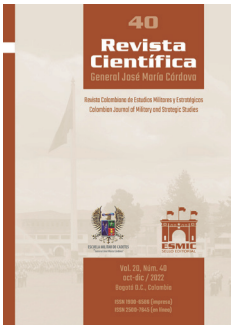
Revista Científica General José María Córdova
ISSN: 1900-6586
ISSN: 2500-7645
Escuela Militar de Cadetes "General José María Córdova"

Cano Martínez, Jeimmy José
Prospectiva de ciberseguridad nacional para Colombia a 2030
Revista Científica General José María Córdova, vol. 20, núm. 40, 2022, Octubre-Diciembre, pp. 814-832
Escuela Militar de Cadetes "General José María Córdova"

DOI: https://doi.org/10.21830/19006586.866

Disponible en: https://www.redalyc.org/articulo.oa?id=476274912004



Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)
Bogotá D.C., Colombia

ISSN 1900-6586 (impreso), 2500-7645 (en línea)
Web oficial: https://www.revistacientificaesmic.com

Prospectiva de ciberseguridad nacional para Colombia a 2030

Jeimy José Cano Martínez
https://orcid.org/0000-0001-6883-3461
jeimy.cano@esdegue.edu.co
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D.C., Colombia

Citación APA: Cano Martínez, J. J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, *20*(40), 815-832. https://dx.doi.org/10.21830/19006586.866

Publicado en línea: 1.º de octubre de 2022

Para enviar un artículo:
https://www.revistacientificaesmic.com/index.php/esmic/about/submissions

ESMIC
SELLO EDITORIAL
Miles Doctus

Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)
Bogotá D.C., Colombia

Volumen 20, número 40, octubre-diciembre 2022, pp. 815-832
https://dx.doi.org/10.21830/19006586.866

Prospectiva de ciberseguridad nacional para Colombia a 2030

National cybersecurity outlook for Colombia to 2030

Jeimy José Cano Martínez
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D.C., Colombia

Resumen. Este artículo presenta un ejercicio prospectivo sobre la ciberseguridad nacional de Colombia a 2030, con base en la revisión de fuentes académicas, reportes internacionales y entrevistas con especialistas. Los resultados se agrupan en seis factores siguiendo el marco Pestel: político, económico, social, tecnológico, ecológico y legal, con el fin de ofrecer un panorama integrado útil para comprender y asumir el reto de la protección del Estado y la resiliencia de las organizaciones frente a las dinámicas internacionales de la transformación digital y una sociedad cada vez más presente en el ciberespacio. Este artículo aspira a motivar nuevas investigaciones desde esta prospectiva y apoyar la toma de decisiones frente a las realidades emergentes que hoy ya hacen parte de un entorno cada vez más incierto, complejo y volátil.

Palabras clave: cibernética; gobierno electrónico; prospectiva; protección de datos; seguridad

Abstract. This article presents an outlook of Colombia's national cybersecurity to 2030, based on the review of academic sources, international reports, and interviews with specialists. The results are grouped into six factors following the Pestel framework: political, economic, social, technological, ecological, and legal to offers an integrated panorama to help understand and address the challenge of protecting the State and the resilience of organizations in the face of the international dynamics of digital transformation and a society that is increasingly present in cyberspace. This article aims to motivate further research from this perspective and support decision-making involving the emerging realities, part of an increasingly uncertain, complex, and volatile environment.

Keywords: cybernetics; data protection; electronic government; outlook; security

Sección: Dosier • Artículo de investigación científica y tecnológica
Recibido: 28 de agosto de 2021 • Aceptado: 22 de febrero de 2022

Contacto: Jeimy José Cano Martínez ✉ jeimy.cano@esdeg.edu.co

Introducción

Para entender el mundo digital y tecnológicamente modificado, es necesario reconocer el aumento de la densidad digital en el mundo físico, el incremento de los flujos de información desde los objetos conectados y, especialmente, el cambio en las dinámicas humanas, por el cual las personas privilegian los contactos y relaciones desde dispositivos, particularmente móviles, para sus actividades diarias y potenciar sus posibilidades y oportunidades (McKinsey & Company, 2021).

Este escenario cibernético, esto es, el entorno de interfaces digitales de comunicación y control donde ahora se desarrollan actividades de la sociedad en general, se convierte en una plataforma de desarrollo social y económico que vincula a la nación con los retos de la economía digital y, al mismo tiempo, con las tensiones que generan los riesgos cibernéticos, cuya particularidad es ser sistémicos, emergentes y disruptivos (Cano, 2019).

Por lo tanto, la ciberseguridad nacional se ha convertido en el factor fundamental que articula los esfuerzos desde diferentes frentes estatales para concretar y garantizar un entorno de confianza digital donde la ciudadanía en su conjunto pueda adelantar sus actividades, motivar transformaciones y apalancar iniciativas que generen mayor prosperidad y bienestar para toda la sociedad (Choucri, 2012). En consecuencia, reconocer la nueva realidad digital del país implica establecer referentes básicos de prevención, coordinación, educación, respuesta y visión, que permitan conectar los retos actuales en materia cibernética y las tendencias que se identifican hacia el futuro.

De acuerdo con lo anterior, este artículo se propone explorar las tendencias nacionales e internacionales desde el marco *Pestel* (política, económica, social, tecnológica, ecológica y legal) y sus impactos para la ciberseguridad nacional colombiana en el mediano y largo plazo (2030). Esto representa un ejercicio básico de análisis con el fin de establecer algunos horizontes de desarrollo e iniciativas, lo cual hará posible implementar planes de acción para avanzar en los retos y exigencias de una sociedad digital inmersa en una revolución de tecnologías emergentes y disruptivas, que exigen cada vez experiencias distintas que respondan a sus altas expectativas (Hines & Bishop, 2015).

Con tal propósito, se revisaron documentos elaborados por instituciones multilaterales, informes de centros de pensamiento, artículos académicos, reportes de industria y perspectivas de líderes de opinión nacional y global, en aras de darle forma a una visión prospectiva para la ciberseguridad nacional con miras a 2030. De esa manera, se busca que los resultados de este ejercicio académico y práctico permitan a los interesados y tomadores de decisiones encontrar elementos de reflexión y orientación para configurar sus estrategias empresariales en el escenario nacional.

Finalmente, el resultado de los análisis que se presentan en este documento es susceptible de revisión y actualización conforme pase el tiempo, dado que las propuestas e indicaciones que se detallan deben ajustarse con la experiencia y la revisión de la temática en un momento particular. Así, corresponde a los lectores mantenerse atentos a los cambios acelerados que en materia de ciberseguridad nacional surjan en adelante.

Marco teórico

Desarrollar un marco prospectivo en ciberseguridad nacional implica leer la dinámica de la sociedad colombiana y sus diferentes relaciones con el contexto regional e internacional alrededor de las tensiones que genera el riesgo cibernético. En este sentido, el marco Pestel se utiliza como base para determinar las tendencias que se advierten en el horizonte sobre los retos para la ciberseguridad nacional hacia 2030.

Con ocasión de la emergencia sanitaria internacional y los confinamientos que esta requirió, la transformación digital se aceleró en diferentes sectores productivos del país, así como en las esferas del Estado (World Economic Forum [WEF], 2020). Así, como resultado de esta inesperada realidad, los ciudadanos tuvieron que vincularse rápidamente con el escenario digital, lo que cambió radicalmente su manera de hacer las cosas, ahora desde una computadora o un dispositivo móvil, desde donde la vida adquiere otra dimensión y los riesgos cambian, a consecuencia de un mayor intercambio de información y exposición de las personas (Deloitte, 2019).

Los impactos de una nueva realidad digital han creado diferentes lecturas en la dinámica de la sociedad colombiana. Por un lado, el sector empresarial ha aprovechado para concretar proyectos que estaban en estudio y han creado nuevas experiencias con sus clientes que han cambiado definitivamente la manera como se relacionan con sus compradores. Por otro lado, el sector de la salud, como centro de atención actual, se ha debido ajustar igualmente para despertar a su realidad digital. Esto hace necesario avanzar rápidamente en el desarrollo y la consolidación de una cultura organizacional de seguridad de la información (Donaldson et al., 2015).

Las infraestructuras críticas cibernéticas, ahora con una mayor interacción en modalidad remota, deben entender, conocer y asegurar cómo están sus relaciones con los terceros de confianza para aumentar la resiliencia de sus operaciones frente a adversarios que traten de pasar inadvertidos en medio de las interacciones y el acoplamiento de las soluciones disponibles para su operación (Dupuy et al., 2021; Boyes, 2015).

El aumento de la superficie digital de interacción cambia la manera como el Estado define su relación con la ciudadanía. Debido a este cambio, los ciudadanos se apropian de su papel como participantes de una democracia donde los diferentes actores pueden opinar y generar tendencias, bien sea en sentido propositivo o con posiciones contrarias o reaccionarias (Soler, 2019). En este escenario, se abre un camino de inestabilidades e incertidumbre causados por las noticias falsas, la desinformación y la malinformación, que convierte las tribunas de las redes sociales en escenarios naturales para controvertir y movilizar imaginarios mediante técnicas ya probadas para influenciar positiva o negativamente a la población (Ganghi et al., 2011).

Las recientes movilizaciones en el país, las controversias sobre las noticias falsas, la propaganda política elaborada por diferentes actores y la inestabilidad reciente de los servicios de comunicaciones e internet han generado un ambiente de tensión que reafirma la

polarización del público en general, aumenta el malestar social y termina con una sensación de pérdida de gobernabilidad que poco favorece la búsqueda de soluciones negociadas en el marco de la Constitución y la ley.

Metodología

La aplicación del marco Pestel es un ejercicio de consolidación y análisis de tendencias que amplía la revisión de detalles de diferentes fuentes de información. Para efectos de este ejercicio, se consultaron diferentes publicaciones académicas (artículos de investigación, libros y revistas especializadas) y reportes internacionales (centros de pensamiento, consultoras internacionales y empresas especializadas), los cuales fueron comentados y validados con entrevistas con especialistas en ciberseguridad y ciberdefensa (académicos, ejecutivos y profesionales de ciberseguridad), que permitieron confirmar las posturas que se revelan en esta investigación.

Por otro lado, para el análisis de la ciberseguridad y ciberdefensa nacional se tomaron las diferentes perspectivas de dicho marco (política, económica, social, tecnología, ecológica y legal) situando la dinámica nacional e internacional para cada una frente a las tensiones y situaciones que pueden generar inestabilidad e incertidumbre en el escenario de los riesgos y amenazas cibernéticas. A continuación se detallan algunas preguntas claves planteadas como resultado de la revisión de los documentos y las entrevistas, con el fin de identificar y consolidar el análisis acerca de cuáles fuerzas pueden influir y fortalecerse en el mediano y largo plazo frente al reto de la ciberseguridad nacional (Tabla 1).

Tabla 1. Preguntas claves para la ciberseguridad nacional a 2030

Pestel	Preguntas claves
Político	¿Puede ser influenciado el voto ciudadano en el contexto digital? ¿Los algoritmos pueden cambiar las dinámicas sociales? ¿Se puede manipular la democracia vía redes sociales?
Económico	¿Los datos de las personas serán explotados y vendidos al mejor postor? ¿El Estado será susceptible a robos de información sensible? ¿Está expuesta la dinámica económica del país a operaciones cibernéticas?
Social	¿Las noticias falsas pueden generar tensiones relevantes para la estabilidad del país? ¿La desinformación será parte de las estrategias para generar miedo e incertidumbre? ¿Existen campañas de inestabilidad creadas para generar la percepción de incertidumbre y pérdida de gobernabilidad?

Continúa tabla...

Pestel	Preguntas claves
Tecnológico	¿La creación de perfiles y videos falsos son estrategias para manipular y suplantar a las personas? ¿La inteligencia artificial será utilizada como arma para engañar a los mecanismos de defensa actuales? ¿Pueden ser manipulados los patrones de comportamiento para crear escenarios adversos e inestables con inteligencia artificial?
Ecológico	¿Un mayor procesamiento de datos puede aumentar la emisión de gases efecto invernadero? ¿El uso de criptominería por parte de los adversarios puede afectar la huella de carbono? ¿Es deseable movilizar esfuerzos hacia el uso de computación verde como alternativa ecoeficiente?
Legal	¿Habrá un aumento de normas y regulaciones sobre protección de datos y ciberseguridad? ¿Se advierte el surgimiento del concepto de responsabilidad digital empresarial? ¿Habrá mayor control sobre el uso de los datos a nivel nacional e internacional?

Fuente: Elaboración propia

Resultados

Luego de la aplicación del marco Pestel con base en una revisión y análisis de las preguntas orientadoras hacia la ciberseguridad y la ciberdefensa nacional, se presentan a continuación las fuerzas identificadas para cada una de las perspectivas del marco y se abordan de forma individual, soportadas con algunas evidencias que sugieren su visualización y confirmación en el entorno nacional.

Tendencias a nivel político

Los elementos asociados con el ejercicio de la democracia y el respeto de las instituciones en el escenario digital plantean un reto exigente toda vez que la dinámica de la representación y la participación ciudadana está más allá del ejercicio de derechos, deberes y libertades del mundo físico. Ahora las redes sociales y la disponibilidad de información por parte de la población pueden ser un vector que potencie las garantías constitucionales o una oportunidad de debilitar y comprometer la democracia de un país (Maurer, 2018).

Tendencia 1. Influencia en el voto ciudadano

Impacto: El ejercicio de la democracia, el derecho de elegir y ser elegido en un contexto como el actual, mediado por una mayor conectividad y abundancia de información, exige el desarrollo de habilidades y competencias ciudadanas que están más allá de la

información y la educación. Se requieren capacidades individuales asociadas con la curaduría de documentos, el juicio crítico y la duda razonable, capacidades que pueden generar mayor resistencia a los intentos de terceros para favorecer una campaña específica (Lonergan, 2017).

Evidencia: Ha habido una radicalización de discursos a favor o en contra de una postura política, así como propaganda social y *social bots,* que generaron movimientos en redes sociales en contra del gobierno, muchos motivados por el uso de técnicas informáticas basadas en algoritmos y equipos de personas conformadas para crear dichas tendencias (Ospina-Valencia, 2021).

Tendencia 2. Uso de algoritmos de seguimiento y alteración de discursos sociales en línea

Impacto: El escenario digital actual mediado por plataformas, algoritmos y datos constituye un contexto base para que agentes adversos, conocidos y desconocidos, desarrollen estrategias que pueden cambiar la dinámica social de las tendencias sobre temáticas que desarrollan los ciudadanos en internet a través de sus redes sociales (Buchanan, 2020).

Evidencia: Se ha hallado el posicionamiento de temas en comunidades, cambios de perspectiva de temas sociales vigentes y manejo de noticias con verdades a medias. También se utilizan líderes de opinión e influenciadores para crear una postura deseada y difundirla con rapidez gracias a la credibilidad y visibilidad de sus autores (*El Tiempo,* 28 de mayo de 2021).

Tendencia 3. Manipulación de la democracia a través de redes sociales y comunidades

Impacto: Manipular los discursos políticos y los mensajes orientados a movilizar las intenciones de voto de los ciudadanos es una práctica que se ha potenciado a través de la desinformación, la mala información y las noticias falsas. Esto, sumado a la baja capacidad crítica de las personas frente a la confiabilidad de la información, hace que las sociedades sean proclives a engaños y manipulaciones en internet (Rowe, 2015).

Evidencia: Hay campañas de desinformación, posicionamiento de mensajes agresivos, noticias y videos falsos. Durante el 2019 y el 2020, se propagaron mensajes agresivos que llamaban a la revuelta; asimismo, hubo noticias falsas sobre acciones efectuadas por agentes del Estado y campañas de desinformación y engaño frente al tema de la pandemia (Torres, 2020).

Tendencias a nivel económico

En la actualidad, el ciberespacio configura un escenario extendido de las dinámicas sociales y económicas de una nación. En este sentido, habilitar elementos de confianza digital y nuevas oportunidades de negocio permite movilizar no solamente conexiones, sino diferentes alternativas y el desarrollo de capacidades que pueden llevar al posicionamiento de industrias e iniciativas donde se crean nuevas experiencias y surgen nuevas propuestas de valor (Hepfer & Powell, 2020).

Tendencia 1. Exfiltración y venta de información sensible de personas

Impacto: El uso de engaños, las vulnerabilidades técnicas y la baja ciberhigiene de las personas por lo general conforma un entorno propicio para las brechas de seguridad donde se comprometen datos sensibles de las personas: datos biométricos, sexo, religión, partido político, entre otros (Boney et al., 2018). Estos datos terminan siendo objeto de venta en la web oscura, donde los delincuentes los ofertan y venden al mejor postor (Maurer, 2018).

Evidencia: Hay filtraciones de datos personales, robo de bases de datos de bancos, listados de números de teléfonos móviles. Se ha venido observando un incremento de acciones delictivas por parte de los ciberdelincuentes que implica robos de identidad, robos de dinero y generación de engaños que llevan a comprometer los datos personales mediados por aplicaciones móviles (Infobae, 8 de octubre de 2021).

Tendencia 2. Robo de información sensible de Estados

Impacto: En medio de una tensión entre la transparencia y la protección de la información clave para la defensa del Estado, los adversarios distraen la atención de los Gobiernos con eventos de gran magnitud para poder, mediante el reconocimiento de los puntos débiles de sus infraestructuras, materializar fugas de información durante estas distracciones, que permitan crear ventajas estratégicas en el contexto regional y global (Daswani, 2021).

Evidencia: Se ha hallado robo de información de servidores públicos, fuga de información de miembros de las fuerzas militares (FF. MM.) y revelación de información de inteligencia. Los atacantes en Colombia han centrado la atención en bases de datos de los miembros de las FF. MM., particularmente de inteligencia, que han generado tensiones internas por la sensibilidad de la información filtrada y la posibilidad de poner en riesgo la integridad física de los integrantes de las FF. MM. (Noticias Caracol, 2021).

Tendencia 3. Patrocinio de ataques cibernéticos con fines económicos y de extorsión

Impacto: Los intereses estratégicos en el ciberespacio representan espacios de tensiones entre diferentes actores, estatales y no estatales, cada uno de los cuales busca posicionar doctrinas y estrategias que lleven al dominio de su oponente. Las ciberoperaciones, esto es, acciones cibernéticas generalmente desarrolladas por debajo del umbral del uso de la fuerza, configuran las mejores estrategias ofensivas, ya que pueden pasar desapercibidas, o ser ignoradas y negadas si llegan a ser descubiertas (Yannakogeorgos, 2014; Ahmad et al., 2012).

Evidencia: Se ha hallado la denegación de servicio en páginas oficiales del Gobierno, afectaciones de infraestructura crítica y materialización de extorsión de datos. Durante los años 2019 y 2020, con ocasión de la pandemia y la crisis social derivada de esta condición, algunas páginas del Estado fueron objetivo de denegación de servicio. De igual modo, se generaron campañas de desestabilización articuladas con agentes extranjeros que termina-

ron de acrecentar las tensiones internas y crearon el escenario para un conflicto asimétrico (Infobae, 21 de enero de 2021).

Tendencias a nivel social

Hoy por hoy, las redes sociales son el medio más expedito para que los ciudadanos de todas las edades encuentren información de forma ágil y eficiente. Pese a las bondades que estos medios pueden ofrecer, se advierten al menos tres temáticas claves que se deben tomar en cuenta de cara a la intensificación de los movimientos sociales y las tensiones entre los diferentes actores de la sociedad colombiana: Estado, partidos políticos, gremios, agremiaciones sindicales, familias y jóvenes (Douzet, 2014).

Tendencia 1. Generación de tensiones sociales con noticias falsas

Impacto: La generación de noticias falsas y el desarrollo de una arquitectura de la persuasión constituyen los conceptos básicos para comprender la manipulación de los imaginarios sociales en el contexto actual del país. Este ejercicio de posicionamiento de mensajes y temas en la dinámica social digital del país, construido desde "verdades a medias" desplegadas de manera masiva, son el referente de operaciones cognitivas que inician con una audiencia objetivo y luego continúan con mensajes y contenidos personalizados, los cuales se repiten con algunas variantes para mantener la temática vigente y así motivar un comportamiento específico en la población seleccionada (Maurer, 2018).

Evidencia: Se ha encontrado el manejo de mensajes y fotografías sobre las movilizaciones, información parcial sobre acontecimientos en las marchas y mensajes agresivos contra la fuerza pública (*El Tiempo,* 28 de mayo de 2021).

Tendencia 2. Estrategias de desinformación para crear inestabilidad nacional

Impacto: La desinformación, entendida como información falsa y deliberadamente creada para dañar a una persona, grupo social, organización o país, se ha convertido en un elemento fundamental para desarrollar una guerra cognitiva. En este contexto, la población más expuesta son los jóvenes, quienes permanecen más tiempo conectados y pocas veces contrastan lo que reciben en sus teléfonos móviles. Se observa una tendencia natural a adherirse a tribus en internet, lo que se manifiesta en mensajes movilizados por los sentimientos y no por los hechos y datos (Soler, 2019).

Evidencia: Se ha hallado el uso de *trolls,* el desarrollo de campañas de odio contra la fuerza pública, así como el uso de imágenes y videos no verificados para manejar las versiones de los hechos (Campaña Defender la Libertad, 2021).

Tendencia 3. Creación de campañas de incertidumbre y desestabilización

Impacto: Las campañas de incertidumbre y desestabilización se construyen con el propósito de crear angustia, confusión y contradicciones en la población en general. Para estas campañas se usan los eventos más representativos de la actualidad, donde no hay

posiciones formales de las autoridades y múltiples versiones circulan alrededor del tema (Jordán, 2021).

Evidencia: Hay manipulación del discurso de la efectividad de las vacunas, videos manipulados donde no se aplica la vacuna y estadísticas alteradas sobre decesos por aplicación de los agentes biológicos (Meza, 2021).

Tendencias a nivel tecnológico

La tecnología avanza a pasos agigantados y su incorporación a la vida cotidiana se hace de manera acelerada. Los *chatbots,* los asistentes digitales y la robótica constituyen nuevas tendencias donde la convergencia y convivencia entre lo humano y lo digital se hace más evidente. En este contexto, los avances propios de la inteligencia artificial que mejoran las condiciones de vida de la mayoría de personas contrastan con los usos adversos que empiezan a despuntar y a generar incertidumbre en la dinámica del ciberespacio (Deloitte, 2019).

Tendencia 1. Diseño y generación de suplantaciones y videos falsos

Impacto: El uso acelerado de los algoritmos de inteligencia artificial ha generado muchas oportunidades en diferentes sectores de negocio al tiempo que ha incorporado nuevas amenazas y riesgos para los que muchas organizaciones no se encuentran preparadas. La manipulación de las imágenes, voz y videos con fines no autorizados se ha incrementado por el uso de algoritmos de aprendizaje y de aprendizaje profundo, que logran darle forma a suplantaciones, extorsiones y engaños (Cano, 2018).

Evidencia: Existe manipulación de imágenes de personalidades públicas, manipulación de videos públicos y suplantación de voz de ejecutivos (Ospina-Valencia, 2021).

Tendencia 2. Generación de ciberataques con inteligencia artificial sobre infraestructuras críticas

Impacto: Las infraestructuras críticas cibernéticas han venido siendo blanco de operaciones ofensivas en el ciberespacio. El uso de algoritmos de aprendizaje profundo con el fin de engañar los mecanismos de defensa disponibles pone en evidencia las nuevas capacidades de los adversarios para profundizar sus estrategias de engaño y manipulación más allá de las vulnerabilidades conocidas hasta hace poco (Raban & Hauptman, 2018).

Evidencia: Se han hallado ataques mediados por drones operados con inteligencia artificial, suplantación de voz de ejecutivos de alto nivel y activación de *malware* sensible a características de las personas. Si bien no todos los eventos mencionados se han materializado en el país, hay evidencia a nivel internacional de eventos adversos de ciberataques basados en inteligencia artificial (Semana, 2021).

Tendencia 3. Uso de la inteligencia artificial con fines adversos

Impacto: La inteligencia artificial como posibilidad de automatización y generación de acciones semejantes a las humanas puede ser usada con fines no autorizados. Cuenta

con la capacidad de compilar, analizar y generar patrones de comportamiento, obtener analíticas de imágenes o sonidos, configurar un escenario emergente de armas autónomas especializadas que sean capaces de cambiar y mutar sus estrategias a medida que hayan sido identificadas (Xiao et al., 2018).

Evidencia: Existe inteligencia artificial adversarial, generación de redes adversariales, desarrollo de robots con inteligencia artificial autónoma. Estos elementos se evidencian en una visión prospectiva con el fin de mantenerlos en monitoreo, ya que actualmente despuntan a nivel internacional y poco a poco estarán disponibles no solo para los países en desarrollo, sino igualmente para los adversarios (Riquelme, 2020).

Tendencias a nivel ecológico

A nivel internacional se ha venido insistiendo en los impactos concretos que se tienen sobre el cambio climático. La tecnología no ha sido ajena a esta dinámica, de modo que se han revisado las políticas de adquisición de nuevos componentes tecnológicos y de proveedores de servicios en la nube, y se ha ampliado la conciencia frente a su huella de carbono. Si bien esto aún no se concibe como una política concreta en las organizaciones, comienza a despuntar en la medida que crece la presión internacional sobre el tema. En consecuencia, las organizaciones y naciones tendrán que mantener y desarrollar una perspectiva ecológica que conecte sus retos propios de la transformación digital con el desafío de mitigar sus aportes a la emisión de gases de efecto invernadero (Soler, 2019).

Tendencia 1. Aumento del efecto de gases invernadero por mayor procesamiento de datos

Impacto: El uso intensivo de procesamiento de información por las organizaciones y el aumento de participación de terceros con infraestructura en la nube (McKinsey & Company, 2021) incrementan el uso de energía, cuya disipación aumenta los gases de efecto invernadero. En particular las empresas Gafam (Google, Apple, Facebook, Amazon, Microsoft) tienen una amplia influencia a nivel global, ya que generan porcentajes de CO_2 equivalentes a lo que producen los vehículos en un año (Nogueira, 2020).

Evidencia: Hay contaminación digital por búsquedas, una huella de carbono importante de las Gafam y una mayor utilización de la computación en la nube. Mientras continúe aumentando el procesamiento de información con terceros, como ha venido ocurriendo con ocasión de la emergencia sanitaria internacional, esta tendencia se mantendrá al alza en los próximos años.

Tendencia 2. La criptominería como factor clave en la huella de carbono

Impacto: Con el aumento de la penetración del internet de las cosas (IoT), la domótica y la convergencia entre lo físico, lo lógico y lo biológico, se expande la superficie de dispositivos disponibles y conectados. Estos dispositivos pueden ser comprometidos e incorporados de manera no autorizada a redes de minería de criptomonedas que, de forma imperceptible, utilicen su capacidad de procesamiento, lo cual puede generar bajo

desempeño en los dispositivos y, por lo tanto, aumentar la huella de carbono sin ser detectados (Oliver, 2020).

Evidencia: Ha habido un incremento de IoT, transformación digital de empresas y criptominería en IoT. Estos elementos serán temas relevantes en los próximos años con la aceleración de la puesta en marcha de iniciativas digitales en el país, así que habrá que estar atentos a analizar y mantener especial atención al tema de seguridad y control en estos dispositivos, para que no sean pivotes que generen procesamiento de información innecesario y terminen afectando la huella de carbono de las empresas.

Tendencia 3. Uso de la computación verde como alternativa ecoeficiente para las empresas y naciones

Impacto: La computación verde es una apuesta de las organizaciones y naciones para incorporar dispositivos que consuman menos energía y estén construidos con componentes menos contaminantes. En la medida que se plantean esquemas de transición energética a nivel global, la computación de igual forma debe alinearse con esta tendencia. El proceso de transformación digital deberá considerar estas nuevas condiciones propias del reconocimiento de la huella de carbono y sus impactos por posibles acciones no autorizadas que comprometan la manera como manejan sus emisiones de CO_2 (Saha, 2018).

Evidencia: Hay inversiones en computación verde, centros de cómputo bajo el océano y plantas de energías alternativas. En el país se advierte un movimiento consolidado de empresas que incluyen cada vez más en sus prácticas de negocio el tema de la sostenibilidad ambiental, lo que implica que habrá más iniciativas que terminen incorporando tecnologías verdes como alternativa natural de sus inversiones para alinearlas con sus perspectivas de respeto por el medio ambiente (Lastra, 2007).

Tendencias a nivel legal

En la dinámica internacional del ciberespacio se hace necesario comprender la responsabilidad y el cumplimiento que se debe tener respecto a las iniciativas digitales y sus impactos a nivel individual, corporativo, nacional y global. En este sentido, las iniciativas de regulación y control de corte legal y jurídico, así como las acciones no vinculantes, se están acelerando, dado el hecho de que en este nuevo ciberdominio, donde la interacción humana ahora se amplía, existen muchos vacíos y acciones que están quedando fuera de los radares legislativos, lo cual genera zonas grises que son aprovechadas por agentes agresores no estatales o apalancados desde las sombras por otros Estados (Buchanan, 2020).

Tendencia 1. Regulaciones vigentes sobre protección de datos y ciberseguridad

Impacto: Con el aumento de la densidad digital, se advierte un mayor flujo de datos personales a través de dispositivos de IoT, relojes inteligentes, aplicaciones móviles, entre otras plataformas, en un entorno donde el ciberriesgo se puede materializar en cualquier conexión o acoplamiento de iniciativas digitales disponibles. Esto puede terminar no solo afectando el producto o servicio, sino en algunos casos la misma vida humana (Cano, 2019).

Evidencia: Hay una creciente transformación digital, conexión de dispositivos médicos y domótica.

Tendencia 2. Incorporación del concepto de responsabilidad digital empresarial

Impacto: En su ejercicio de conexión entre la dinámica empresarial y el desarrollo de experiencias de valor para los individuos, las organizaciones proponen estrategias que vinculan retos o problemáticas con iniciativas tecnológicas. En este contexto, los datos individuales y las interacciones de los clientes se convierten en el insumo fundamental con que capitalizan sus esfuerzos, bien para producir cambios significativos en la forma de hacer las cosas o para cambiarlas de manera disruptiva, lo que conecta el producto o el servicio con distintas aristas sociales, económicas, ambientales y tecnológicas, entre otras (Wade, 2020).

Evidencia: Existe confianza digital, responsabilidad digital y retribución por uso de los datos. Si bien los recientes documentos de política pública incluyen los temas de confianza digital como habilitadores del bienestar y desarrollo económico del país, las iniciativas internacionales, al reconocer que ahora las empresas son negocios básicamente de manejo de datos, están avanzando en incorporar el concepto de *responsabilidad digital empresarial* como el nuevo sello que reconoce los esfuerzos corporativos por encontrar un balance en medio de las tensiones y exigencias que se tienen en el tratamiento de datos de las personas (Cano & Marroquín, 2021).

Tendencia 3. Incremento de las regulaciones y control de los datos

Impacto: En diferentes publicaciones nacionales e internacionales se ha insistido que los datos y la información constituyen uno de los activos más importantes para las empresas, no solo por lo que representan para sus modelos de negocio, sino por la relevancia que adquieren frente a los derechos de los individuos en un contexto digital como el actual. En este sentido, múltiples actores reguladores, entidades multilaterales y Gobiernos han venido insistiendo en propuestas regulatorias y exigiendo una mayor protección de los datos como ejercicio de responsabilidad corporativa y nacional frente al uso y tratamiento de la información de la ciudadanía (Shiroishi et al., 2018).

Evidencia: Existen leyes de privacidad, regulaciones propias de sectores productivos, así como el reconocimiento de los derechos humanos en el ciberespacio. En Colombia, la normatividad sobre protección de datos y respeto de derechos en el contexto cibernético ha avanzado de la mano con las acciones que se han derivado de la lucha contra el crimen cibernético. Es importante anotar que algunos sectores vienen incluyendo regulaciones más exigentes en los temas de ciberseguridad.

Discusión

Los resultados presentados en este estudio, fundados en las revisiones hechas desde el marco Pestel para la ciberseguridad nacional, establecen un punto de partida para realizar

mayores y mejores análisis sobre la evolución de las diferentes tendencias identificadas. En este sentido, los analistas y tomadores de decisiones deben permanecer atentos a la evolución del entorno actual en el país y las tensiones que se derivan de múltiples eventos a nivel internacional, como la reciente toma de control de los talibanes en Afganistán, que motivó un movimiento humanitario por parte del Gobierno colombiano para recibir al menos 4000 refugiados de este país, lo que finalmente no se dio (*Portafolio,* 20 de septiembre de 2021).

Por otro lado, los eventos recientes de ataques a la infraestructura crítica norteamericana han puesto a prueba el nivel de preparación de EE. UU. frente a este tipo de eventos adversos, lo que ha revelado fragilidades inherentes en diferentes sectores críticos. Fragilidades como estas pueden terminar afectando la dinámica política, económica y social del país, lo que genera una sensación de incertidumbre que puede ser aprovechada por otros países para concretar acciones que tienden a consolidar conflictos en la zona gris. En este nuevo entorno no es posible actuar de forma individual, sino a través de alianzas internacionales y acciones conjuntas para disuadir y tratar de desescalar las acciones de adversarios que se mueven en la niebla de las mismas tensiones internacionales (Jordán, 2018).

En este contexto, Colombia se encuentra en una zona de conflicto cibernético que ha vinculado a diferentes actores no estatales, quienes aprovechan las dinámicas sociales y el aumento del uso de la tecnología para capitalizar tendencias y acciones con fines adversos. Estas acciones se sirven de movimientos sociales con el fin de concretar agresiones en contra de las instituciones nacionales y la infraestructura pública. De esta forma, los resultados de este estudio confirman los recientes eventos ocurridos en el país con ocasión de la protesta social, que inicialmente se configuró como un ejercicio democrático y pacífico, pero luego terminó con manipulaciones y desinformación diseminada por agentes no estatales a través de redes sociales.

Las posibilidades de que se presente un ciberataque a cualquier nación u organización de cualquier tamaño y de cualquier sector hacen necesario aumentar la capacidad de anticipación, de demora y disuasión frente a las capacidades de acción que puedan tener los adversarios (Skopik & Pahi, 2020). Es necesario reconocer al menos los movimientos naturales de los adversarios, como la inteligencia, las técnicas de engaño, la identificación de pivotes (puntos de ingreso) y el despliegue de acciones maliciosas, con el fin de concretar la brecha o inestabilidad prevista, y trabajar desde allí, para avanzar en una estrategia no estandarizada, que haga más difíciles las acciones y propósitos de un posible agresor. Esto, en últimas, significa romper con la dinámica de lo conocido en pro de crear capacidades apropiadas para enfrentar la incertidumbre.

Conclusión

Mirar al futuro es un ejercicio que debe iniciar en el presente. Es un reto que implica explorar con claridad las perspectivas y tendencias que se advierten en el entorno, no en

busca de certezas, sino explorando las posibilidades que puedan darle forma a la incertidumbre. Así se podrá ver dónde ubicar la mirada para trazar rutas alternas que permitan concretar las estrategias más adecuadas frente a los retos particulares de las empresas y naciones (Fergnani et al., 2020; Wolfowitz et al., 2018).

En este escenario, la ciberseguridad nacional enfrenta diferentes tensiones y fuerzas a nivel político, económico, social, tecnológico, legal y ecológico, que demandan salir de la postura tradicional de "esperar y ver", para movilizar reflexiones y esfuerzos que permitan "delinear y actuar". Esto es lo que hará posible adoptar decisiones estratégicas para identificar alternativas que le permitan al país situarse en una posición privilegiada, desde la cual trabaje por influenciar nuevos patrones de acción que confirmen su liderazgo nacional e internacional (McNulty, 2021).

A nivel político, es importante mantener la mirada puesta en las dinámicas de la democracia, como un factor fundamental para fortalecer la institucionalidad ahora en el ciberespacio. Esto implica aprender a convivir y desarrollar las prácticas de participación ciudadana en el ciberespacio que las hagan resistentes a acciones como la desinformación, la manipulación y otras estrategias híbridas. Esto se convierte en el nuevo horizonte de la gobernabilidad del país y las empresas, más allá de las actividades tradicionales que se desarrollan en la actualidad (Lonergan, 2017).

A nivel económico, es importante comprender que los datos y la información se han transformado en activos valiosos, que adquieren valor no solo por su existencia, sino por la capacidad que tienen de cambiar la realidad, transformar la experiencia de las personas, darles acceso a nuevas oportunidades o por el contrario convertirse en objetivos de acciones adversas que pueden comprometer su buen nombre, sus valores financieros o su integridad física. En este sentido, la extorsión y los robos de información sensible deben ser parte de la agenda de seguridad tanto de empresas como de Estados (Alcolea, 2012; Cano, 2021).

A nivel social, el reto resulta mayor, puesto que las tensiones sociales propias de las dinámicas de los países terminan siendo parte de operaciones psicológicas y cibernéticas para crear zozobra, inestabilidad y entornos agresivos que terminan favorecieron intereses oscuros. Las redes sociales, el manejo de agentes automáticos, *influencers, trollers,* entre otros, deben ser temas que marquen la agenda del plan de ciberseguridad nacional, como parte del equilibrio de garantías que los Estados deben brindar tanto para el uso de estos medios sociales de forma legítima como para los usos que resulten en deterioro de la convivencia y la estabilidad nacional (Singer & Brooking, 2018).

A nivel tecnológico, es importante mantener un panorama actualizado de las tecnologías emergentes y disruptivas, con el fin de evaluar sus potencialidades y oportunidades para ofrecer mayores y mejores productos y servicios, así como revisar, analizar y simular sus posibles usos adversos. Esto permitirá reconocer nuevos patrones y amenazas que puedan comenzar a comprometer las condiciones defensivas, de modo que se pueda actuar de forma anticipada para atender incidentes que se puedan presentar. En la actualidad, omi-

tir el seguimiento de los nuevos desarrollos de la inteligencia artificial y sus usos adversos representa una posición temeraria para cualquier Estado o empresa, dado que podrán ser fácilmente superados con las capacidades que se advierten a la fecha y en el futuro para estas tecnologías (Hoffman & Levite, 2017; Dash et al., 2021).

A nivel ecológico, en principio parecería que la ciberseguridad nacional no tiene aspectos que cuidar y mantener; pero nada es más distante de la realidad, pues las implementaciones tecnológicas actuales y la mayor dependencia de terceros hace al ciberespacio corresponsable de la huella de carbono global. Esto implica que el factor ambiental no puede excluirse de la ecuación cibernética, sino que debe ser un tema vinculante, dado que la "polución que genera el tratamiento de los datos" no solo hace parte del reto de los Estados y empresas en el ciberespacio, sino que es un compromiso más frente a la protección del entorno, que debe considerarse en el diseño y la puesta en operación de las iniciativas digitales actuales y futuras (Nogueira, 2020).

A nivel legal, las naciones y empresas se enfrentan a la dificultad de una construcción dinámica de buenas prácticas y estándares que de forma acelerada quedan obsoletos. Por ello mismo, las iniciativas internacionales de organismos multilaterales, las tendencias alrededor de la responsabilidad digital empresarial y la exigencia de la protección de datos se convierten en el mapa base de la revisión y actualización constantes, al que se deben mantener atentas las diferentes profesiones, como un ejercicio de responsabilidad digital convergente, donde los derechos, deberes y libertades de los individuos siempre estarán en juego (Pricewaterhouse Coopers [PwC], 2020).

En consecuencia, este ejercicio de prospectiva sobre la ciberseguridad nacional al 2030 deja de ser una mirada futurista y elevada de la realidad para convertirse en una manera de aterrizar los retos y realidades del país y las empresas, como protagonistas principales de las transformaciones que requiere la nación de cara a una acelerada transformación digital. Esta acelerada y constante transformación ha cambiado la manera de hacer las cosas e invita a todos los actores a sumar esfuerzos para potenciar las ventajas del ciberespacio en la dinámica de la sociedad (Téllez, 2016), al tiempo que se cierran filas frente a aquellos adversarios (visibles e invisibles) que quieran aprovechar sus vulnerabilidades inherentes como vectores de desestabilización e inestabilidad (Buchanan, 2020).

Agradecimientos

El autor desea agradecer a la Escuela Superior de Guerra "General Rafael Reyes Prieto" por su apoyo en la realización de este artículo.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo. Este artículo presenta los resultados del proyecto de investigación "La guerra asimétrica, híbrida e irrestricta: Retos, amenazas y desafíos para los Estados, la seguridad y defensa regional", del grupo de investigación "Masa Crítica", de la Escuela Superior

de Guerra "General Rafael Reyes Prieto", categorizado como A1 por MinCiencias y con código de registro COL0123247. Los puntos de vista pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Financiamiento

El autor no declara fuente de financiamiento para la realización de este artículo.

Sobre el autor

Jeimy José Cano Martínez es Ph.D. en *business administration* por la Newport University y Ph.D en educación por la Universidad Santo Tomás. Es ingeniero y magíster en ingeniería de sistemas y computación por la Universidad de los Andes, y especialista en derecho disciplinario por la Universidad Externado. Profesor investigador de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

https://orcid.org/0000-0001-6883-3461 - Contacto: jeimy.cano@esdeg.edu.co

Referencias

Ahmad, R., Yunos, Z., Sahib, S., & Yusoff, M. (2012). Perception on cyber terrorism: A focus group discussion approach. *Journal of Information Security, 3*(3). https://doi.org/10.4236/jis.2012.33029

Alcolea, D. (2012). *Las nuevas estrategias de defensa nacional* (Documento de Opinión n.º 68). Instituto Español de Estudios Estratégicos. https://bit.ly/3twS5PU

Boney, B., Hayslip, G., & Stamper, M. (2018). *CISO Desk Reference Guide. A practical guide for CISOs* (vol. 2). CISO DTG Joint Venture Publishing.

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review, 5*(4), 28-34. http://timreview.ca/article/888

Buchanan, B. (2020). *The hacker and the state. Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Campaña Defender la Libertad. (2021, 9 de mayo). *Fiscalía y Procuraduría deben investigar discursos de odio que han instigado los atentados sicariales en contra de las manifestantes del Paro Nacional*. https://bit.ly/3is8sqp

Cano, J., & Marroquín, J. (2021). Responsabilidad digital corporativa: una revisión sistemática. *ISLA 2021 Proceedings 6*. https://aisel.aisnet.org/isla2021/6

Cano, J. (2018). Repensando los fundamentos de la gestión de riesgos. Una propuesta conceptual desde la incertidumbre y la complejidad. *Revista Ibérica de Tecnología y Sistemas de la Información, E15*(4), 76-87. https://bit.ly/3JAdD3q

Cano, J. (2019). Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo. *Revista Sistemas, 151*, 63-73. https://doi.org/10.29236/sistemas.n151a5

Cano, J. (2021). *Ciberseguridad empresarial. Reflexiones y retos para los ejecutivos del siglo XXI*. Lemoine Editores.

Choucri, N. (2012). *Cyberpolitics in international relations*. The MIT Press.

Dash, P., Karimibiuki, M., & Pattabiraman, K. (2021). Stealthy attacks against robotic vehicles protected by control-based intrusion detection techniques. *Digital Threats: Research and Practice, 2*(1), 1-25. https://doi.org/10.1145/3419474

Daswani, N. (2021, 15 de enero). *Understanding third-party hacks in the aftermath of the SolarWinds breach*. Helpnet Security. https://bit.ly/3ws2VbK

Deloitte Development. (2019). *The future of cyber survey 2019. Cyber everywhere. Succeed anywhere*. https://bit.ly/3Jv44mh

Donaldson, S., Siegel, S., Williams, C., & Aslam, A. (2015). *Enterprise cybersecurity. How to build a successful cyberdefense program against advanced threats*. Apress.

Douzet, F. (2014). Understanding cyberspace with geopolitics. *Hérodote, 1-2*(152-153), 3-21. https://doi.org/10.3917/her.152.0003

Dupuy, A., Nussbaum, D., Butrimas, V., & Granitsas, A. (2021, 13 de enero). Energy security in the era of hybrid warfare. *NATO Review*. https://bit.ly/3KVxgDw

El Tiempo. (28 de mayo de 2021). Las noticias falsas que no debe creer en medio del paro. https://bit.ly/3tvfX6s

Fergnani, A., Hines, A., Lanteri, A., & Esposito, M. (2020, 25 de septiembre). Corporate foresight in an ever-turbulent era. *European Business Review*. https://bit.ly/37Ka78F

Ganghi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimension of cyber-attacks. Social, political, economic, and cultural. *IEEE Technology and Society Magazine, 30*(1), 28-38. https://doi.org/10.1109/MTS.2011.940293

Hepfer, M., & Powell, T. (2020). Make cybersecurity a strategic asset. *MIT Sloan Management Review, 62*(1), 40-45. https://bit.ly/36l6c1Y

Hines, A., & Bishop, P. (2015). *Thinking about the future. Guidelines for strategic foresight*. Formating Experts.

Hoffman, W., & Levite, A. (2017). *Private sector cyber defense: Can active measures help stabilize cyberspace?* Carnegie Endowment for International Peace. https://bit.ly/3JFa1NH

Infobae. (2021, 21 de enero). *Gobierno dice que ciberataque a páginas de la Presidencia de Colombia se hizo desde Rusia y Ucrania*. https://bit.ly/3Nby498

Infobae. (2021, 8 de octubre). *Estos son los ciberdelitos más comunes en Colombia, según la Policía Nacional*. https://bit.ly/3L63Y4Y

Jordán, J. (2018). El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo. *Revista Española de Ciencia Política, 48*, 129-151. https://doi.org/10.21308/recp.48.05

Jordán, J. (2021). *Disuasión en la zona gris: una valoración exploratoria aplicada a Ceuta y Melilla* (Global Strategy Report 28). Global Strategy. https://bit.ly/3L9sjqK

Lonergan, S. (2017). *Cyber power and the international system* (tesis doctoral, Graduate School of Arts and Sciences, Columbia University). Columbia Academic Commons. https://doi.org/10.7916/D88D07PH

Maurer, T. (2018). *Cyber mercenaries. The state, hackers, and power*. Cambridge University Press

McKinsey & Company. (2021). *The top trends in tech. Executive summary download*. https://mck.co/3uszuDC

McNulty, E. (2021, 7 de enero). To see the future more clearly, find your blind spots. *Strategy+Business*. https://bit.ly/3qzwrsd

Meza, A. (2021, 10 de febrero). Cuatro grandes mentiras sobre las vacunas contra el Covid-19. *Revista Digital. France24*. https://bit.ly/3IzJMqD

Nogueira, R. (2020, 21 de diciembre). Reducir el CO_2 a golpe de clic. *Ethic*. https://bit.ly/356Nydm

Noticias Caracol. (2021, 11 de julio). *La historia secreta del hackeo más grave contra las Fuerzas Militares de Colombia*. https://bit.ly/3wwpN9U

Oliver, R. (2020, 13 de febrero). Bitcoins, el 'supervillano' virtual del medio ambiente. *Ethic*. https://bit.ly/3tBqVHv

Ospina-Valencia, J. (2021, 6 de mayo). Protesta popular en Colombia: ¿guerra de imágenes falsas en redes sociales o realidad inimaginada en las calles? *DW*. https://bit.ly/3qzkvql

Portafolio. (2021, 20 de septiembre). Por ahora, refugiados afganos no llegarán a Colombia. https://bit.ly/3ICnzbp

Pricewaterhouse Coopers (PwC). (2020). *Global Digital Trust Insights Survey 2021. Cybersecurity comes of age* (Global Report). https://pwc.to/3iLzs4f

Raban, Y. & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *Foresight, 20*(4), 353-363. https://doi.org/10.1108/FS-02-2018-0020

Riquelme, R. (2020, 3 de febrero). Conoce a los robots con inteligencia artificial. *El Economista*. https://bit.ly/374aXgo

Rowe, N. (2015). The attribution of cyberwarfare. En Green, J. (Ed.), *Cyber warfare. A multidisciplinary analysis*. Routledge.

Saha, B. (2018). Green computing: current research trends. *International Journal of Computer Sciences and Engineering, 6*(3), 467-469. https://doi.org/10.26438/ijcse/v6i3.467469

Semana. (2021, 19 de octubre). Imitando la voz del gerente con computadora, ladrones hurtan más de 35 millones de dólares a un banco. https://bit.ly/3tPlJ2F

Shiroishi, Y., Uchiyama, K., & Suzuki, N. (2018). Society 5.0: for human security and well-being. *IEEE Computer, 51*(7), 51-55. https://doi.org/10.1109/MC.2018.3011041

Singer, P. W., & Brooking, E. (2018). *LikeWar. The weaponization of social media*. Houghton Mifflin Harcourt Publishing Company.

Skopik, F., & Pahi, T. (2020). Under false flag: using technical artifacts for cyber attack attribution. *Cybersecurity, 3*(8). https://doi.org/10.1186/s42400-020-00048-4

Soler, E. (2019). *El mundo en 2020: diez temas que marcarán la agenda global* (CIDOB Notes 220). https://bit.ly/3K58YGU

Téllez, F. (2016). Prefijo CIBER: arqueología de su presencia en la sociedad del conocimiento. *Investigación y Desarrollo, 24*(1), 142-162. https://dx.doi.org/10.14482/indes.24.1.8688

Torres, M. (2020). *Desde Venezuela se manipularon marchas en Colombia para generar violencia: John Müller*. La FM. https://bit.ly/3iLzIQK_

Wade, M. (2020, 28 de abril). Corporate responsibility in the digital era. *Sloan Management Review*. https://bit.ly/3DqpChH

Wolfowitz, P., Rivera, K., & Ware, G. (2018, 9 de octubre). Planning for the unexpected. *Strategy+Business*. https://bit.ly/2WKbsVJ

World Economic Forum (WEF). (2020). *COVID-19 Risks Outlook. A preliminary mapping and its implications* (Insight Report). https://bit.ly/3qJGaMQ

Xiao, C., Li, B., Zhu, J., He, W., Liu, M., & Song, D. (2018). Generating adversarial examples with adversarial networks. En *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence* (IJCAI-18, pp. 3905-3911). https://doi.org/10.24963/ijcai.2018/543

Yannakogeorgos, P. (2014). Rethinking the threat of cyberterrorism. En T. Chen, L. Jarvis, & S. Macdonald (Eds.), *Cyberterrorism. Understanding, assessment, and response* (pp. 43-62). Springer Verlag. https://doi.org/10.1007/978-1-4939-0962-9_3