La guerra cognitiva en el ciberespacio

Por Micaela Soledad Constantini. Encuentro Patriótico. Argentina
mica.constantini@gmail.com

Frente al actual nuevo orden internacional multipolar, el ciberespacio se ha convertido en uno de los principales territorios geopolíticos de disputa.

En este sentido, el ciberespacio se ha convertido en un territorio que puede funcionar como campo de batalla, como herramienta y como medio. Esto significa, que como campo de batalla, en el ciberespacio se puede atacar y ser atacado con la posibilidad de destrucción de infraestructura tanto digital y virtual como material tangible, así el ciberespacio ha sido militarizado, transformado en escenario de ciberguerras, sabotajes, ataques a infraestructuras críticas, hackeos y operaciones encubiertas. Como herramienta, posee características únicas que le permite introducirse de forma silenciosa e imperceptible en espacios donde antes era mucho más difícil o imposible, sin ser reconocidos, como en las formas de vigilancia y espionaje o incluso a simple vista como la recolección de datos, así el ciberespacio se convierte en un instrumento sutil pero penetrante de gobernanza algorítmica y acumulación de poder. Como medio, a través de las plataformas digitales, los algoritmos, las redes sociales y los medios online el ciberespacio permite moldear percepciones, construir consensos, operar psicológicamente sobre mayorías sociales y construir hegemonía cultural, así el ciberespacio permite la penetración ideológica, cultural y simbólica en los demás territorios.

Sin embargo, aunque presentamos al ciberespacio como un nuevo territorio geopolítico, las tácticas, las estratégias y los objetivos no son nuevos. La construcción de un enemigo; la ‘ayuda humanitaria’; el apoyo a las oposiciones y élites locales; el financiamiento y utilización de grupos militares o paramilitares; la deslegitimación; anular el apoyo popular; las operaciones psicológicas; atacar la identidad político-cultural; el desgaste diplomático; las ofensivas mediáticas; la construcción de opinión pública; la utilización de medidas económicas, políticas, informacionales y humanitarias para potenciar las protestas entre la población; la utilización de mercenarios; el caos administrado; el lawfare utilizando el poder judicial, inhabilitando políticamente y destruyendo la imágen pública de una persona en específico; la desestabilización y debilitamiento de las instituciones, el fogoneo a manifestaciones violentas o revueltas, forman parte de los modos que fue adoptando el guerrerismo imperialista.

Cada uno de estos elementos se perfeccionaron y potenciaron a partir de las nuevas tecnologías utilizando el ciberespacio para influir en el pensamiento y acciones de las personas -de los ‘objetivos’- para lograr un determinado fin o diversos fines. En este punto, el ciberespacio es tanto el medio, la herramienta como el campo de batalla, el big data el principal instrumento, el monopolio una necesidad, el trabajo interdisciplinario una gran ventaja y el principal objetivo es someter territorios y pueblos sin necesidad de recurrir al

poder militar ni uso de la fuerza o, en todo caso, preparar la opinión pública (tanto local como global) para justificar la intervención a la fuerza.

Algunos de los ejemplos que podemos mencionar como antecedentes son las protestas en la región árabe, Túnez, Argelia, Jordania, Egipto y Yemen, lo que se conoció como Primaveras Árabes (2010-2012); también se pueden observar, en el mismo período, patrones similares en protestas en Europa central y en el Este (2012-2014); características semejantes y contemporáneas se observaron en América Latina, como en Brasil o Venezuela; especialmente en el llamado 'Euromaidán' en Ucrania.

En 2015, el analista geopolítico, Andrew Korybko comenzó a conceptualizar estas nuevas formas del guerrerismo imperialista como "guerras híbridas" explicando que a partir de la combinación de las revoluciones de colores y la guerra no convencional se desarrolla una nueva teoría de desestabilización de los Estados.

El analista explica que las movilizaciones y protestas organizadas para desestabilizar un gobierno, no requieren de la mayoría de la población, pero que depende de la particularidad de cada país, su liderazgo, la fuerza del gobierno y su aparato de seguridad. Utilizan principalmente técnicas ideológicas, psicológicas y de información, para lograr que esa población sea usada de forma caótica contra las autoridades. Por lo que "el núcleo de las revoluciones de colores se sintetiza en la dominación social", es decir ganar el "control sobre aspectos intangibles, tales como sociedad, ideología, psicología e información".

La guerra no convencional, por su parte, "aspira a la dominación sobre aspectos tangibles del campo de batalla, pero no de la misma manera que la guerra convencional". Es decir, no se realiza una intervención directa por parte de un Estado externo, sino que busca "conquistar el máximo dominio físico posible dentro de los cinco anillos originales del Estado objetivo", especialmente la población, la infraestructura y las bases del sistema; atacar los otros dos anillos, las fuerzas armadas y el liderazgo, dice el analista, puede volverse en contra.

La combinación de ambas estrategias, las revoluciones de colores y la guerra no convencional contienen un caos inherente que "se extiende por todo el "sistema" enemigo tal como un "virus" hace en un ordenador, como dice la lógica de Mann, con la eventual esperanza de que resultará en su total deterioro y en la necesidad de iniciar un "reboot del sistema" (cambio de régimen) para eliminar la amenaza" (Korybko, 2015).

En 2011, el Comité de Relaciones Exteriores del Senado estadounidense advirtió que los ejemplos de lo sucedido "a través de la ola de manifestaciones que se produjeron en el mundo árabe que comenzó en diciembre de 2010, conocida como la Primavera Árabe, el mundo fue testigo de cómo los ciudadanos pueden utilizar los medios sociales y plataformas de información como Facebook, Twitter y Google para movilizarse contra los gobiernos represivos", y por dicho motivo recomendaba un informe titulado "Los gobiernos de América Latina necesitan ser 'amigos' de los medios sociales y la tecnología".

Korybko (2015) explica que “el objetivo es crear una mente de enjambre de incontables individuos que se dedican en la cruzada contra el gobierno y se convierten en una sola mente”, logrando ‘el caos orquestado’, “contra las cuales es extremadamente difícil para las autoridades prepararse y repelerlas”.

No encontramos atravesando un contexto histórico donde se está desarrollando una nueva forma de guerrerismo imperial optimizada que apunta a la cognición, a la psique individual y colectiva, no sólo centrándose en qué y cómo piensan las poblaciones, sino también queriendo hacerse del control sobre cómo actúan, ser quienes guíen las acciones individuales y colectivas.

Los think thank de la OTAN ubicados en Estados Unidos, definen la “cognición” como “la base del comportamiento humano. Es el centro de gravedad; y es un objetivo bajo ataques permanentes”.

“La mejor manera de hacer que las personas se comporten de la manera que desea, sin coerción, es moldear cómo entienden su entorno y luego tomar decisiones. ¡La mejor manera es moldear su cognición!”, se describe desde el principal espacio de debate de expertos de la OTAN.

Allí investigan sobre Inteligencia Artificial, toma de decisiones, pensamiento crítico, neurociencias, realidad virtual, guerra cognitiva, lo cibernético, tecnología y guerra de la información, biotecnología, redes sociales y social media, ciencias sociales, ingeniería de sistemas, la genética, los complementos neuronales en forma de nanotecnología, las interfaces neuronales, la inteligencia humana; todo ello relacionado con la seguridad nacional, la guerra y los conflictos mundiales.

Afirman que “la Guerra de la Información y la Guerra Cognitiva se convertirán probablemente en cursos de acción permanentes para obtener el estado final deseado, que es la desestabilización de un líder político, una fuerza enemiga, un país o incluso una Alianza”.

A diferencia de la guerra informativa, que intenta controlar lo que la población objetivo ve, la guerra psicológica, que controla lo que la población objetivo siente, y la guerra cibernética, que intenta perturbar las capacidades tecnológicas de las naciones objetivo, la guerra cognitiva se centra en controlar cómo piensa y reacciona la población objetivo, explican los expertos de la OTAN. Así, “el cerebro humano se convierte en el teatro de operación”.

“La guerra cognitiva es un enfoque de armas combinadas que integra las capacidades bélicas no cinéticas de la ingeniería cibernética, informativa, psicológica y social con el fin de ganar sin combatir físicamente. Es un nuevo tipo de guerra que se define como el armamento de la opinión pública por parte de entidades externas. Se lleva a cabo con el propósito de influir y/o desestabilizar una nación. Estos ataques pueden visualizarse como una matriz: que abarca a unos pocos y a muchos; que influye en el pensamiento y en la acción; que tiene como objetivo desde toda la población hasta medidas individuales; a través de comunidades y/o

organizaciones. Los ataques buscan cambiar o reforzar los pensamientos, influyendo/confirmando la forma de pensar de la gente para afectar a la acción en el mundo real. La forma en que se lleva a cabo difiere de los dominios más tradicionales de la guerra", explica el informe de los expertos de la OTAN.

El científico cognitivo francés, Bernard Claverie, y el teniente coronel retirado del ejército francés y jefe de los proyectos de los expertos de la OTAN, François du Cluzel, afirman que el objetivo es "nuestra inteligencia, tanto a nivel individual como colectivo", que se "opera en un escenario global, ya que la humanidad en su conjunto está ahora conectada digitalmente" y que "utiliza la tecnología de la información y las herramientas, máquinas, redes y sistemas que la acompañan".

Claverie y du Cluzel explican que la guerra cognitiva utiliza las herramientas cibernéticas para "alterar los procesos cognitivos del enemigo, explotar los sesgos mentales o el pensamiento reflexivo, y provocar distorsiones del pensamiento, influir en la toma de decisiones y obstaculizar las acciones, con efectos negativos, tanto a nivel individual como colectivo", por lo que la guerra cognitiva va más allá de la información o de las consecuencias de la ciberguerra (ingeniería informática, robótica y programas), el "efecto cognitivo no es un subproducto de la acción, sino su propio objetivo".

Estos autores afirman que no se trata de complementar "a la estrategia o derrotar a un enemigo sin lucha", sino de librar una guerra en sí, "contra lo que una comunidad enemiga piensa, ama o cree, alterando las percepciones", que une dos campos operativos que antes se trataban por separado "las PSYOPS y las operaciones de influencia (soft power), por un lado, y las ciberoperaciones (ciberdefensa) destinadas a degradar o destruir los activos físicos de información, por otro".

Para ello, explican Claverie y du Cluzel, "la dimensión cognitiva se basa en el conocimiento de la psicología de los actores implicados, de la psicosociología de poblaciones o grupos específicos y de la influencia de la cultura en la toma de decisiones y la racionalidad de los distintos actores".

De esta manera, el big data será el instrumento principal, ya que a partir de la generación de datos en bruto, el almacenamiento masivo y eficiente de datos, la computación en la "nube", el procesamiento eficaz de datos, el análisis efectivo de información y el aprendizaje automático, se puede establecer cuatro dimensiones de análisis de los datos:

- el análisis descriptivo: lo que está ocurriendo;
- el análisis diagnóstico: describe o explica por qué está pasando;
- el análisis predictivo: anticipa un probable resultado;
- y el análisis preceptivo: puntualiza cómo hacer que algo ocurra.

Así, se comenzó a analizar, a partir de ciertos criterios determinados, la psique y la conducta de una persona individual y en colectivo. Esta práctica se denominó psicometría.

La psicometría mide los rasgos psicológicos como las emociones, las actitudes, la personalidad, las habilidades cognitivas a través de datos cuantificables obtenidos del big data, que ofrece miles de millones de microdatos del comportamiento digital. De esta manera se utilizan para perfilar psicológicamente a individuos o poblaciones enteras de forma automática, rápida y precisa.

“Big Five” es la técnica estándar de la psicometría. Su finalidad es buscar, cuantificar y operativizar lo psíquico de acuerdo a cinco características (OCEAN, por sus siglas en inglés) de las personalidades que responde a:

1.- Disposición y apertura a la experiencia: ¿Qué tan dispuesto está el individuo a nuevas experiencias?
2.- Consciencia y responsabilidad: ¿Qué tan perfeccionista es el individuo?
3.- Extraversión y sociabilidad: ¿Qué tan sociable es el individuo?
4.- Amabilidad y empatía: ¿Qué tan considerado y cooperativo es el individuo?
5.- Neuroticismo y tendencia a emociones negativas: ¿Qué tan fácil de enfadar es el individuo?

El ciberespacio como medio, herramienta y campo de batalla facilita tanto la recolección de datos, el análisis y estudio del comportamiento humano, las operaciones de influencia y el alcance global de las mismas.

Aunque el interés por influenciar a los ciudadanos no es nuevo en las estrategias para los actores de poder, la posibilidad de acceder a un plano de sugestión tan profundo como el que permite el big data, llegar a la psique, resalta su valor estratégico.

Frente a este escenario, América Latina debe prepararse para el desafío actual de guerra cognitiva. La urgencia es evidente, la construcción de cibersoberanía se vuelve una tarea impostergable. La guerra cognitiva demuestra que ya no basta con resguardar territorios físicos, hoy el verdadero campo de disputa es la psique individual y colectiva de nuestros pueblos. En un mundo multipolar, donde las grandes potencias concentran las capacidades tecnológicas y de manipulación algorítmica, desde América Latina como parte del Sur Global necesitamos avanzar hacia un bloque regional de integración que construya cibersoberanía, capaz de defender nuestros intereses comunes, fortalecer nuestras infraestructuras críticas y garantizar que nuestras poblaciones no queden sometidas a la dependencia tecnológica y cognitiva de las grandes potencias. La construcción de este bloque no es sólo una cuestión de seguridad, sino de dignidad, soberanía y futuro.