Cibergeopolítica y la guerra cognitiva

por Leonid Savin

Internet se ha convertido en parte de la vida diaria para todo el mundo. Ahora, nos conecta no solamente a través de los ordenadores de mesa, sino también a través de dispositivos móviles, redes Wi-Fi en áreas públicas, y otros numerosos programas y aplicaciones (desde las redes sociales a los archivos fotográficos). La gente usa las redes para comprar bienes y servicios, realizan transferencias bancarias, se dirigen a las autoridades, y satisfacen otras necesidades esenciales. Además de ser un medio de comunicación, Internet también es una poderosa arma política que podría usarse tanto para hacer el bien como para hacer el mal.

En tiempos recientes, escuchamos noticias sobre el papel creciente del ciberespacio como herramienta política o dominio, donde la confrontación tiene lugar entre varias organizaciones políticas, países, e incluso alianzas de Estados. El caso de Edward Snowden es indicativo de la manera en que se ha vuelto importante la comunicación por internet y la interdependencia del entorno social con la política, la economía y el sector militar, y que afecta tanto a la agenda actual como a la planificación estratégica de los líderes de las mayores potencias mundiales.

Para la ciencia política tradicional y la geopolítica clásica, estos procesos son complejos y a menudo son un fenómeno muy poco intuitivo. El problema es que algunos de los temas relacionados con el ciberespacio son la herencia de expertos altamente especializados. Una comprensión adecuada de ellos requiere una aproximación multidisciplinaria, ya que los juristas no serían capaces de entender el ciberespacio al detalle sin la ayuda de ingenieros y programadores, mientras que los creadores de políticas públicas, no solamente deberían entender los intereses de los consumidores en las nuevas oportunidades, sino también los aspectos técnicos y económicos del ciberespacio. Por tanto, es necesario poner atención no solamente a los aspectos políticos y económicos, sino también analizar los niveles ideológico, social, y militar, esto es, algunos elementos de la estructura geopolítica de cualquier Estado o alianza.

Como en todo proyecto o teoría política hay un fondo de conceptos filosóficos, y en el caso de Internet hay una serie de ideas que han influido en la creación y desarrollo de la red.[1]

El investigador holandés, Paul Treanor[2], cree que el modelo de red central tiene su origen en el liberalismo clásico. De alguna manera, es un libre-mercado electrónico. La aparición de una ideología particular, el "Net-ism" ["red-ismo"], está basado en una promoción agresiva de la presión política ("lobbying") y de Internet. A tales lobistas, Paul Treanor atribuye la creación de la Electronic Frontier Foundation [Fundación Frontera Electrónica], el grupo de Martin Bangemann que formuló la estrategia de información para el Consejo Europeo[3]. Treanor considera que los trabajos, "El ciberespacio y el sueño americano: Una carta magna para la era del conocimiento" por el futurista Alvin Toffler, y "Pueblo y sociedad en el ciberespacio" por George Keyworth, son los documentos introductorios a la ideología ciber-liberal.

En el artículo "Ciberespacio y sueño americano: Una carta magna para la era del conocimiento", Ester Dyson, George Gilder, George Keyworth y Alvin Toffler dijeron que "*la tercera ola, y la era del conocimiento se ha abierto, y no cumplirá su potencial a menos que añada el dominio social y político a su fuerza tecnológica y económica que se acelera. Esto significa revocar las leyes de la segunda ola y retirar las actitudes de la segunda ola. También da a los líderes de las democracias avanzadas una responsabilidad especial: Facilitar, apresurar, y explicar la transición. Según la humanidad explora esta nueva 'frontera electrónica' de conocimiento, debe confrontarse de nuevo a las preguntas más profundas de cómo organizarse a sí misma para el bien común. El significado de libertad, de las estructuras de auto-gobierno, de la definición de propiedad, de la naturaleza de la competición, de las condiciones para la cooperación, del sentido de comunidad y de la naturaleza del progreso se redefinirán para la era del conocimiento – al igual que fueron redefinidas para una nueva era de la industria hace unos 250 años*".[4]

Al final de su trabajo doctrinal sobre el ciber-liberalismo, Toffler, Keyworth, y sus colegas revelaron el verdadero propósito de sus intenciones. "*Hay temas clave*

---

1 Leonid Savin. Cibergeopolítica: Cuestiones de ideología. 16.06.2018 https://www.geopolitica.ru/es/article/cibergeopolitica-cuestiones-de-ideologia

2 Paul Treanor. Internet as Hyper-liberalism, 1996. http://web.inter.nl.net/users/Paul.Treanor/net.hyperliberal.html

3 Bangemann Report, Europe and the Global Information Society, 1994 http://www.cyber-rights.org/documents/bangemann.htm

4 Esther Dyson, George Gilder, George Keyworth, and Alvin Toffler. Cyberspace and the American Dream: A Magna Carta for the Knowledge Age. Future Insight, Release 1.2, August 1994. http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html

sobre los que esta circunscripción futura puede coincidir. Para empezar, la liberación de las reglas, las regulaciones, los impuestos y las leyes de la segunda ola puestas ahí para servir a los barones y burócratas del pasado. Después, por supuesto, debe llegar la creación, la creación de una nueva civilización fundada en las verdades eternas de la idea estadounidense".

Los ideólogos de esta nueva dirección asociada con el ciberespacio emergente se basan en sus predecesores ideológicos liberales. Citas de ideas libertarias pueden ser encontradas a menudo en sus trabajos, tales como citas de Ayn Rand, y menciones de "*la frontera"* nos retrotraen a la era de la creación de la doctrina del '*destino manifiesto'*, cuando los intelectuales de EEUU justificaron su misión histórica de la divina providencia.

Con la superioridad tecnológica de los Estados Unidos y las capacidades ofensivas en el ciberespacio, el riesgo de americanización global aún permanece. Los planes agresivos de los Estados Unidos confirman los últimos desarrollos relacionados con la militarización de las redes sociales y las técnicas de ingeniería social.

Por ejemplo el proyecto Innovation for Defence Excellence and Security (IDEaS), también conocido como Innovation Hub, que tiene su sede en Canadá, está desarrollando nuevos métodos de guerra cognitiva[5].

El prefacio de estudio del IDEaS dice lo siguiente: "La Guerra Cognitiva ha resultado ser un gran desafío, especialmente porque altera la comprensión y la reacción, de forma gradual y sutil, ante ciertos acontecimientos. Sin embargo, todo esto tiene efectos nocivos a lo largo plazo, ya que posee un alcance universal que afecta a los individuos, los Estados y las organizaciones multinacionales, nutriéndose en la mayoría de los casos de las técnicas de desinformación y propaganda que buscan agotar psicológicamente a los receptores de la información. Todo el mundo contribuye a ella en mayor o menor medida, consciente o inconscientemente, y es por eso que desata una gran inestabilidad en todas nuestras sociedades, especialmente en sociedades abiertas como las occidentales. El conocimiento puede fácilmente ser convertido en un arma... Los instrumentos de la guerra informática van de la mano de las "neuro-armas" desarrolladas por la nueva tecnología, por lo que este campo se convierte en un frente de batalla del futuro. Todo esto se ve reforzado por los rápidos

5 Leonid Savin. La OTAN desarrolla nuevos métodos de guerra cognitiva. 01.11.2021. https://www.geopolitica.ru/es/article/la-otan-desarrolla-nuevos-metodos-de-guerra-cognitiva

avances en las NBIC (Nanotecnología, Biotecnología, Informática y Ciencias Cognitivas), además de las investigaciones sobre el cerebro humano"[6].

Por supuesto, estas tecnologías y el interés en ellas no es nada nuevo desde el punto de vista militar. Agencias estadounidenses como DARPA e IARPA han trabajado en proyectos similares durante décadas. Pero lo interesante es que en este caso la OTAN reconoce que tal vector estratégico hará parte de las guerras del mañana, junto con la creación de neuro-armas.

El informe ofrece toda una serie de definiciones sobre este asunto: *"La guerra cognitiva es una guerra ideológica que busca erosionar la confianza sobre la que ha sido construida la sociedad... La desinformación se aprovecha de las vulnerabilidades cognitivas de sus objetivos, especialmente las ansiedades o creencias que predisponen a sus objetivos a considerar como verdadera toda clase de información falsa. Todo ello requiere que el agresor posea un vasto conocimiento de las dinámicas sociopolíticas de su enemigo, al igual que saber cuándo y cómo atacar con tal de explotar las vulnerabilidades de su oponente*".[7]

El informe también habla de la economía del comportamiento humano, que es definida como un método de análisis económico aplicado a la comprensión psicológica de nuestro comportamiento y que busca descifrar la razón por la cual se toman ciertas decisiones. Las investigaciones sobre este tema han demostrado que los seres humanos se comportan cada vez más como máquinas.

Desde el punto de vista operativo eso implica un uso masivo y metódico de datos sobre el comportamiento humano y el desarrollo de técnicas que permitan la constante obtención de los mismos. La enorme cantidad de datos (comportamiento) que generamos, tanto consciente como inconscientemente, permite que los seres humanos sean cada vez más fáciles de manipular.

Las grandes empresas que dominan el sector de la economía digital han desarrollado nuevos métodos de recopilación de datos con tal de obtener información personal que los usuarios no necesariamente desean compartir. Esto ha permitido que los datos repetitivos sean utilizados en la creación de publicidad personalizada. Como el documento muy bien lo dice "*el origen del capitalismo de la vigilancia se alimenta de este brebaje inédito y lucrativo: excedentes de comportamiento, ciencia de los*

---

6 François du Cluzel. Cognitive Warfare. Innovation Hub - Nov 2020. https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf

7 Ibidem.

datos, infraestructura material, poder computacional, sistemas algorítmicos y plataformas automatizadas".

Estas nuevas formas de producción han sido implementadas por gigantes occidentales como Facebook, Google, Amazon, Microsoft y otros, por lo que no resulta accidental que tales empresas se han criticados constantemente no solo por el monopolio que ejercen, sino también por utilizar los datos de sus usuarios para manipularlos. Y dado que todos ellas cooperan activamente con las agencias de seguridad estadounidenses, se corre el riesgo de que los usuarios a nivel mundial terminen por ser usados como conejillos de indias.

También se ha criticado que la falta de regulación del espacio digital no solo proporciona muchos beneficios a los gobiernos que han adoptado estas nuevas tecnologías digitales, que pueden ejercer una importante influencia no solo sobre las redes informáticas y los cuerpos humanos, sino también sobre las mentes de sus ciudadanos al utilizarlas con fines malignos, como muy bien lo demostró el escándalo de Cambridge Analytica.

Los modelos digitales generados por Cambridge Analytica se basaban en la combinación de los datos personales con el aprendizaje automático y de ese modo usar esta información con fines políticos. Esto permitió la elaboración deperfiles individuales de los votantes y enviarles publicidad política personalizada. Cambridge Analytica hizo uso de las más avanzadas técnicas de encuesta y psicometría con tal de recopilar una enorme cantidad de datos personales que les ayudaron a comprender, a través de la información económica, demográfica, social y comportamental, lo que cada individuo pensaba sobre ciertos temas. Podemos decir que esta información literalmente permitió a las empresas sondear la mente misma de la población.

El documento dice sobre este asunto lo siguiente: "*La gigantesca colección de datos obtenidos a través de las tecnologías digitales es utilizada hoy con tal de definir y anticipar el comportamiento humano. El conocimiento del comportamiento humano es un problema estratégico. La economía del comportamiento adapta los métodos de la investigación psicológica a los modelos económicos y con ello crea modelos más precisos de las interacciones humanas*"[8].

Otro aspecto interesante de la guerra cognitiva señalado en este informe es la ciberpsicología, que sería la unión entre la psicología y la cibernética. Como hemos señalado anteriormente, "estos campos son relevantes tanto para la defensa como para la seguridad, que son de extrema importancia para llevar a cabo

8 Ibidem.

transformaciones significativas dentro de la OTAN. Si nos centramos en el esclarecimiento de los mecanismos que permiten el pensamiento, sin hablar de las concepciones, usos y límites de los sistemas cibernéticos, podemos decir que la ciberpsicología será un campo muy importante para las Ciencias Cognitivas. La aparición de la IA llevará a la creación de nuevas palabras y conceptos, pero también de nuevas teorías que expliquen la interacción entre los seres humanos y las máquinas, ya que estas últimas se han integrado plenamente en nuestro entorno natural (que ahora es antropo-técnico). Los seres humanos del futuro se verán obligados a crear una psicología basada en la relación con las máquinas. No obstante, el verdadero reto será desarrollar una psicología de las máquinas, del software, de la inteligente artificial y de los robots híbridos. La ciberpsicología es un campo científico complejo que abarca todos los fenómenos psicológicos asociados a las tecnologías o, al menos, de todo lo que se ve afectados por ellas. La ciberpsicología examina la forma en que los humanos y las máquinas interactúan mutuamente y explora cómo los seres humanos se relacionan con ellas. La IA cambiará la forma en que los seres humanos interactúan y se comunican con las máquinas".

El informe también hace énfasis en los aspectos problemáticos del pensamiento humano diciendo que "los problemas cognitivos pueden llevar a juicios inexactos y a una toma de decisiones pobre que puede provocar una escalada involuntaria o impedir la identificación oportuna de ciertas amenazas. Comprender las fuentes y los problemas que generan estas deficiencias cognitivas puede ayudarnos a reducir los malentendidos y a desarrollar estrategias mucho más eficaces a la hora de responder a los intentos de nuestros enemigos de usar estas fallas en nuestra contra.

El documento dedica todo un apartado a Rusia y, como es muy común en esta clase de informes, se usa a este país como un modo de justificar la necesidad de invertir en el desarrollo de armas neuronales o técnicas basadas en la guerra cognitiva, ya que la OTAN deber superar a sus adversarios en tales campos.

No debe extrañarnos que este mismo Centro publicó en junio del 2021 otro estudio sobre la guerra cognitiva, afirmando que la OTAN ha aceptado participar en ella: "*La guerra cognitiva es el uso integrado y combinado de armas con capacidades no cinéticas y cibernéticas que mediante la información, la psicología y la ingeniería social buscan ganar una lucha sin la necesidad de interacción física. Se trata de un nuevo tipo de guerra donde las potencias externas se valen de la opinión pública como una especie de arma con el propósito de influir y/o desestabilizar una nación. Estos ataques pueden visualizarse del siguiente modo: abarcar mucho*

mediante muy poco y de ese modo influir en el pensamiento y la acción de los objetivos, que pueden ser poblaciones enteras o individuos particulares, al igual que ciertas comunidades y/o organizaciones. Estos ataques buscan cambiar o reforzar cierta clase de pensamientos, influyendo/radicalizando la forma de pensar de la gente y de ese modo afectar la realidad material. La forma en que esto se lleva a cabo difiere bastante de los métodos tradicionales de guerra, pues la guerra informativa trata de controlar lo que la población ve, la guerra psicológica controla lo que la población siente y la guerra cibernética intenta perturbar las capacidades tecnológicas del enemigo. Finalmente, la guerra cognitiva busca controlar cómo piensa y reacciona una población ante determinados acontecimientos"[9].

Además, el documento presenta toda una serie de tecnologías que permitirían a la OTAN intervenir mejor en estos campos: *"La primera tecnología necesaria para la Guerra Electrónica Cognitiva (GEC) es el uso de sistemas cognitivos como la IA o formas de aprendizaje automático que permitan mejorar el desarrollo de las tecnologías de guerra electrónica (GE), ya que estas se vuelven cada vez más indispensables para los sistemas de defensa. Se trata de una guerra automatizada que difiere de los sistemas cognitivos legítimos ya que toma en cuenta el pensamiento y el comportamiento de los adversarios. Podemos decir que se divide en dos herramientas distintas: la primero es una forma de guerra no cinético que utiliza la GE para cambiar los pensamientos/comportamientos del adversario atacando sus sistemas de información/influencia. La otra forma sería el uso de estos sistemas para cambiar los pensamientos y comportamientos del adversario mediante un ataque directo a su sistema nervioso"*[10].

Por último, cabe señalar que la Conferencia de la *Red de Innovación de la OTAN* ha sido programada para el 9 de noviembre y el 30 de noviembre se celebrará en Ontario la conferencia *NATO Innovation Challenge*, todo lo cual nos indica que Occidente continuará desarrollando las nuevas tecnologías de la guerra cognitiva.

Por lo tanto, observamos una situación paradójica. Mientras que las nuevas herramientas de comunicación en el ciberespacio deben servir para el bien de las personas (facilitar el acceso a diversos servicios, compartir información, etc.), ciertos Estados las utilizan para reorganizar su dominio a nivel mundial. La naturaleza

9 Cognition Workshop. Innovative Solutions to Improve Cognition. June 1-3, 2021. https://www.innovationhub-act.org/sites/default/files/2021-07/210601%20Cognition%20Workshop%20Report-%20v3.pdf

10 Ibidem.

transfronteriza del ciberespacio facilita las operaciones de influencia, y las redes sociales sirven como una interfaz que oculta las verdaderas intenciones del agresor.

–

Leonid Savin es director del Fundacion Fidel Castro para el desarollo de las relaciones Ruso-Cabanas; investigador científico asociado del RUDN Universidad; autor de numerosos libros sobre el tema de los conflictos, la geopolítica y las relaciones internacionales.

editor@geopolitica.ru