenario de confrontación bélica, de tal manera que complemente los dominios de tierra, mar, aire y espacio (Realpe & Cano, 2020).

Paralelamente se deben abordar los tratados internacionales, ya que si un país es agredido cibernéticamente, en respuesta no podría usar la fuerza en el campo militar, pues está fuera de su alcance físico. El quinto dominio, entonces, ejerce como un ambiente facilitador de ciberataques, no es un arma en sí mismo, es un dominio operacional en el que los datos interaccionan continuamente. Así pues, resulta complejo individualizar al ciberagresor e identificar desde qué lugar se ejecutó, de manera que no se podría acudir a la legislación descrita para el conflicto tradicional, en particular el "artículo 51 de la Carta de las Naciones Unidas para invocar el derecho a la defensa propia ante un ataque armado, tal y como también contempla el artículo 5 del Tratado de Washington" (Pontijas, 2023, p. 12). En este sentido, surgen varios interrogantes frente a los ciberataques con tecnología cuántica por la naturaleza de la acción.

De acuerdo con Yáñez (2022), la computación cuántica podría convertirse en la bomba nuclear del mundo digital, pues su capacidad podría rivalizar con las armas nucleares. "En la guerra moderna, la forma de disuasión más efectiva es, sin duda, la capacidad nuclear, pues el grado del daño que puede causar obliga a las potencias mundiales a ser muy cautas ante un posible conflicto bélico" (s. p.). En el mundo, según el Stockholm International Peace Research Institute (SIPRI), "existen alrededor de 14 400 armas nucleares en responsabilidad de nueve países, aunque Rusia y Estados Unidos" concentran cerca del 92 % del poder nuclear, todos esos modelos nucleares conectados a sistemas informáticos y posiblemente amenazados como objetivos cibernéticos.

En ese orden de ideas, se reitera la tesis de que es fundamental comprender el desarrollo y los usos de la computación cuántica, principalmente en lo concerniente a las nuevas amenazas que pongan en riesgo la seguridad y la defensa de las naciones. En el campo de los estudios estratégicos, que tienen entre sus preceptos promover la investigación prospectiva, dichas exploraciones ayudan a mejorar las tareas de predicción y preparación en el contexto de la carrera por la innovación, con el interés absoluto de contribuir a fortalecer, académicamente, los componentes de la sociedad digital actual y futura.

Desde una óptica diferente, es valioso reseñar el importante avance que tuvo la carrera cuántica en octubre de 2019, cuando la compañía de tecnología Google informó que había logrado la supremacía cuántica, es decir, que había desarrollado

un ordenador capaz de superar a un procesador clásico para encontrar soluciones mucho más complejas. Si bien esta noticia supuso un gran hito tecnológico, también planteó nuevos retos para la seguridad cibernética, el riesgo hacia los seres humanos y la ética (Marzal, 2020).

En este contexto, se afirma que los avances cuánticos en el ámbito militar serán impactantes, de manera que la artillería cuántica debe ser supervisada para evitar su uso indebido. Por lo tanto, la ciberdefensa es crucial para controlar la fabricación y la distribución de estas armas digitales, que definirán las guerras del futuro. Se trata de una situación similar a la que ocurrió en el siglo pasado, cuando un adelanto tecnológico marcó la pauta en el carácter de la guerra: la máquina Enigma, a la cual ya se había hecho referencia. Esta máquina de rotores, diseñada para cifrar y descifrar mensajes, es uno de los mejores ejemplos de la importancia que tiene la tecnología en instancias armamentísticas para enfrentar una guerra. Específicamente, la criptografía, cuyo objetivo es transformar un mensaje para evitar que sea comprensible para un tercero, es uno de los usos militares que puede tener la computación cuántica, ya que rompería el cifrado del emisor al receptor sin ningún problema. Por lo tanto, la sofisticación de los ciberataques es un asunto bastante sensible que requiere de la mayor atención, pues con el uso de la computación cuántica serían aún más difíciles de detectar que en la actualidad, principalmente en operaciones militares de ciberespionaje, así como en acciones de ciberterrorismo, tráfico de ciberarmas y ciberguerra en sí misma (Marzal, 2020).

Acorde con lo anterior, la computación cuántica, como una tecnología emergente, despliega dimensiones particulares en el escenario del ciberconflicto y, en particular, en lo relacionado con las responsabilidades de acción sobre los usos indebidos. Llegados a este punto y para aclarar lo referente a la actuación en las operaciones militares en el ciberespacio, conviene examinar brevemente un pronunciamiento de la Corte Penal Internacional (CPI) en el que enfatiza que dicho estamento perseguirá los cibercrímenes de guerra.

El fiscal jefe de la CPI, Karim Ahmad Khan (2023), con competencia para juzgar a los responsables de cometer crímenes graves contra la humanidad, publicó recientemente en un artículo de la gaceta *Digital Front Lines*, que las herramientas utilizadas para cometer delitos internacionales graves están cambiando y evolucionando constantemente. Señaló que las armas cibernéticas están desempeñando un papel de suma trascendencia dentro de los conflictos armados, y subrayó que la efectividad del armamento impulsado por el internet e incluso con tecnologías a base de inteligencia artificial ha permitido que los Estados puedan realizar

ciberoperaciones militares. "Este nuevo y rápido desarrollo de los medios militares y bélicos puede utilizarse indebidamente para cometer o facilitar crímenes de guerra, crímenes contra la humanidad, genocidio e incluso la agresión de un Estado contra otro" (Khan, 2023, p. 50).

Además de la posición de la CPI respecto a los cibercrímenes de guerra, es oportuno indicar que en septiembre de 2023 este tribunal sufrió un grave ataque en sus sistemas informáticos por parte de grupos de cibercrimen transnacional. Si bien el incidente de ciberseguridad pudo ser detectado, se trató de un ataque selectivo y sofisticado que tenía el objetivo de hacer ciberespionaje, definido como un serio intento de socavar el mandato de la alta corte (International Criminal Court [ICC], 2023).

En resumen, la responsabilidad de investigar y contrarrestar las amenazas cibernéticas no recae únicamente en las autoridades competentes, sino que toda la sociedad debe asumir sus derechos y deberes. En este escenario, la teoría de la comunicación humana resalta la importancia de entender el flujo de información en un contexto saturado de datos, lo cual representa un verdadero reto para los futuros líderes y gobernantes, quienes deben adaptarse y enfrentar los cambios tecnológicos que impactan la seguridad y la defensa nacionales.

Liderazgo estratégico militar del ciberespacio en la era de la computación cuántica

El liderazgo estratégico para afrontar los desafíos a la seguridad y la defensa que tiene la humanidad requiere de personas prolijas, visionarias, preparadas, con experiencia; futuristas que miren al mundo con un direccionamiento y una proyección militar a 20, 50 o 100 años.

De acuerdo con Castien (2019), el fenómeno del liderazgo se instituyó en la antigüedad clásica, en donde se le atribuía principalmente las funciones de análisis y reflexión. Posteriormente, en la modernidad el liderazgo ha trascendido al ámbito de las empresas, la ciencia política, la historia, los conflictos, entre otros. En ambas perspectivas históricas, su importancia radica en que permite analizar de forma metódica las aptitudes del líder, sus rasgos de personalidad y sociabilidad, así como, en general, su estilo particular para ejercer el liderazgo. En los asuntos militares, la dirigencia política o el direccionamiento empresarial, la función trascendental del liderazgo se observa claramente en la naturaleza de la toma de decisiones y la conducción de seres humanos.

Con base en este acercamiento conceptual, a continuación se destaca el liderazgo estratégico de Winston Leonard Spencer-Churchill (1874-1965), pues su trayectoria militar y política es un claro ejemplo de que adoptar posturas decisivas en materia tecnológica puede definir los acontecimientos militares. Su marcada personalidad y carisma, estilo político y experiencia militar lo condujeron a ser reconocido como uno de los personajes más importantes de los últimos siglos, por cuanto no solo imprimió su sello en la conducción de arduas batallas contra la Alemania nazi en la Segunda Guerra Mundial entre 1939 y 1945, sino que además apoyó e impulsó incluso tecnología avanzada en Bletchley Park, el lugar donde se descifró el código secreto de los nazis con la creación de tecnología avanzada.

Winston Churchill (1874-1965), estadista, oficial del ejército, historiador, escritor, orador y político británico, es reconocido por su liderazgo en tiempos de guerra. Ocupó el cargo de primer ministro del Reino Unido en dos períodos (1940-45 y 1951-55) y obtuvo el premio Nobel de Literatura en 1953. Al inicio de la Segunda Guerra Mundial fue nombrado nuevamente Primer Lord del Almirantazgo y tras la dimisión del Neville Chamberlain (mayo de 1940), asumió como primer ministro. Contra lo esperado, Churchill no quiso firmar la paz luego de la derrota de Francia e hizo fracasar el intento de Hitler de sentar a Gran Bretaña en la mesa de negociaciones a través de los bombardeos aéreos. Con su gran habilidad oratoria, traspasó esta firmeza a los británicos, inspirándolos con sus discursos y programas de radio durante los cruentos años que duró la guerra. (Riquelme, 2015, p. 72)

El liderazgo no era tarea fácil y no existe una receta mágica para conseguir un direccionamiento exitoso. En la vida militar el desarrollo de líderes inicia desde el primer día, pues, en resumen, cada soldado es un líder en sí mismo. Qué hacer y para qué, en lugar del cómo, son los interrogantes que configuran la esencia de quien lidere organizaciones bajo cohesión, confianza, comprensión, serenidad, conocimiento y ética. Se podría definir liderazgo estratégico como el "proceso de alinear personas, sistemas y recursos para lograr la visión de la organización, mientras permite lograr una necesaria cultura adaptativa e innovativa para obtener una ventaja en un medio ambiente altamente competitivo" (Martínez & Galvin, 2019, p. 2).

No es solo en tiempos de paz en los que surge la capacidad de liderazgo, sino cuando estos deben enfrentar desafíos complejos. Es en tiempos de crisis que salen a relucir verdaderas personas con ese calificativo, quienes demuestran vigorosidad a través de su probada fortaleza, especialmente los poseedores de virtudes éticas, intelectuales, filosóficas y morales, elementos primordiales de un liderazgo positivo (Griffiths, 2020). Es decir, no son líderes simplemente por el hecho de

ocupar posiciones de mandato, sino porque a lo largo de su vida han afrontado pruebas de fuego que forjaron su carácter, cordura, conocimiento y sabiduría.

Específicamente, las guerras de quinta generación demandan un tipo de liderazgo integral, que comprenda y aplique los conceptos sobre la guerra que se han elaborado a lo largo de la historia en la construcción de los imperios y que asuma los nuevos escenarios de confrontación con determinación. En la actualidad, las estrategias militares dependen casi en su totalidad de la utilización del internet y los componentes digitales que permiten respaldar las redes de comunicación, fortalecer la logística, realizar actividades de inteligencia y estudiar profundamente al enemigo.

De este modo, el ciberespacio, como dominio de la guerra creado por el ser humano, supone un punto de quiebre valiosísimo en la escalada y el desarrollo del conflicto. En este contexto, actores de cualquier ángulo pueden utilizar la desinformación como un arma con la ayuda de herramientas digitales, lo cual conduce a los usuarios de las redes sociales a dividir opiniones y tomar parte activa en los hechos debido al componente emocional implícito de los conflictos. Por momentos, esto hace que se pierda la objetividad y empuja al desenfoque y a la reacción de las masas, un elemento clave en las guerras de quinta generación.

Un ejemplo reciente de este tipo de guerras es la explosión de elementos digitales con videos, imágenes y publicaciones desde que inició el conflicto en Oriente Medio. Después de los ataques terroristas y la incursión en Israel del grupo de corte yihadista, nacionalista e islamista Hamás, en la plataforma X, anteriormente Twitter, comenzaron a circular publicaciones desinformativas sobre el desarrollo de esa guerra. En respuesta, el responsable de derechos digitales de la Unión Europea, Thierry Breton, informó que dio a la plataforma X no más de 24 horas para explicar cómo cumpliría las nuevas normas digitales dispuestas por ese estamento de control. Por su parte, Linda Yaccarino, consejera delegada de X, aseguró que estaban haciendo lo procedente con el fin de controlar los contenidos ilegales que proliferan en la red social (Associated Press, 2023).

Las particularidades de las guerras actuales y futuras demandarán líderes militares conocedores del pasado y pensadores prospectivos de los conflictos armados, teóricos de la guerra, visionarios, con profundidad en los conceptos del ser, documentados de los adelantos tecnológicos y reafirmados en perspectivas ciberestratégicas y ciberfilosóficas. Evidentemente, la era cuántica probará a esos líderes con conciencia situacional del escenario tecnológico y la comprensión del ser humano, que asuman con alto grado de respeto la importancia del dominio cibernético para concebir, respaldar y fortalecer el futuro del planeamiento estratégico militar.

Conclusiones

Los resultados de este análisis evidencian que la evolución de la ciencia y la tecnología ha hecho posible la interacción en el ciberespacio. Como parte de este desarrollo histórico, la computación basada en principios cuánticos transformará radicalmente este escenario y, en consecuencia, es menester interpretar también los riesgos, los cuales se deben asumir con conciencia situacional. La combinación de varios de los factores tratados ha propiciado el replanteamiento de una serie de problemáticas relacionadas con el uso de la tecnología en la guerra y el liderazgo en el marco de la ética, los derechos fundamentales y la cibercriminalidad.

En este capítulo se han presentado las implicaciones de la computación cuántica en torno a la guerra y el liderazgo estratégico, con el fin de poner en contexto las características del siguiente nivel de la computación como parte fundamental de análisis en los estudios estratégicos de seguridad y defensa. Al exponer la problemática implícita en el desarrollo tecnológico, la posibilidad de adaptación, control y resiliencia de los procesos aumenta a medida que se comprendan los riesgos que existen tanto por los avances científicos como por el comportamiento humano.

Las naciones, los ejércitos, las compañías, las instituciones y, por supuesto, las personas del común están en la obligación de asimilar fundamentos clave del actual contexto digital. La seguridad en el ciberespacio es un asunto que no se puede dejar a la suerte, de manera que es una responsabilidad social profundizarla exhaustivamente con el fin de proteger a las personas en temas como la defensa de la identidad digital, el funcionamiento apropiado de la economía y, fundamentalmente, la prevención de los riesgos que amenazan el objetivo estratégico de la seguridad nacional.

La computación cuántica se ha consolidado como un componente crucial en la seguridad nacional, especialmente en el contexto de las guerras de quinta generación, pues su capacidad para procesar información a velocidades sin precedentes la convierte en una herramienta estratégica indispensable. Es imperativo que los líderes, bien preparados y con una visión estratégica, integren esta tecnología en sus planes de acción para anticipar y enfrentar los desafíos emergentes. Para maximizar su potencial, los gobiernos, junto con la academia y el sector empresarial, deben fomentar una colaboración activa en la investigación y el desarrollo, identificando aplicaciones, evaluando riesgos y formulando políticas que garanticen su uso ético y seguro. De este modo, no solo se protegerá a la sociedad, sino que también se asegurará la posición de la nación en un entorno internacional

cada vez más competitivo, estableciendo la computación cuántica como un pilar esencial para la defensa y el avance de la soberanía nacional en el siglo XXI.

Lo expuesto demuestra que si bien la computación cuántica impulsará beneficios para la humanidad, es inevitable que también aparezcan nuevas vulnerabilidades, las cuales podrían ser aprovechadas por organizaciones de cibercrimen transnacional. En este sentido, debido a las permanentes y sofisticadas amenazas que ponen en riesgo la sostenibilidad del mundo digital, es necesario aplicar de forma minuciosa la teoría de la comunicación humana en las actuales circunstancias de intercambio de información.

Los ataques cibernéticos no solo tienen una motivación económica, sino también militar y política, además intervienen en la naturaleza y el carácter de la guerra; en suma, las consecuencias del movimiento del ajedrez geopolítico inciden en las ciberoperaciones militares en un escenario clave de confrontación. Por lo tanto, fortalecer la ciberseguridad y la ciberdefensa en el ámbito militar es fundamental para aprovechar las tecnologías existentes y trabajar en las tecnologías futuras con el objetivo primordial de proteger las infraestructuras críticas cibernéticas.

Este capítulo confirma la tesis sobre la importancia que tiene la computación cuántica en conflictos militares cibernéticos. Se recomienda a los líderes y comandantes establecer organismos militares cibernéticos preparados para afrontar la era cuántica, asegurando así una respuesta efectiva para proteger la seguridad nacional en el futuro cercano. En particular, un liderazgo como el que tomó, durante la Segunda Guerra Mundial, el primer ministro del Reino Unido Winston Churchill, en un momento decisivo de la historia cuando creyó en la tecnología de vanguardia para cambiar el curso de la guerra al descifrar el código secreto de la máquina Enigma.

Es necesario recalcar que los gobiernos deben afrontar con decisión, basados en un amplio discernimiento, los inmensos retos que plantea el uso del internet en relación con la sociedad y el uso de herramientas digitales como armas. El crimen, y especialmente el cibercrimen, se ha acondicionado rápidamente al nuevo escenario delictivo con el auge de la sociedad digital, que basa sus procesos en redes informáticas cada vez más vulnerables. Por lo tanto, se sugiere incluir en la agenda cibernética nacional una estrategia nacional que aborde la ciberseguridad cuántica de manera urgente y pública, que aborde riesgos y bondades de esa tecnología emergente.

En virtud de los antecedentes que se mencionaron a lo largo del capítulo, en el ámbito de las operaciones militares en el ciberespacio es fundamental seguir con rigurosidad los protocolos y convenios establecidos, con la precaución de no cometer los cibercrímenes de guerra contemplados recientemente por la CPI. En

este escenario, se debe considerar que los ciberataques son una amenaza que podrían tener graves consecuencias y afectación a la población civil en una guerra asimétrica, donde no está claro quién es el enemigo que se está enfrentando.

Cabe anotar que este capítulo se apoyó en los estudios estratégicos que fomentan la investigación, la planificación y el desarrollo de la seguridad y la defensa. Así pues, se logró construir, alrededor de la computación cuántica, una temática oportuna en estos tiempos de divisiones externas tan marcadas, en las cuales la tecnología forma parte primordial del devenir de los acontecimientos militares geoestratégicos.

Finalmente, resulta pertinente reiterar que las unidades responsables de las tecnologías de los ejércitos deben dedicar una línea de enfoque a los estudios, análisis, recomendaciones y conclusiones que planteó la OTAN en materia de innovación, los cuales se basan en las estrategias que prioriza esta investigación denominada DIANA. Por otra parte, deben hacer seguimiento y aprovechar la información disponible frente a la inversión en el desarrollo de tecnologías cuánticas y las decisiones de este organismo internacional en cuanto a la seguridad digital global.

La vida de muchos seres humanos, la democracia y el progreso de una nación dependen de las decisiones que se toman con el profundo conocimiento de la sociedad en su conjunto. Como parte de los elementos de juicio del líder estratégico, es clave que tenga en cuenta la tecnología, pues si bien es cierto que ha estimulado el desarrollo y el progreso, también ha sido utilizada para aumentar los riesgos a los que está expuesta la humanidad.

En un mundo donde la tecnología redefine el campo de batalla, la verdadera victoria no se mide solo en territorios conquistados, sino en la capacidad de entender y gestionar la ardua interacción entre máquinas y el comportamiento humano. Las guerras del futuro no serán ganadas únicamente por la superioridad armamentista, sino también por aquellos que integren la sabiduría de las ciencias sociales en sus estrategias, priorizando la protección de la vida civil en medio de la agitación social y geopolítica.

Con la llegada de la computación cuántica, las dinámicas del conflicto se transformarán aún más, ofreciendo tanto oportunidades como riesgos sin precedentes. Así, el desafío radica en un doble compromiso: dominar la tecnología y humanizar su uso, transformando la guerra en un arte que respete la dignidad humana y promueva la paz en un mundo interconectado cada vez más convulsionado y volátil.

Referencias

- Associated Press. (2023, 12 de octubre). Elon Musk's X removes thousands of Israel-Hamas misinformation accounts and posts amid EU demand. <https://tinyurl.com/499che6h>
- Barreno, D., Carrión, D., & Tenecora, I. (2016). Evolución de la tecnología móvil. Camino a 5G. *Revista Contribuciones a las Ciencias Sociales*, (octubre-diciembre), s. p. <https://tinyurl.com/5n7hukd4>
- Bravyi, S., Dial, O., Gambetta, J. M., Gil, D., Nazairo, Z. (2022). The future of quantum computing with superconducting qubits. *Journal of Applied Physics*, (132), 160902. <https://doi.org/10.1063/5.0082975>
- Castien, J. (2018). Aznar Fernández-Montesinos, F. (2018): 'Repensando el liderazgo estratégico', Madrid, Sílex, 436 pp. *Política y Sociedad*, 56(3), 807-809. <https://doi.org/10.5209/poso.63151>
- Cobelli, N., Juambeltz N., Pérez J., & Techera M. (2022). *Aplicaciones de la computación cuántica a la inteligencia artificial* [Tesis de pregrado, Universidad de la República de Uruguay]. Repositorio Institucional. <https://tinyurl.com/ynvy77k4>
- Congressional Research Service. (2023, 7 de septiembre). *Quantum computing: Concepts, current state, and considerations for congress [CRS Report, n.º R47685]* Congressional Research Service. <https://tinyurl.com/8ckymkj2>
- Fernández Aparicio, J. (2023). Ciberguerra y cibercrimen global, cuando lo virtual transciende a lo real (reedición). *Boletín IEEE*, (31), 44-71. <https://tinyurl.com/23bt54ta>
- Fojón, E. (2022). Ucrania: La tecnología en la guerra. *Boletín IEEE*, (28), 509-511. <https://tinyurl.com/h98puxnp>
- Frenkel, S., & Minsberg, T. (2023, 17 de octubre). Hamas hijacked victims' social media accounts to spread terror. *The New York Times*. <https://tinyurl.com/ynrb35bv>
- Gerasimov, V. (2016). El valor de la ciencia está en la capacidad de prever lo que sucederá o podría suceder en el futuro. *Militar Review*, (marzo-abril), 47-54. <https://tinyurl.com/yc2u85k3>
- Gayozzo, P. (2021). Guerra de quinta generación en la Cuarta Revolución Industrial. *Futuro Hoy*, 2(1), 31-34. <https://doi.org/10.5281/zenodo.4654906>
- Goodreads. (2011). Winston S. Churchill. https://www.goodreads.com/author/show/14033.Winston_S_Churchill
- Griffiths Spielman, J. (2020). Liderazgo estratégico en tiempos de crisis. <https://tinyurl.com/46sbhyf8>
- Grobman, S. (2020). Quantum computing's cyber-threat to national security. *PRISM*, 9(1), 53-66. <https://tinyurl.com/mwab64je>
- Hammes, T. X. (2007). Fourth Generation Warfare Evolves, fifth emerges. *Military Review*, 87(3), 14-23. <https://tinyurl.com/4j8r8uta>

- Hassan Alwan, S., & Jassim Muhammad, A. (2023). Fifth generation wars: Between theoretical rooting and contemporary applications (a study of the concept, tools, features, and motives). *Russian Law Journal*, 11(9), 664-681. <https://doi.org/10.52783/rlj.v11i9s.1839>
- Centro Superior de Estudios de la Defensa Nacional [CESEDEN]. (2023). Objetivos. <https://www.ieee.es/quienes-somos/objetivos/>
- International Criminal Court [ICC]. (2023, 20 de octubre). Measures taken following the unprecedented cyber-attack on the ICC. <https://tinyurl.com/jymna6bn>
- Jorge Ricart, R. (2023, 29 de septiembre). Innovación en defensa y tecnologías profundas en la OTAN: Cuestión de disposición y eficacia. <https://tinyurl.com/nthyydwr>
- Khan, K. (2023). Technology will not exceed our humanity. <https://tinyurl.com/5n6uvhv>
- Krelina, M., & Dúbravčík, D. (2023). Quantum technology for defence: What to expect for the air and space domains. Joint Air Power Conference Centre. *The Journal of the JAPCC*, (35), 39-46. <https://tinyurl.com/278nvr99>
- López de Mesa, J. (2022). De las tecnologías para la guerra a la guerra por la tecnología. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, 17(2), 7-12. <https://doi.org/10.18359/ries.6798>
- Manning, R. A. (2020, 7 de julio). Emerging technologies: New challenges to global stability. <https://tinyurl.com/4j55rz5k>
- Martinez, S., & Galvin, T. (2019). Leadership at the Strategic Level. En T. Galvin & D. Watson (Eds.), *Strategic leadership: Primer for senior leaders* (pp. 1-12). U.S. Army War College. <https://tinyurl.com/3eraysus>
- Marzal, C. (2020, 1 de julio). La computación cuántica y la ciberdefensa. <https://tinyurl.com/4h5ufdwm>
- Metcalfe, G., & Chow, J. (2018). Quantum computers: Are we there yet? En National Academy of Engineering (Ed.), *Frontiers of engineering: Reports on leading-edge engineering from the 2018 symposium* (pp. 5-8). National Academies Press. <https://tinyurl.com/eaetz797e>
- McKinsey & Company. (2021, 11 de junio). The top trends in tech - executive summary [Diapositivas]. <https://tinyurl.com/2vfskx36>
- Oficina de Comunicación del Ministerio de Defensa. (2022). *Nuevo concepto estratégico de la OTAN*. Ministerio de Defensa. <https://tinyurl.com/3b5atmp3>
- Pontijas Calderón, J. L. (2023). Unión Europea: Ciberseguridad y ciberdefensa. *Boletín IEEE*, (29), 54-67. <https://tinyurl.com/5x97r7aj>
- Qureshi Ahmad, W. (2019). Fourth- and Fifth-Generation Warfare: Technology and perceptions. *San Diego International Law Journal*, 21(1), 187-216. <https://tinyurl.com/23byzw7v>
- Realpe, M. E., & Cano, J. (2020). Amenazas cibernéticas a la seguridad y defensa nacional: Reflexiones y perspectivas en Colombia. En V. Gauthier Umaña, R. A. Méndez Romero, J. Cano, J. Ramíó Aguirre & L. E. Sánchez Crespo (Eds.), *Seguridad Informática: X Congreso Iberoamericano, CIBSI 2020* (pp. 105-113). Universidad del Rosario. <https://doi.org/10.12804/si9789587844337.10>

- Reding, D. F. & Eaton, J. (2020). *Science & technology trends 2020-2040: Exploring the S&T Edge*. NATO Science & Technology Organization. <https://tinyurl.com/yc4xf2zu>
- Riquelme Oyarzún, B. (2015). La persona detrás del líder. *Revista Marina*, (2), 72-75. <https://tinyurl.com/2dufrhr>
- Ruiz Jiménez, C. (2021). *Sobre la computación cuántica* [Tesis de maestría, Universidad Nacional de Educación a Distancia]. Repositorio institucional. <https://tinyurl.com/axrhdfy>
- Saniz Balderrama, R. (2001). Computación cuántica. *Acta Nova*, 1(2), 190-196. <https://tinyurl.com/n42x8463>
- United States Government Accountability Office. (2021, octubre 19). Quantum Computing and Communications: Status and prospects [Report to Congressional Addressees]. <https://tinyurl.com/3ne9j4c7>
- Vanegas Gómez, A. (2016). El camino hacia el ordenador cuántico: qubits y qudits.
- Watzlawick, P., Beavin Bavelas, J., & Jackson, D. D. (1991). *Teoría de la comunicación humana*. Editorial Herder.
- World Economic Forum. (2022). State of quantum computing: Building a quantum economy. <https://tinyurl.com/mtruywuf>
- Yáñez, F. (2022, 27 de febrero). Computación cuántica: La bomba nuclear del mundo digital. <https://tinyurl.com/yvmkxjz2>