Cibergeopolítica y la guerra cognitiva

Cybergeopolitics and the Cognitiva Warfare

Dr. C. Leonid Savin
Director de la Fundación Fidel Castro para el desarrollo de las relaciones Ruso-Cubanas; investigador científico asociado del RUDN Universidad; autor de numerosos libros sobre el tema de los conflictos, la geopolítica y las relaciones internacionales.
e-mail: editor@geopolitica.ru
Número ORCID: 0000-0002-0109-4200

Resumen

El ciberespacio en su sentido más amplio es visto hoy como un escenario principalísimo de la actividad política internacional, de ahí que para el mismo se hallan desarrollado varias doctrinas de carácter ideológico que lo asumen como una nueva zona para la expansión hegemónica, no en vano determinados poderes están tratando de asegurarse ventajas en el mismo para su uso exclusivo.

Eso es lo que explica el marcado interés no solo por la actividad comercial en el nuevo espacio, sino también, por los intentos de varias compañías tecnológicas para establecerse allí de manera monopólica y también se aprecia en la dimensión tecnológico-militar de las actividades del cíbercomando de las fuerzas armadas de los EE.UU., que de cierta manera, ha encontrado acompañamiento desde la OTAN, donde los miembros de esta alianza desempeñan un papel especial en el desarrollo y la implementación de tales proyectos.

Su enfoque coordinado y sus intenciones agresivas contra otros Estados, en primer lugar, contra Rusia, son también hoy muy evidentes. Los diferentes centros de la OTAN están atrayendo a sus laboratorios a científicos que se ocupan del estudio de las ciencias cognitivas, la cibernética, la inteligencia artificial, la biotecnología, etc., con el fin de asegurarse una clara ventaja estratégica en el futuro.

Sobre esta base, se puede suponer que el objetivo de la OTAN y de los países que encabezan esta alianza es conseguir el dominio del ciberespacio, incluida la posibilidad de influir en los ciudadanos de otros países a través de diversos formatos de interacción activa en el mismo mediante la aplicación de procedimientos como la manipulación en línea, la publicidad contextual, la recopilación de datos personales para crear un retrato psicológico para su posterior influencia, la vigilancia electrónica, la difusión de información falsa, etcetera.

Los considerables recursos que se invierten en el funcionamiento de estos centros y en la ejecución de diversos programas, como IDEaS y la aplicación de métodos de comunicación estratégica, indican una toma de decisiones centrada en estas cuestiones clave. El concepto de guerra híbrida también se refiere a actividades maliciosas en el ciberespacio.

Los casos mencionados en esta publicación muestran que muchos desarrollos occidentales en esta área se utilizan activamente para la guerra "por otros medios" contra Rusia. De ahí que ante esto, Rusia se ha visto obligada a responder, lo que ha hecho mediante el desarrollo de sus proyectos de ley, doctrinas y la introducción de nuevas tecnologías para garantizar su defensa y seguridad.

Dado que no existe una legislación internacional para regular el ciberespacio (con la excepción de los conceptos generales y una serie de resoluciones basadas en la ONU), existe el riesgo de que el conflicto se intensifique en esta área. Aunque Rusia había propuesto anteriormente desarrollar y firmar un documento regulatorio, los magros avances en las actividades del grupo de trabajo en la ONU muestran que Estados Unidos está frenando deliberadamente este trabajo pues no le conviene que haya orden en este escenario y apuestan por el caos con la idea de manejarlo a conveniencia.

Palabras clave: Ciberespacio, OTAN, Guerra, EE.UU., tecnologías.

Abstract

Cyberspace is considered as a field of political activity in a broad sense. It is revealed that the United States has developed several ideological doctrines for cyberspace and defines it as a new sphere for its expansion. Hence, there is not only an interest for commercial activity of a new kind and attempts by various technology companies to establish their monopolies, but also a military-technological dimension, from the activities of the cyber command of the US armed forces to special projects aimed at conducting information and psychological operations. NATO and its members play a special role in the development and implementation of such projects. Their coordinated approach and aggressive intentions directed against other states, primarily against Russia, are obvious. Various NATO centers attract scientists dealing with cognitive sciences, cybernetics, biotechnology, etc., in order to create a clear strategic advantage in the future.

Based on this, it can be assumed that the goal of NATO and the countries at the head of this alliance is to achieve dominance in cyberspace, including the possibility of influencing citizens of other countries through various formats of active interaction in cyberspace (online manipulation, contextual advertising, collection of personal data in order to compile a psychological portrait for further influence, electronic surveillance, dissemination of false information, etc.). The considerable resources that are spent on the maintenance of these centers and the implementation of various programs, such as IDEaS and methods of strategic communications, indicate purposeful decision-making on these issues. The concept of hybrid warfare also refers to malicious activity in cyberspace.

The cases indicated in the publication show that many Western developments in this area are actively used for war by other means against Russia. Russia is forced to respond to this by developing its own bills, doctrines and introducing new technologies.

Since there is no international legislation in the field of cyberspace regulation (with the exception of general concepts and a number of UN-based resolutions), there is a risk of escalation of conflict in this area. Although Russia has previously offered to develop and sign such a document, the activities of the working group at the UN show that the United States is deliberately slowing down this work.

Key words: Cyberspace, NATO, War, USA, technologies.

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 (Savin, 2018).

El investigador holandés, Paul Treanor, cree que el modelo de red central tiene su origen en el liberalismo clásico (Treanor, 1996). 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 (Bangemann Report, Europe and the Global Information Society, 1994). 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 ciberliberal.

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 (Dyson, Gilder, Keyworth & Toffler, 1994): 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 autogobierno, 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.

Al final de su trabajo doctrinal sobre el ciberliberalismo, Toffler, Keyworth, y sus colegas revelaron el verdadero propósito de sus intenciones (Dyson, Gilder, Keyworth & Toffler, 1994): Hay temas clave 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 EE.UU. 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 (Savin, 2021).

El prefacio de estudio del IDEaS dice lo siguiente (Cluzel, 2020): 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 "neuroarmas" 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 avances en las NBIC (Nanotecnología, Biotecnología, Informática y Ciencias Cognitivas), además de las investigaciones sobre el cerebro humano.

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 (Cluzel, 2020): 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.

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 com-

portamiento 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 datos, infraestructura material, poder computacional, sistemas algorítmicos y plataformas automatizadas" (Cluzel, 2020).

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 de perfiles 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 (Cluzel, 2020) 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".

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 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 de 2021 otro estudio sobre la guerra cognitiva (Cognition Workshop. Innovative Solutions to Improve Cognition, 2021), 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 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 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.

Además, el documento presenta toda una serie de tecnologías que permitirían a la OTAN intervenir mejor en estos campos (Cognition Workshop. Innovative Solutions to Improve Cognition, 2021): 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.

Otro ejemplo es el proyecto, "Rusia y la guerra híbrida: Definiciones, capacidades, alcance y posibles respuestas" (report 1/2016), fue realizado por Bettina Renz y Hanna Smith, con las percepciones de Tor Bukkvoll, Antulio J. Echevarria, Keir Giles, Sibylle Scheipers, Sir Hew Strachan y Rod Thornton (Renz y Hanna Smith, 2016: 21). Es importante indicar que Antulio J. Echevarria (2015) es un analista militar que desarrolla nuevas aproximaciones para la guerra no-convencional. Su teoría más novedosa está dedicada a las "zonas grises de conflicto" donde propone repensar los métodos de la actividad paramilitar.

No es sorprendente que los autores afirmen que Rusia está actuando en violación de la legislación internacional, de los derechos humanos, de las normas europeas, etc. También se declara: "Las acciones rusas en el antiguo espacio soviético pueden ser explicadas por su intención de reinstaurar y mantener su posición como el actor regional dominante, por la fuerza militar si fuera necesaria, que no es lo mismo que buscar la recreación de la Unión Soviética por medio de la expansión territorial". También es importante mencionar que este documento fue publicado en Finlandia, que no es miembro de la OTAN.

Pero ¿qué son exactamente las comunicaciones estratégicas? En un informe especial sobre la experiencia de la OTAN, el rango de cuándo y cómo se usan las comunicaciones estratégicas, es descrito como "un entorno de información global cada vez más participativo, que progresivamente cuestiona la justificación para los cortafuegos de potencial entre las actividades de información, y además es el momento adecuado para investigar la estructura, los resultados, y la cultura organizativa dentro de las disciplinas tradicionales de StratCom sobre Diplomacia Pública (DP), Asuntos Públicos (AP), Asuntos Públicos Militares (APM), Operaciones de Información (Info Ops [en inglés]) y Operaciones Psicológicas (PSYOPS [en inglés]) (Savin, 2020: 35). La comprensión mutua de las perspectivas nacionales (e interpretaciones diversas) en estas áreas es tan crítica como determinante lo qué —en qué combinación— tiene relevancia y repercusión para el futuro" (Mapping of Stratum Practices in NATO Countries, 2015: 4).

Esta aproximación a las comunicaciones estratégicas fue reorganizada en la OTAN allá por 2014 con un presupuesto especial y equipos de trabajo. En 2015, el Centro de Excelencia de las Comunicaciones Estratégicas (con sede en Riga, Letonia), lanzó la revista *Comunicaciones Estratégicas de Defensa*. El volumen 1, número 1, publicado en invierno de 2015 estaba dedicado a Rusia, al daesh, a los medios de comunicación sociales, y a la experiencia de la OTAN/RU/EEUU en las operaciones psicológicas y las comunicaciones políticas. De hecho, la publicación fue un buen inicio para presentar e involucrar a principiantes.

Podemos ver claramente la narrativa de los "gemelos del mal" —Rusia y daesh— ubicados en las dos primeras publicaciones, con más artículos orientados al estudio sobre planificación y análisis político-militar implantado en la cultura de la comunidad euro-atlántica.

La OTAN también se enfocó en "los valores euro-atlánticos y la comunicación estratégica de Rusia en el espacio euro-atlántico", proporcionando una enorme investigación sobre la actividad de la televisión rusa en el contexto de las empeoradas relaciones entre occidente y Rusia, así como la diferencia entre las estructuras morales de las sociedades occidentales y rusa.

Otros conjuntos de recursos y folletos de propaganda (en su mayoría anti-rusa) fueron publicados más tarde y están disponibles en el sitio web del centro.[1]

Pero esta aproximación no es la únicamente de la OTAN. En el informe número 30, de julio de 2016, del Instituto de la Unión Europea para Estudios de Seguridad (ubicado en París, Francia) titulado "Comunicaciones estratégicas, contrarrestando a Rusia y al ISIS/daesh", en el cual, de modo bastante interesante, se repite la combinación de Rusia y daesh (Strategic communications Countering Russia and ISIL/Daesh, 2016): "Lo que sigue es un catálogo tentativo de puntos de acción que pueden ser considerados por los creadores de políticas de la UE para mejorar la efectividad de las propias comunicaciones estratégicas de la UE. Algunas se aplican tanto a Rusia como al daesh, mientras que otras están más personalizadas y ajustadas al caso específico".

Es muy posible que esta idea de los "gemelos del mal" naciera en un laboratorio u oficina de inteligencia de EE.UU. y después se reprodujera y diseminara a través de sus socios europeos.

Por un lado, las iniciativas de comunicaciones estratégicas están dirigidas a justificar la ampliación de la OTAN (incluyendo los países todavía

[1] Véase: http://stratcomcoe.org/redefining-euro-atlantic-values-and-russias-strategic-communication-euro-atlantic-space.

neutrales de Suecia y Finlandia) y el incremento de su presupuesto militar ante tan artificial enemigo como es Rusia. Por un lado, podemos ver que en estos intentos se ponen más anclas en países europeos (y no solo europeos), así como en sus capas políticas, económicas y sociales.

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

Las tecnologías digitales también afectan a la recopilación, almacenamiento y procesamiento de la información y, por consiguiente, a los mecanismos de toma de decisiones. El uso de robots para revisar los enfoques de planificación estratégica está ejemplificado por la Tercera Estrategia de Compensación de los Estados Unidos. Hay nuevas decisiones tácticas. Por ejemplo, un enjambre de robots de combate. Pero, a diferencia de muchos Estados, Rusia conserva características geográficas, estratégicas, etnográficas e ideológicas únicas, así como un potencial de recursos que le permite, en modo autárquico, crear no sólo nuevas tecnologías militares, sino también doctrinas teóricas y plataformas para diversos experimentos (científicos, económicos y sociales) que, en condiciones adecuadas, pueden adaptarse a la política interior y exterior.

Si a todo lo anterior añadimos las numerosas relaciones y asociaciones diplomáticas y de otro tipo, así como el cambio en el equilibrio de poder en muchas regiones que han reducido significativamente el papel y la influencia de los Estados Unidos, entonces tiene buenas perspectivas la capacidad de Rusia para enfocar adecuadamente el *coaching* de guerra, incluyendo el desarrollo de una estrategia proactiva dirigida a disuadir, neutralizar y, si es necesario, eliminar las fuerzas hostiles en sus diversas manifestaciones (Savin, 2020: 249).

Lo anterior nos permite asegurar, de que estamos ante la posibilidad de una escalada de conflictos a través del ciberespacio y sobre el control del ciberespacio. Dado que las opiniones de la mayoría de los países están divididas, un grupo liderado por Estados Unidos cree que el ciberespacio debe estar abierto a todos los actores, incluidas las grandes empresas (coincidiendo con que los principales actores en este campo son las empresas estadounidenses), y otro grupo, donde aparecen Rusia y China, que defiende la opinión de que debe haber soberanía estatal sobre el ciberespacio de acuerdo con las fronteras físicas y del espacio radioeléctrico de cada país.

Lo cierto es que la falta de una coherente legislación internacional en esta esfera permite diversas interpretaciones, sobre todo, interpretaciones de carácter político y la situación se complica más, por el hecho de que el ciberespacio es un entorno artificial creado por el hombre y que está en constante modificación y reacomodo.

Así las cosas, lo más probable es que esta bipolaridad se mantenga durante un cierto tiempo, y los líderes de los dos bloques intentarán atraer a su lado a los Estados que todavía se muestran indecisos. Pero eso no impedirá que los países tecnológicamente más avanzados, principalmente los Estados Unidos y sus satélites occidentales, desarrollen y utilicen armas cognitivas en el ciberespacio.

References bibliográficas

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

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

Cluzel, Francois du (2020): "Cognitive Warfare", June-November, https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf.

Mapping of Stratum Practices in NATO Countries (2015).

Strategic communications Countering Russia and ISIL/Daesh (2016): Report No. 30, European Union Institute for Security Studies, Paris.

Dyson, E., G. Gilder, G. Keyworth, & A. Toffler (1994): Cyberspace and the American Dream: A Magna Carta for the Knowledge Age. Future Insight, Release 1.2, http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html.

Echevarria, A.J. (2015): "How we should think about 'gray zone wars'", Infinity Journal, 5(1).

Renz, B. & H. Hanna Smith (2016): Russia and Hybrid Warfare: definitions, capabilities, scope and possible responses, report 1/2016. Aleksanteri Institute, University of Helsinki, Finland.

Savin, L. (2018): "Cibergeopolítica: Cuestiones de ideología", https://www.geopolitica.ru/es/article/cibergeopolitica-cuestiones-de-ideologia.

Savin, L. (2020): Marchas de guerra por otros senderos: Coaching de guerra. Ediciones Fides.

Savin, L. (2021): "La OTAN desarrolla nuevos métodos de guerra cognitiva", https://www.geopolitica.ru/es/article/la-otan-desarrolla-nuevos-metodos-de-guerra-cognitiva (enero 11).

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