Elementos para la conceptualización de la ciberseguridad nacional

Manuel Balcázar Villarreal*

Resumen

La ciberseguridad nacional se visualiza como un concepto en permanente construcción y alto grado de atomización con un desarrollo asimétrico entre los cuatro campos tradicionales del poder. En este texto se evalúan de manera integral los elementos más representativos en cada campo de poder. Asimismo, se propone una definición integral en la que los enfoques tradicionales de seguridad nacional se trasladan al ámbito cibernético bajo un enfoque global que permita la rectoría del Estado-Nación, atendiendo las características que este concepto pueda tener en los distintos países.

Palabras clave: Ciberseguridad nacional, contenido cibernético.

Abstract

National cybersecurity is seen as a concept in permanent construction and a high degree of atomization with an asymmetric development between the four traditional fields of power. In this text, the most representative elements in each field of power are comprehensively evaluated. Likewise, a comprehensive definition is proposed in which traditional national security approaches are transferred to the cyber sphere under a global approach that allows the stewardship of the Nation-State, taking into account the characteristics that this concept may have in different countries.

Keywords: National cybersecurity, cybercontent.

* Mtro en Administración Pública en el INAP; investigador asociado del Centro de Estudios sobre Seguridad, Inteligencia y Gobernanza (CESIG) del ITAM | manuelbalcazar@madisonmex.com

Definiciones generales

Seguridad nacional: Condición requerida para el cumplimiento de los objetivos nacionales permanentes y actuales, en un marco de ausencia de amenazas y riesgos manejables para el desarrollo de las actividades sociales, políticas y económicas. Dicha condición se basa en la protección de intereses y fortalecimiento de capacidades en los cuatro campos tradicionales del poder.

Ciberseguridad nacional: Conjunto de condiciones generadas dentro del espectro cibernético y transmitidas por cualquier red digital orientadas a propiciar el cumplimiento de los objetivos nacionales, actuales y permanentes, en un entorno de amenazas contenidas y detección de riesgos en interacción con los gobiernos de los países democráticos para promover el desarrollo de actividades sociales, políticas, económicas y de seguridad en los cuatro campos tradicionales de poder a escala nacional e internacional.

En el concepto tradicional de Estado-Nación, la trilogía población, territorio y gobierno tienen un espacio concreto de actuación que origina el sentido de pertenencia y detona esquemas de organización para la convivencia de la población en base a un pacto social y normativo.

Bajo la dinámica cibernética el **componente poblacional** se mantiene y amplía permitiendo que ciudadanos de otras naciones tengan interacción en territorio nacional mediante la vía digital, desafiando la conceptualización tradicional de soberanía y límites territoriales, en donde el consenso —interno y externo— se encuentra en proceso de construcción.

De esta manera es cada vez más frecuente que los connacionales de cualquier país se involucren en actividades de apoyo a causas, personas o sucesos, generando grandes comunidades virtuales de cibernautas que, al margen de la proximidad física, han logrado tener incidencia en la agenda pública de varios países.

Asimismo, la creación de espacios virtuales como el metaverso, plataformas de videojuegos en línea, comercio digital y servicios financieros, así como espacios de redes sociales, permite también la generación de lazos estrechos, vinculación de personas que de no ser por la tecnología jamás habrían coincidido, generando relaciones que podrían vulnerar la seguridad nacional, como se demostró con las filtraciones de Jack Teixeira, ex integrante de la Guardia Nacional de Estados Unidos.

Esta inminente interacción global de cibernautas aglutinados para dar respaldo a causas específicas de tipo social fue ampliamente estudiada y conceptualizada a mediados de la década de 1990 del siglo pasado por David Rondfelt y John Arquilla (RAND Corporation), quienes mencionaban ya el concepto de "guerras sociales transnacionales".[1]

En este concepto los autores mencionaron que "la guerra de redes sociales está en su infancia como modelo de conflicto y los gobiernos están apenas empezando a aprender de él. México es uno de los primeros en experimentarlo".

1 D. a. A. J. e. a. Ronfelt, «The Zapatista Social Netwar in Mexico,» RAND Arroyo Center, Santa Monica, CA, 1998.

Con relación a la **territorialidad** asociada al concepto tradicional de Estado-Nación, el enfoque cibernético amplía también el espacio de interacción, promoción y defensa de los intereses nacionales, haciendo del intangible espacio virtual un espacio no geográfico de reconocimiento territorial. Sin embargo, las legislaciones sobre la jurisdicción de las leyes se encuentran aún incipientes en varios países del hemisferio, con áreas de ambigüedad que implican ventanas de vulnerabilidad explotadas por organizaciones delictivas nacionales o internacionales que se ven beneficiadas por la ausencia de criterios para identificar la competencia legal de los estados nacionales dentro del espacio virtual.

Así, el surgimiento de territorios virtuales y habitantes cibernéticos a escala global lleva también a la redefinición del paradigma de territorialidad que, en ocasiones, puede basarse en infraestructura no localizada en la órbita terrestre, articulada por conexión satelital, con participación de empresas privadas con roles fundamentales, como se observa en el conflicto por la invasión de Rusia a Ucrania, en donde el apoyo de la red satelital proporcionada por *Starlink* ha sido determinante para mantener telecomunicaciones y desarrollar acciones ofensivas mediante drones.

En materia de la redefinición asociada al concepto tradicional de **gobierno** del estado nacional, la expansión de empresas, la alta movilidad laboral global —especializada y no especializada— y el dinamismo de los mercados internacionales en los sectores tradicionales de la economía, sumados al sector tecnológico amplía también la presencia de intereses nacionales en distintas latitudes, que apoyan su operación mayoritariamente en plataformas virtuales del espectro cibernético, demandando a los gobiernos nuevas soluciones tecnológicas y esquemas de interacción electrónica permanente.

Bajo este esquema enfoques weberianos como el monopolio legítimo de la violencia pueden ampliarse hacia el monopolio legítimo de la información, además de considerar otro tipo de esquemas como la violencia digital, manipulación, desinformación y negación de servicios mediante la restricción del acceso a las redes, manipulación de sistemas cibernéticos y/o afectación a la infraestructura crítica de cualquier Estado-Nación.

Así, bajo una profunda redefinición de los conceptos tradicionales, surgen nuevos elementos potencialmente constitutivos de un ciberestado nacional, en tanto generadores de poder y multiplicadores de la fuerza como son los sistemas de operación autónomos y la inteligencia artificial, cada vez más disponible a menor costo a un mayor número de habitantes, con grandes oportunidades para resolver los problemas nacionales e internacionales. Pero también con el potencial mal uso de transformarse en ventanas de vulnerabilidad empleadas por unos pocos grupos para beneficio ilegítimo, al margen de cualquier esquema de legalidad, ética y moralidad.

Bajo esto contexto es necesario establecer una conceptualización de los temas más apremiantes para la ciberseguridad nacional, basada en los mayores impactos a los campos de poder y una agenda de riesgos informáticos, dado que "los incidentes cibernéticos de

valor para la seguridad internacional ocurren con regularidad incremental. Conocer como documentar las actividades cibernéticas es de valor para muchas organizaciones, tanto corporativas como gubernamentales, académicas y para especialistas de seguridad"[2].

Lo anterior permitirá orientar las discusiones, identificar las prioridades y determinar la asignación de recursos y construcción de capacidades que permitan encauzar y mantener actualizada la transición cibernética para la consecución de los objetivos nacionales, tomando como punto de partida los cuatro campos tradicionales del poder: social-cultural; económico; político y militar-seguridad.

Campo socio cultural

Dentro del impacto del avance cibernético en el campo sociocultural, se aprecia de manera destacada el acceso masivo a dispositivos digitales móviles y uso de internet, que de acuerdo con la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020 del INEGI, reportó un total de 84.1 millones de usuarios de internet y "88.2 millones de usuarios de teléfonos celulares, de los cuales para 2020, 91.8% de los usuarios de teléfono celular cuenta con un equipo inteligente (*Smartphone*)"[3].

De esta manera, se estima que, de los 129 millones de mexicanos residentes en territorio nacional, 62% (80 millones 697 mil 600) cuenta con un *smartphone*. Ello implica también el acceso a plataformas y contenidos digitales para la generación, difusión y consumo de contenidos en temas de gran variedad y cobertura geográfica básica y nacional, que puede identificarse en la generación de *chats* en plataformas de mensajería para temas de vivienda, colonias, regiones, entidades federativas o el país, sin menoscabo de temas de interés específico, comunidades de compra-venta de bienes y servicios, entre otros.

A estos más de 80 millones de mexicanos se debe agregar el número de connacionales radicando en el extranjero que, de acuerdo con la Secretaría de Relaciones Exteriores (SRE), ascendió a 12 millones 145 mil 143 mexicanos en el 2021[4].

Como puede apreciarse, el potencial de ciberciudadanos mexicanos representa un universo muy significativo, al que se agregan personas de otras nacionalidades con presencia física o virtual en México, que representan un área de oportunidad para impulsar criterios de política pública y espacios de atención gubernamental e interacción social para el fortalecimiento de los valores nacionales.

Dentro de una visión general, el segmento poblacional por grupos etarios resulta relevante en la conceptualización de una cibersociedad, al registrarse una brecha tecnológica entre las personas de la tercera edad, madurez, juventud e infancia.

2 C. a. J. N. Bronk, «Cyber Cases: The PICCA Framework for Documenting Geopolitical Relevant Cyber Action,» vol. 16, nº 1, 2023.

3 INEGI, IFT y SCT, «Gobierno de México,» 22 06 2021. [En línea]. Available: https://www.gob.mx/cms/uploads/attachment/file/647466/ENDUTIH_2020_co.pdf. [Último acceso: 29 09 2023].

4 Secretaría de Relaciones Exteriores, «Instituto de los Mexicanos en el Exterior,» [En línea]. [Último acceso: 29 09 2023].

Respecto a estos cuatro grandes segmentos, la interacción tecnológica constituye una actividad importante para la tercera edad, ya que 84% usa su tiempo en "hablar por teléfono/enviar mensajes/usar internet" de acuerdo con la Encuesta Nacional sobre Salud y Envejecimiento en México (ENASEM 2021)[5]. Pese a ello, el acceso a plataformas digitales e interacción en otras aplicaciones puede resultar más complejo y generar una sensación de exclusión, además de dejar en condición vulnerable de exclusión digital a los adultos mayores, lo cual se acentúa en comunidades marginadas, rurales y con menor acceso a recursos tecnológicos.

Con relación a la población adulta, joven e infantil, se identifica el surgimiento de comunidades virtuales con altos niveles de segmentación, con capacidad de poner en riesgo la seguridad nacional, como ocurrió con filtraciones en el Departamento de Defensa de Estados Unidos, que sorpresivamente vio que varios de sus documentos clasificados habían sido expuestos por un miembro de la Guardia Nacional, quien habría sustraído el material y compartido su contenido en una comunidad virtual de la plataforma *Discord* con integrantes de un grupo de videojuegos[6].

Este aislamiento y sobre exposición pueden ser predictores de una multicibersociedad con localización nacional o internacional, basada en comunidades virtuales que se crean y recrean a partir de sí mismas y los intereses en común que las unen, generando colectivos con una muy alta capacidad de comunicación y esquemas medios de movilización sobre causas específicas.

En este contexto, las distintas plataformas virtuales compiten por la atención de los usuarios presentes y potenciales, con la finalidad de atraer más adeptos en base a la utilidad, funcionalidad, nivel de entretenimiento y satisfacción de quienes las usan, siendo la principal característica la posibilidad que se da a las personas de ser protagonistas de sus historias, compartirlas y monetizarlas, generando nuevos esquemas de enseñanza-aprendizaje, comercialización y competencia, que en ocasiones puede estar basada en abusos, que de no ser porque tienen como vector plataformas virtuales tendrían severas sanciones legales.

Ante esta situación las empresas dedicadas a la producción tecnológica se mantienen en constante evolución para desarrollar y mantener la atención de los usuarios para la producción, difusión y consumo de contenidos en las distintas plataformas, con algunos casos asociados a contenidos adictivos, siendo el más sobresaliente *TikTok*, cuyo uso durante 2023 fue prohibido en dispositivos propiedad del gobierno de Estados Unidos, Unión Europea, Canadá y Bélgica[7].

5 INEGI, «INEGI,» [En línea]. Available: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/ENASEM/ENASEM_21.pdf. [Último acceso: 30 09 2023].

6 CNN en Español,» CNN, 14 4 2023. [En línea]. Available: https://cnnespanol.cnn.com/2023/04/14/lo-que-sabemos-jack-teixeira-filtrador-documentos-clasificados-del-pentagono-trax/. [Último acceso: 30 9 2023].

7 "Debate", 13- 3-2023. [En línea]. Available: https://www.debate.com.mx/tecnologia/TikTok-En-cuales-paises-esta-prohibida-la-red-social-china-20230313-0263.html.

Así, la nueva relación entre grupos sociales y plataformas digitales plantea un desafío para el Estado-Nación, no sólo por la construcción de nuevas relaciones sociales, también por modelos de comunicación emergente de alto dinamismo que tienen la capacidad de generar reacciones masivas en lapsos de tiempo muy breves, basándose en contenidos imprecisos, tergiversados o deliberadamente maquillados para confundir, engañar y manipular a amplios segmentos sociales, construyendo cadenas de difusión altamente virales que explotan coyunturas específicas y apelan a la emocionalidad de las personas para detonar reacciones, ya sea inmediatas o de largo plazo que buscan una alta incidencia en el comportamiento y elecciones de cada uno de los grupos sociales estructurados en micro objetivos para ejercer influencia.

La explotación de coyunturas mencionada también visualiza en la identidad un campo para la generación de desinformación, que puede incidir en la fragmentación y división social basada en un esquema de desinformación activo. "Desestabilizar la confianza dentro de la población se logra al focalizar el miedo de que ciertos valores serán erosionados, incrementando la desconfianza que la voluntad del gobierno o poder, aseguren los valores de la población —principalmente los del grupo dominante— estén protegidos"[8].

Bajo este contexto el concepto de cultura se redefine también y virtualiza de una manera no vista anteriormente con procesos de comunicación basados en nuevas actividades que informan y entretienen mediante plataformas como *YouTube* y *TikTok*, haciendo de esto opciones de ocupación, dando a segmentos jóvenes de población vertientes de desarrollo al asumirse como youtuberos o tiktokeros, que implican la producción de contenidos de temáticas variadas que buscan el mayor número de seguidores posibles para estar en condiciones de generar ganancias económicas pagadas por las propias plataformas.

En la generación de estos contenidos se identifica una nueva tendencia que se orienta hacia la realización de retos o actividades poco convencionales con elevado nivel de riesgo que podrían atraer simpatizantes y buscan viralizarse, con el objetivo de que el mayor número de personas replique las autoridades que se presentan en los videos mediante las plataformas, llegando en algunos casos a provocar lesiones autoinfligidas o severos daños a la salud, al carecer de medidas de protección y seguridad.

En el espectro privado también la dinámica cultural se modifica mediante la construcción de relaciones virtuales que van desde lo personal hasta lo profesional, generando nuevos espacios de interacción en los que las reacciones y restricciones de privacidad pueden diluirse en el ciberespacio y dar lugar a sanciones en la vida real, como ocurrió en Japón en donde tras un divorcio virtual unilateral, la mujer afectada decidió asesinar el avatar de su excónyuge. Para hacerlo, accedió a su cuenta y lo eliminó, lo

8 G. y J. O. Hoogensen, «Hybrid CoE,» 09 11 2023. [En línea]. Available: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-34-identity-as-a-tool-for-disinformation-exploiting-social-divisions-in-modern-societies/. [Último acceso: 11 11 2023].

cual derivó en el arresto de la mujer por violación a la privacidad del usuario[9].

En una perspectiva más actual, y con el apoyo de plataformas de inteligencia artificial, actos de acoso y violación a la privacidad son también expresiones potenciales que corren el velo de la interacción de nuevas relaciones sociales, basadas en el espacio virtual, pero con repercusiones directas en el mundo real, tanto en lo individual como en lo colectivo, por lo que se requiere considerar esquemas de normatividad y ordenamiento, además de la construcción de mecanismos de orientación hacia una cultura digital saludable para todos los usuarios.

Como área de oportunidad se advierte la posibilidad de construir un laboratorio social virtual alimentado con referencias del comportamiento social colectivo a lo largo de la historia, con esquemas de interacción en vivo con distintos segmentos de internautas para visualizar potenciales conflictos y trabajar en mecanismos de distensión en el campo social, que podría permear también en el ámbito político, que en su dimensión virtual muestra grandes desafíos.

Campo político

Al igual que la conceptualización tradicional del Estado-Nación y el espectro social registran importantes variaciones en el espectro cibernético, la arena política muestra importantes cambios, retos, oportunidades y usos para el desarrollo y transformación de las relaciones de poder en la escala global.

Quizá el principal cambio obedezca a la profunda transformación del campo social, que presenta oportunidades diversas y novedosas para establecer canales de comunicación entre las expresiones políticas y los intereses sociales, así como plataformas para la proyección de soluciones y captación de partidarios.

Desde esta perspectiva se aprecia una dinámica mixta, en la que convergen mecanismos tradicionales de interacción política partidista, empleada principalmente en América Latina, Asia y África, basados en propaganda física, organización de grupos de votantes, promoción de candidaturas y vinculación directa con programas de gobierno.

De manera paralela converge también un esquema de comunicación basado en plataformas digitales, redes sociales y dispositivos electrónicos que establecen vínculos con los electores y virtualizan la interacción con mecanismos que frecuentemente pueden pasar desapercibidos por los ciudadanos, y que pareciera ser una de las nuevas tendencias hacia donde se orientarán los temas político-electorales. En este contexto, la adquisición, mantenimiento y explotación de metadatos de las distintas actividades sociales en interacción con dispositivos digitales y/o espacios virtuales, representan una fuente de valor para el desarrollo de predicciones asociadas al comportamiento, creencias y acciones de potenciales votantes, o consumidores, dependiendo del enfoque, y podrían ser una oportunidad para detectar áreas de oportunidad para políticas públicas asistidas con inteligencia artificial.

Dentro de los retos más evidentes en la arena política destaca la automatización

9 The Guardian, «The Guardian,» 24 10 2008. [En línea]. Available: https://www.theguardian.com/world/2008/oct/24/japan-games. [Último acceso: 14 10 2023].

de la persuasión electoral y narrativas ideológicas que, mediante la identificación de preferencias de los ciudadanos (incluidos los virtuales) a un nivel de segmentación muy detallado, así como el patrón de sesgos, puede inducir a votantes indecisos o ciudadanos pacíficos en fervientes defensores de causas ideológicas con las que sólo los uniría un detallado esquema de manipulación macro basado en una narrativa polarizante y discursos de odio simplificados que encuentran en la oposición un blanco perfecto para señalar y enfocar la atención y sentimientos negativos.

Si bien estas técnicas de propaganda y manipulación no son nuevas, la masificación, virtualización y generación de metadatos sí, permitiendo que en cuestión de horas se puedan moldear opiniones, generar reacciones y detonar acciones altamente emocionales para el apoyo de objetivos políticos, aun cuando estos sean de tipo ilegal al tener como base la alteración de normas legales y preceptos constitucionales, como es posible observar en distintos puntos del orbe.

En México es posible ver como la propaganda gubernamental es aprovechada por organizaciones criminales mediante la generación y difusión masiva en plataformas digitales, de manera que el eslogan "Abrazos no balazos" es propaganda diseñada para convencer a la población, asediada por la violencia, que hay un nuevo y mejor mecanismo para enfrentar a las OTD (Organizaciones de Tráfico de Drogas). Esta nueva aproximación, que pareciera cubrir con bondad y comprensión la acción y violencia criminal, ha sido aprovechado por grupos como el Cártel de Jalisco Nueva Generación (CJNG), que "entiende la importancia de la propaganda, y la ha usado para empuñarla como un arma para lastimar la imagen del gobierno, exponiendo la nueva estrategia de pacificación del gobierno como propaganda"[10].

Dentro del espectro de manipulación, la desinformación y generación de noticias falsas resultan un componente fundamental, tanto para la construcción de mentalidades tendientes a la credulidad de teorías o hechos no basados en evidencia alguna, como la credulidad a toda prueba hacia actores políticos que pese a pésimos resultados en sus gestiones administrativas mantienen su popularidad y detonan emociones y seguimientos encontrados en sus partidarios y/o detractores, construyendo un capital político basado en la virtualización y encauzamiento de la opinión pública hacia interpretaciones diversas sobre temas puntuales, aun cuando sean opuestas o ajenas al gobierno o arena política.

En este contexto la ciberpolítica cuenta con herramientas que permiten mitigar los riesgos de desinformación y narrativas dañinas promovidas por actores hostiles que pueden ubicarse tanto al interior de las fronteras geográficas de un Estado-Nación, o desde el exterior, ya sea por actores locales o internacionales con una lógica geopolítica de influencia o económica, que enmarcaba a ambas, como ocurrió con el caso Cambridge Analytica, que ofrecía el análisis de datos para desarrollar campañas para marcas y políticos que buscan "cambiar el comporta-

10 D. Weisz, «El Centro Small Wars Journal,» 22 04 2021. [En línea]. Available: https://smallwarsjournal.com/index.php/jrnl/art/propaganda-war-cjng-and-amlo.

miento de la audiencia"[11], y lo lograron con la influencia en la votación de la población británica. En el Brexit, y en la elección estadounidense del 2016, que intentó repetirse en el 2020, dando pie a una campaña de desinformación que puso a prueba el sistema democrático y legal de los Estados Unidos.

Esta interacción entre la política de orden nacional e internacional mediante el espacio cibernético ha permitido el surgimiento de conceptos como la ciberdiplomacia, registrada por primera vez en 2011, durante la administración en Estados Unidos de Barak Obama, con el documento Estrategia Internacional para el Ciberespacio, que fue considerado "el primer documento de gobierno en el mundo enfocado enteramente en aspectos internacionales de temas cibernéticos"[12].

Bajo conceptualizaciones más elaboradas en la década siguiente, la ciberdiplomacia ha evolucionado a un espectro ampliado, como lo muestra la Ley de Ciber Diplomacia estadounidense 2021, que retoma las definiciones para "trabajar internacionalmente en la promoción de infraestructura de información y telecomunicaciones abierta, interoperable y segura que apoye el comercio internacional, fortalezca la seguridad internacional y promueva la libre expresión e innovación"[13].

En contra posición, en este mismo documento se identifican esfuerzos de otros países que podrían tender hacia la "represión digital", mediante la limitación en la producción, difusión y consumo de contenidos que podrían atentar contra intereses de camarillas de poder o aparatos políticos de corte dictatorial.

En este sentido la misma Ley de Ciber Diplomacia cita en sus antecedentes que "en enero 2015, China, Kazajistán, Kirguistán, Rusia, Tayikistán y Uzbekistán propusieron un preocupante código internacional de conducta para la seguridad de la información, que podría utilizarse como pretexto para restringir la disidencia política, e incluye "frenar la difusión de información que incite al terrorismo, el separatismo o el extremismo o que se promueva el odio por motivos raciales, étnicos o religiosos"[14].

Como puede apreciarse en la esfera cibernética se dirimen también enfoques opuestos sobre el uso y finalidad de este espacio, con visiones opuestas que han dado pie a campañas abiertas de desinformación basadas en los cambios sociales ya comentados, con agendas políticas definidas a nivel nacional y encubiertas en el plano internacional, con campañas de desinformación, confusión y contrainformación, que, además de objetivos propagandísticos, buscan la captación de adeptos y detonación de acciones radicales, que pueden ser prevenidas por el "monitoreo de sentimientos con distintas aplicaciones, como pueden ser: proteger a los ciudadanos de campañas de desinformación;

11 BBC Mundo, «BBC News Mundo,» 20 3 2018. [En línea]. Available: https://www.bbc.com/mundo/noticias-43472797. [Último acceso: 15 10 2023].

12 C. Monahan, ¿Un Dominio Diplomático? La Evolución de la Diplomacia en el Ciberespacio, Washington, D.C., 2021.

13 Senate of the United States, «United State Congress,» 22 04 2021. [En línea]. Available: https://www.congress.gov/bill/117th-congress/house-bill/1251/text?s=1&r=62. [Último acceso: 17 10 2023].

14 Logically, «Logically Intelligence,» [En línea]. Available: https://www.logically.ai/logically-intelligence. [Último acceso: 17 10 2023].

identificar y responder a campañas hostiles de estados nacionales; inhibir actividades ilegales en línea; salvaguardar procesos democráticos de campañas de desinformación e influencia negativa; proteger a personas, marcas y activos de amenazas de desinformación", entre otros.

Ante este ambiente y expresiones de la ciberpolítica doméstica e internacional, cabe considerar la situación como una etapa que trasciende el fin de la historia hacia un escenario de reescritura en base a narrativas alternas promovidas por las minorías y adoptadas por las mayorías con elementes altamente emocionales que lo mismo trascienden en el ámbito de la política nacional que internacional, presentando un desafío permanente para que las distintas expresiones tengan garantizados sus derechos sin alterar las condiciones fundamentales que permiten la gobernabilidad y desarrollo democrático.

Campo económico

En esta área las tecnologías y espectro cibernético han tenido quizá el mayor avance, de una manera rápida y silenciosa, que va desde el desarrollo de aplicaciones comerciales, bancarias y financieras para teléfonos inteligentes, hasta el desarrollo de la industria 4.0, que implica una nueva forma de relacionamiento, producción y generación de riqueza a escala global.

De acuerdo con lo que comenta el BID los "nuevos modelos de organización de los negocios surgen de la mano... de nuevas conectividades 5G, de nuevos esquemas de trabajo *freelance*... El remplazo de las tareas rutinarias por máquinas crecientemente analíticas refuerza la necesidad de transformar *soft-skills* en los trabajadores y *managers*"[15].

A esto se suman esquemas de comercialización y mercadotecnia, en donde la "redes sociales se han transformado en un mercado esencial para las compañías modernas. Plataformas en línea como *Instagram*, *Facebook* y *Twitter* permiten a los negocios fácilmente expandir su alcance, comunicarse con su audiencia ideal y construir confianza al postear contenido orgánico. Desafortunadamente, el uso de redes sociales también aumenta los riesgos de ciberseguridad"[16].

De esta manera los modelos de producción tradicional están también viviendo una transformación acelerada, en la que las industrias nacionales parecen cambiar su esencia por consorcios globales que tienen en la tecnología una innovación y motor permanente de desarrollo, en el que tanto el campo, la industria y el sector servicios tienen en la tecnología y espacio cibernético un área con gran potencial de desarrollo, pero que puede implicar también una vulnerabilidad, que es el secuestro, robo o manipulación de sus sistemas informáticos, y por ende de producción, haciendo necesario desarrollar nuevas mentalidades en los Consejos de Administración, Comités Directivos, Directores, Gerentes y personal en general, para reducir las ventanas de vulnerabilidad digital.

15 B. G. C. D. y. G. P. Basco Ana Inés, «Banco Interamericano de Desarrollo,» Banco Interamericano de Desarrollo, Julio 2018. [En línea]. Available: https://publications.iadb.org/es/industria-40-fabricando-el-futuro. [Último acceso: 18 10 2023].

16 Z. Amos, «How Social Media Impacts Business Cybersecurity,» River Publishers, 22 07 2022. [En línea]. Available: https://cybersecurity-magazine.com/how-social-media-impacts-business-cybersecurity/. [Último acceso: 11 11 2023].

Otra de las grandes áreas disruptivas del ciberespacio es el surgimiento de plataformas de servicios que redefinen la relación tradicional cliente-proveedor, reduciendo grados de intermediación, disminuyendo costos, rompiendo monopolios y limitando la participación administrativa de los gobiernos nacionales, como se ha registrado en los casos de *Uber, Didi, Rapi y Airbnb,* por citar los más conocidos.

Si bien con estos modelos de negocios hay modificaciones importantes, también se consideran desafíos importantes por las lagunas de registro y control para la prevención de conductas ilícitas, que pueden aprovechar la amplia oferta de servicios de reparto y transporte para enviar de manera anónima todo tipo de mercancías, o desplazar y alojar personas en espacios lejanos a los controles implementados por las autoridades que pueden ser utilizados para la trata y tráfico de personas, secuestros, extorsiones, narcotráfico y/o actividades terroristas.

Pese a estos riesgos el margen de utilidad y el cambio de reglas hacia la simplificación, han motivado que más personas se conviertan en usuarios o proveedores de estas plataformas, además de desarrollar nuevos esquemas tendientes hacia la virtualización del quehacer económico tradicional, siendo los casos más notables los de la industria del entretenimiento, con el surgimiento de plataformas de video y música en línea, además del auge de los videojuegos y nuevos esquemas para la producción de contenidos de manera sencilla con fines de monetización por parte de los generadores.

Quizá el cambio más importante en el campo económico ha sido el surgimiento de esquemas monetarios virtuales como las cripto monedas, que han generado presión no solo en los sistemas bancarios nacionales, sino también en el sistema bancario internacional, que frente a estos esquemas enfrenta numerosos desafíos, que posiblemente no han avanzado por el escaso conocimiento de los cripto activos y relativa especialización tecnológica para la minería de estos recursos y manejo a nivel internacional.

Otro de los elementos poco visualizados asociados a la minería de cripto activos se encuentra en la elevada necesidad de consumo de energía eléctrica, así como la disponibilidad de computadores de alta capacidad y velocidad para realizar las transacciones de manera competitiva y asegurar los ingresos por el minado de monedas virtuales, cosas que hasta ahora han sido alcanzado por un segmento minoritario.

Pese a estas restricciones, el avance en el uso de criptomonedas ha sido creciente, logrando incluso que algunos países de Latinoamérica consideren interactuar más activamente. En el caso de El Salvador, en 2021 se consideró incluso usar el "*bitcoin*" como moneda de curso legal en el país centroamericano, lo cual para 2022 se había frenado por la contracción en este tipo de cripto activos, lo cual implicó la afectación a las finanzas salvadoreñas[17] y la desaceleración de esta novedosa divisa.

Pese a los altibajos que puede presentar el uso y manejo de un nuevo sistema mone-

17 S. T. Wang Philp, «CNN en español,» CNN, 15 06 2022. [En línea]. Available: https://cnnespanol.cnn.com/2022/06/15/bitcoin-el-salvador-criptomonedas-nayib-bukele-trax/. [Último acceso: 18 10 2023].

tario digital, se han encontrado expresiones y actividades que buscan la transferencia de costos y riesgos a terceros, aprovechando desconocimiento de otras personas, falta de controles o disponibilidad de recursos asignados para las áreas de Tecnología de la Información o Informática dentro de las organizaciones públicas o privadas, como ocurrió en un plantel educativo de San Luis Potosí, en donde se identificó la operación no autorizada de una cripto mina de bitcoin que fue detectada por los altos consumos de energía eléctrica[18], poniendo en alerta a las autoridades cibernéticas de ese estado.

Al igual que todo lo relacionado con la tecnología y ciberespacio, los cambios en el poder económico nacional y sus expresiones seguirán presentando transformaciones sin precedentes y vertiginosas que ameritan una revisión sistemática y permanente para adaptar la capacidad de respuesta de las autoridades nacionales, así como actores de las esferas públicas y privadas en cada país.

Campo militar

Al igual que en los otros tres campos tradicionales del poder nacional registran profundas transformaciones en la interacción con el ciberespacio, el campo militar muestra también profundas transformaciones para la reflexión y el análisis.

Dentro de los cambios asociados al contexto, es recomendable considerar la variación en los enfoques tradicionales de la guerra regular, dando paso al marco de conflictos asimétricos y *Guerra de IV Generación (IVGW),* que da paso al surgimiento de amenazas no convencionales, con surgimiento en un campo no militar, pero con una alta demanda de respuesta por parte de las Fuerzas Armadas.

Así, en el terreno militar el espectro cibernético implica un nuevo dominio de combate, entendiendo en ciberespacio como "un dominio global dentro del ambiente de información consistente en una red interdependiente de infraestructura de tecnologías de la información, redes de telecomunicaciones, sistemas computacionales y procesadores y controladores incluidos"[19].

En este contexto la red de telecomunicaciones satelital es uno de los principales componentes en la interacción de la esfera cibernética y el campo militar, aun cuando las empresas privadas tienen ya participación, como se comentó previamente.

En este sentido el desarrollo de redes satelitales promovidas, controladas y administradas por los Estados-Nación tiene un componente estratégico, siendo hasta ahora notorio el avance de Estados Unidos con el *GPS*; la Unión Europeo con *Galileo* y Rusia con *Glonass*, que han buscado ampliar la cobertura y precisión para asegurar la transmisión y conectividad a escala global del ciber espacio.

Complementariamente a la conectividad, el uso de herramientas para la penetración de sistemas, control, robo y secuestro de información de tipo militar es también una de las actividades que más presión genera en el campo militar, particularmente cuando se asocia a la operación de

18 M. J. Castañeda, «La mina de criptomonedas que operó por más de un año en un colegio estatal en México,» El País, 2022.

19 United States Cybercomand, «U.S. Military Cyberspace Operations,» Washington, D.C., 2023.

instalaciones estratégicas, como ocurrió en Estado Unidos con los ductos *Colonial,* o a la fuga y filtración de información sensible, como los casos del ejército mexicano y estadounidense, conocidos como *Guacamaya Leaks y Teixeira*, respectivamente, en los que se puso a disposición de la opinión pública datos reservados propios de la operación de estas organizaciones militares.

Otro de los elementos centrales del campo de ciber poder militar está asociado con la generación de narrativas falsas para generar ambientes hostiles en los teatros de operación, en los que se construyen ideas distorsionadas sobre las acciones, propósitos y víctimas de conflictos en los que intervienen las Fuerzas Armadas, buscando apelar a la emocionalidad de los receptores, con direccionamiento a población abierta o a los propios miembros del campo militar, sembrando desconfianza, divisiones y tensión entre tropa y mandos, haciendo necesario establecer mecanismos de monitoreo y canales de comunicación para combatir estar expresiones y reducir los niveles de entropía inducida.

En el campo de las operaciones, el uso de Vehículos Aéreos no Tripulados (VANT) es quizá el campo más notorio, que en el conflicto generado por la invasión Rusia a Ucrania ha mostrado un potencial ofensivo importante, así como para tareas de reconocimiento. Con menos visibilidad, pero igualmente útiles, los vehículos submarinos y terrestres no tripulados también muestran una gran oportunidad para ser tripulados a distancia y recabar datos de inteligencia, ubicar potenciales minas y apoyar en la guía de vehículos motorizados con tripulación humana.

Esta modalidad de vehículos no tripulados ha demostrado un mayor potencial de daño al contar con armas autónomas que, apoyadas con inteligencia artificial, cuentan con capacidad de analizar la situación, determinar un potencial blanco hostil y abrir fuego, aun cuando los niveles de precisión pueden ser cuestionables, lo mismo que la determinación del nivel de hostilidad para autorizar una reacción de fuerza, normalmente letal.

Otro de los elementos centrales del campo de ciber poder militar está asociado con la generación de narrativas falsas para generar ambientes hostiles en los teatros de operación, en los que se construyen ideas distorsionadas sobre las acciones, propósitos y víctimas de conflictos en los que intervienen las Fuerzas Armadas, buscando apelar a la emocionalidad de los receptores, con direccionamiento a población abierta o a los propios miembros del campo militar, sembrando desconfianza, divisiones y tensión entre tropa y mandos, haciendo necesario establecer mecanismos de monitoreo y canales de comunicación para combatir estar expresiones y reducir los niveles de entropía inducida.

En el campo de las operaciones, el uso de Vehículos Aéreos no Tripulados (VANT) es quizá el campo más notorio, que en el conflicto generado por la invasión Rusia a Ucrania ha mostrado un potencial ofensivo importante, así como para tareas de reconocimiento. Con menos visibilidad, pero igualmente útiles, los vehículos submarinos y terrestres no tripulados también muestran una gran oportunidad para ser tripulados a distancia y recabar datos de inteligencia, ubicar potenciales minas

y apoyar en la guía de vehículos motorizados con tripulación humana.

Como un riesgo emergente dentro del campo militar, el surgimiento de células armadas con distintas orientaciones ideológicas, políticas y/o religiosas que buscan disputar el *monopolio legítimo de la violencia* al Estado, así como de la información con esquemas de control territorial, tributación alterna y normatividad paralela a la establecida por el Estado-Nación, cuenta también con el acceso a una amplia gama de herramientas tecnológicas, muchas de ellas accesibles de manera comercial, que ameritan el desarrollo de capacidades de inteligencia por parte de las autoridades para limitar el acceso y producción de armas, así como retomar el control y restringir el acceso a recursos para financiar este tipo de expresiones.

La disponibilidad y evolución tecnológica de estos dispositivos muestra las tendencias en las que se desarrollaría el campo de poder militar en las próximas décadas, y amerita ser analizado por los gobiernos nacionales en todas sus expresiones, tanto para encauzar normativamente el uso, como para desarrollar capacidades preventivas para proteger a los ciudadanos.

Bajo este contexto cabe reflexionar si se está ante una *Guerra Fría 2.0 o* una *Ciberguerra fría* que va de la mano de la competencia tecnológica, conformación de bloques y alianzas regionales, cada vez más cerca por la virtualización de espacios de comunicación y representación tradicionales, en los que el dominio del espectro de telecomunicación, información, meta datos, inteligencia artificial y desarrollo tecnológico serán centrales para definir, en la tercer década del siglo XXI, lo que será hacia el próximo siglo.

Conclusiones

Conceptualizar la ciberseguridad nacional pude implicar resistencias cognitivas por su asociación con el futuro, desarrollo tecnológicos e incertidumbre que normalmente se presentan de manera gradual e independiente, por lo que articularlos bajo una visión de Estado-Nación implica replantear un nuevo paradigma y visualizar retos emergentes.

Una de las características que se identifica en la conceptualización de ciberseguridad, es una mayor transversalidad entre las expresiones del poder nacional, en un esquema tendiente a re balancear las capacidades nacionales y el contexto internacional en función de su adaptación al ámbito cibernético y virtualización de expresiones culturales de distinta naturaleza, con capacidad de expresión inmediata una vez las resistencias ideológicas y cognitivas han sido modificadas.

En este nuevo contexto resulta evidente el cambio de los centros de gravedad en cada uno de los campos de poder tradicionales, otorgando parte de sus activos hacia lo que puede considerarse "el imperio de los datos y la información", que manejada mediante algoritmos y en grandes volúmenes puede generar patrones predictivos e inducir comportamientos mediante la activación o contención de sesgos en individuos y/o comunidades.

Frente a este escenario, el derecho de los ciudadanos a la privacidad, ejercicio libre e informado de las decisiones personales serán

una de las tareas de todos los componentes del Estado-Nacional para asegurar un marco de protección amplio y suficiente que garantice el ejercicio de este derecho, frente al asedio de grupos, individuos e ideologías que se plantean nuevos esquemas de poder bajo esquemas potencialmente dictatoriales mediante la manipulación asistida por medios virtuales y plataformas digitales.

Sin duda ciudadanos, academia, empresas y gobiernos a escala global deberemos sumar esfuerzos para garantizar que los aspectos positivos del desarrollo tecnológico y cibernético prevalezcan y permitan fortalecer las capacidades, para cerrar el paso a expresiones negativas que abusen del espacio cibernético para fines no democráticos.