AMERICA LATINA en movimiento

544

octubre 2019

ISSN 1390-1230

Las redes de la guerra

OLAG

alai

544 octubre 2019
año 43, 2ª época
edición digital

Ilustración de portada:
***Viglancia en todo momento, en todo lugar*, ALAI**

Diseño editorial: **Verónica León**

Publicación internacional de análisis y opinión de la Agencia Latinoamericana de Información

ISSN No. 1390-1230
Director: Osvaldo León

ALAI: Dirección postal
Casilla 17-12-877, Quito, Ecuador
Sede en Ecuador
Av. 12 de Octubre N18-24 y Patria,
Of. 503, Quito-Ecuador
Telf: (593-2) 2528716 - 2505074
Fax: (593-2) 2505073

URL: http://alainet.org

Redacción:
info@alainet.org

Suscripciones y publicidad:
alaiadmin@alainet.org

ALAI es una agencia informativa, sin fines de lucro, constituída en 1976 en la Provincia de Quebec, Canadá.

Suscripción (8 números anuales)

	Individual	Institucional
Ecuador*	US$ 35	US$ 45
A. Latina	US$ 60	US$ 80
Otros países	US$ 75	US$ 140

* incluye IVA

Cómo suscribirse:
www.alainet.org/revista.phtml
se aceptan pagos por Internet

AMERICA LATINA
en movimiento

Las redes de la guerra

co-edición:

OLAG

alai

Investigación realizada gracias al programa PAPIIT. Proyecto Economía y guerra en el siglo XXI (IG300318) de la Universidad Nacional Autónoma de México.

En el siglo XXI:

Redes y entramados de la guerra

Ana Esther Ceceña

En esencia, la Red Centralizada de Guerra traduce la superioridad en información en poder de combate.
Defense Advanced Research Projects Agency

En 1993, Arquilla y Rondfeldt, dos importantes cabezas pensantes del Pentágono, anunciaban la constitución de un nuevo tipo de guerra que correspondía a lo que implícitamente se reconocía como un nuevo dominio. El mundo recibió así el anuncio de una nueva época, que llevaba ya claramente tres décadas de gestación: estábamos en la era ciber.

La estética del mundo se transformó. A los dominios conocidos (mar, tierra, subsuelo y espacio) se agregaba el ciberespacio, construido material y virtualmente con cables, máquinas intercomunicadas, información, códigos, protocolos, algoritmos y ondas que atraviesan de manera permanente el espacio atmosférico, haciendo posible el intercambio de crecientes cantidades de todo tipo de informaciones.

Se colonizó la atmósfera albergando un espacio a la vez virtual y material llamado ciberespacio. Un espacio donde lo inmaterial adquiere cuerpo a través del correo electrónico, los flujos de video, las llamadas telefónicas o las órdenes ejecutadas por los autómatas.

Ese carácter a la vez material e inmaterial dio a la *web*, que emergió en esos años, la apariencia de un entramado misterioso asible e inasible a la vez, que se fue complejizando y sofisticando mientras se introducía en todas las actividades a manera de un sistema orgánico capaz de llegar a los más finos vasos capilares y a los más delicados impulsos emocionales.

La creación del ciberespacio fue inducida, dirigida y controlada por el Pentágono para mantener y ampliar el dominio del sujeto hegemónico constituido por lo que Eisenhower denominara el complejo militar industrial.

En 2003 el Departamento de Defensa de Estados Unidos acuñó el término de *Network centric warfare* para indicar la entrada en escena de la ciberguerra. El ciberespacio alcanzaba ya en ese momento todos los ámbitos de densidad estratégica.

> Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which

Ana Esther Ceceña es Coordinadora del Observatorio Latinoamericano de Geopolítica (OLAG) en el Instituto de Investigaciones Económicas de la Universidad Nacional Autónoma de México; Presidenta de ALAI. Coordinadora del proyecto Economía y guerra en el siglo XXI, UNAM, PAPIIT IG300318.

> an adversary relies in order to "know" itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. (Arquilla y Rondfeldt, 1993: 30)

Los alcances del entramado

El nuevo sistema de comunicaciones creado con fines estratégico militares no estaba dirigido solamente a aumentar la asimetría en el campo de batalla sino a generar condiciones de superioridad tecnológica para el capital, en este caso, de filiación estadounidense. Así pues, manteniendo la confidencialidad, la tecnología pasó a encontrar sus formas de aplicación en la industria, acosada por la competencia de Japón y los tigres asiáticos.

Desde la revolución del taylorismo-fordismo a inicios del siglo XX, con la reducción de las tareas creativas de la producción a movimientos fragmentados y repetitivos que arrebataron el saber de manos del artesano y lo depositaron en la máquina, no había ocurrido una transformación de estatura equivalente. El conocimiento referido al proceso de trabajo y su organización volvió a enfrentar al trabajador colectivo mediante su transformación en impulsos. Los movimientos fraccionados de Taylor aparecen, a finales del siglo, como impulsos binarios: el conocimiento del proceso de trabajo traducido una simple lectura de 0 y 1. El capital organiza el entramado de ceros y unos, así como antes organizó el de movimientos fraccionados. La reconstrucción y el conocimiento del proceso queda del lado del capital mientras que el obrero (o el participante en un punto de la red) sólo tiene conocimiento de su pequeña partecita, de su cero o uno, y quizá del de su círculo cercano. Esto es parte de la guerra dentro del espacio de la producción, pero aquí se llaman relaciones de clase.

En todo caso, este nuevo sistema de comunicaciones y de codificación posibilitó el fraccionamiento del proceso de trabajo en fases desmembradas geográficamente –para beneficiarse de las condiciones específicas de cada lugar–, salvaguardando la precisión necesaria para que el todo embonara en el momento del ensamble final. Es así como surge el *auto mundial*, los productos *plurinacionales*, la industria maquiladora, la movilidad evasiva del capital y la globalización. Es la red de la producción.

Simultáneamente, la web fue penetrando el espacio de la reproducción. Como la sociedad es compleja, la otra pista de las aplicaciones civiles de internet provino de la necesidad de recurrir a universidades y especialistas para ir limando la rudeza y limitada versatilidad de una tecnología emanada del campo de batalla. Y más allá de las universidades, cuando acertadamente el Pentágono decidió abrir su libre uso –con controles centralizados, por supuesto–, hubo una masiva contribución al perfeccionamiento y diversificación de aplicaciones de internet.

Dejar que los investigadores lo usaran para compartir sus hallazgos, sin dejar de supervisar, permitía detectar los espacios de ciencia de frontera potencialmente enriquecedores de la internet. Su uso masivo, en cambio, contribuyó a suavizarlo y hacerlo *amigable*, a la vez que lo llevó hasta los más recónditos lugares y dilemas de la sociedad, incluyendo los de las nuevas formas de trabajo domiciliario que propició la conectividad. No obstante, en sentido contrario, este involucramiento generó alternativas de uso de la red y una experticia no controlada que convirtió el espacio creado en un nuevo campo de disputa. El *hackeo* y la piratería son tan consustanciales al ciberespacio como el espionaje, la vigilancia y el control de voluntades.

El terreno de la ciberguerra

Aproximadamente 3 mil millones de personas (42 % de la población mundial) viven conectadas a la red de redes. La competencia y la adquisición de los estándares tecnológicos han llevado a una alta automatización de los procesos productivo y reproductivo de manera

que los centros neurálgicos de la organización social están vinculados a la red y sometidos a sus protocolos. La amplitud de la *web* y la profundidad de sus tentáculos, así como su verticalidad y transversalidad, la convierten en el medio idóneo para cubrir el espectro completo de la dominación. Un ataque en la red altera la materialidad y la subjetividad, atraviesa diferencias de clase, de cultura y características étnicas, raciales y de género: "…internet no es una sola entidad […] todos los días nacen redes nuevas en el cúmulo global de redes de comunicaciones interconectadas." (Snowden, 2019: 17).

El control, el dominio y el disciplinamiento, que constituyen el propósito focal de las guerras, daba sentido hasta ahora al despliegue de fuerzas militares bajo diferentes modalidades y en terrenos variados: *marines* desembarcando en nuestras costas o comandos interviniendo en nuestros territorios, espionaje y panópticos, guerra psicológica, étnica o cultural, pero todas ellas se ven reforzadas y potenciadas en el siglo XXI por el desarrollo de tecnologías informáticas y experticias que van configurando la hoy ineludible telaraña (*web*). Simultáneamente, modalidades nuevas de relacionamiento y de guerra han ido surgiendo de la emergencia de este nuevo espacio o, más precisamente, nueva dimensión de las relaciones sociales, de las relaciones de poder y de los flujos dinámicos de la reproducción global, al punto que a los comandos territoriales del Comando Conjunto de Estados Unidos se agregó, en 2009, el USCybercom.

El cerebro de la guerra de espectro completo opera en una amplia medida en el ciberespacio, donde conectan y se cruzan todas las informaciones de los operativos "en tiempo real" para garantizar mejores resultados, con datos logísticos o de cualquier otro tipo necesarios para asegurar el cumplimiento de los objetivos trazados.

El ciberespacio, entendido como infraestructura crítica o estratégica, es el campo de la vulnerabilidad y el ejercicio del poder; es ahí donde se juegan las asimetrías más riesgosas puesto que es un espacio compartido entre fuerzas contradictorias. Los más inasibles y peligrosos enemigos del orden establecido, de las jerarquías de poder y del modo de vida alienado circulan por la *web* e intervienen en ella, rompiendo su linealidad y confirmando el ciberespacio como terreno de confrontación y disputa. Por eso, junto con los fabricantes anónimos de armas biológicas, los hackers son considerados entre los enemigos más peligrosos del orden establecido.

Los acontecimientos en Tallin, Estonia, de abril y mayo de 2007 son identificados como el primer caso de ciberguerra, seguidos por los de Georgia en 2008. Una intervención en la web activó las acciones de Denial of Service (DoS) y Distributed Denial of Service (DDoS) y con ello afectó páginas del gobierno, bancos, medios de comunicación y partidos políticos, provocando la suspensión temporal del servicio (Kaiser, 2014: 11).

La intervención en el ciberespacio puede provenir de cualquier lugar pero hay los disruptores aislados, casuales y hasta criminales (roba-bancos, etc.); hay organizaciones de nivel estatal con propósitos geopolíticos y hay los que responden a políticas de estado deliberadas y planeadas que trascienden con mucho las acciones de ciberseguridad o defensa y son parte de las ofensivas de dominación y guerra.

La información como arma múltiple

Ahora bien, los niveles generales de automatización han vuelto a la sociedad totalmente dependiente de la *"información"*. Las capacidades humanas han sido potenciadas y trascendidas por el sistema de máquinas que opera bajo las indicaciones de los algoritmos usando acervos considerables y dinámicos de información que nutre sus acciones o, incluso, en los casos de alta tecnología, la *toma de decisiones* del sistema de máquinas. Si se da información equivocada, no útil o contradictoria, el sistema se confunde o se entorpece y la dinámica general (o específica) pierde

eficiencia y puede conducir a contrasentidos. Ahí está el punto crítico. Poder saltar los candados de la *protección redundante*, alterar los algoritmos (para que desvíen los depósitos del banco a una cuenta privada, o para que irrumpan y modifiquen los protocolos de una planta nuclear, por ejemplo), es poner en situación de vulnerabilidad, que incluso podría ser catastrófica, el dominio en cuestión. Lo mismo entre competidores o enemigos equivalentes confrontados, que en el caso de *hackers sociales*, si se les puede llamar así.

No obstante los riesgos, siempre presentes, el desdoblamiento de las redes en sociales, militares, estratégicas, corporativas, etc., según sus ámbitos y sus usos, éstas ofrecen el mejor andamiaje para diseñar estrategias de guerra de espectro completo. Así, la intervención simultánea en una infraestructura crítica, en el circuito financiero, en las redes comerciales y en la formación de sentidos y la manipulación de la opinión pública conforman parte sustancial de los nuevos entramados de la guerra. La guerra en todos los terrenos: simultánea pero con ritmos diferenciados, envolvente, desconcertante y eficaz para entorpecer la respuesta.

Entre las armas de la ciberguerra podemos encontrar en un lugar muy visible la contrainformación y el uso de mentiras, ocupando los principales espacios mediáticos pero, sobre todo, circulando por las redes sociales con una intensidad que casi impide desmentirlas. Esto, que se conoce comúnmente como guerra de cuarta generación es sólo una parte del escenario. Cubre los hechos y coloca narrativas amañadas y provocadoras que buscan generar o inhibir reacciones en la población para asegurar las condiciones propicias para intervenciones directas o más definitivas.

Las intervenciones o ataques en infraestructuras (financieras, eléctricas, de movilidad y comunicación, de abastecimiento, etc.), que provocan caos temporales o paralizaciones de sectores de amplio impacto y que aparecen muchas veces encubiertas o narradas por el trabajo mediático y de colocación de sentidos, conforman la modalidad cibernética de los bombardeos. Es la alternativa *limpia* para deteriorar las condiciones de reproducción y de funcionamiento general con la intención de fragilizar una región, un país o una pequeña localidad, sin movilizar aviones, misiles o equipo de gran envergadura y costo, y sin asumir responsabilidades frente a la comunidad mundial. Trabajo sucio de manera *limpia* y barata que alivia el peso pero se combina con todas las otras modalidades de la guerra.

De aquí el paso siguiente es ya el ataque de los puntos estratégicos, donde los operativos informáticos pueden adelantarse y hasta prevenir el empleo directo de las fuerzas de ataque convencionales. El cerebro militar, productivo y político. Ataque a importantes refinerías o campos petroleros en el caso que corresponda; a los centros de inteligencia militar; a las fábricas de energía nuclear; a los depósitos de armas estratégicas; a la cabeza del gobierno; a todo aquello que ponga en riesgo la supervivencia del enemigo en cuestión.

Un ciberespacio paralelo

La superioridad tecnológica y operativa en el ciberespacio es herramienta clave de esta guerra. Todos los laboratorios militares de producción e innovación tecnológica dedican la mayor parte de sus recursos materiales y humanos a la búsqueda de alternativas de intervención en el ciberespacio que les permitan tomar el control, por lo menos, de los dispositivos de hackeo.

La Defense Advanced Research Projects Agency (DARPA) de Estados Unidos, está creando, entre otras cosas, un ciberespacio paralelo, protegido y exclusivo, en el que pueda mover su información estratégica. Una vez creado y en operación, no se sabe cuánto tiempo tardarán los expertos informáticos, de múltiples orígenes, en penetrarlo y provocar una nueva carrera hacia adelante pero, mientras tanto, se contaría con una franja segura.

En todo caso, si el campo de batalla más innovador pasa hoy por el ciberespacio, es imprescindible estudiar con cuidado todas sus aristas, potencialidades y vulnerabilidades. La dominación tiene nuevas y poderosas herramientas y la sociedad está siendo sometida a procesos autoritarios inéditos por su profundidad y abarcamiento. Nunca había sido más cierto el panóptico carcelario que estudiara Foucault ni más extendida la lista de anormales a ser vigilados. Por el otro lado, no se explica el autoritarismo sin la rebeldía y ahí están los Anonymus, los Assange, los Snowden y muchos otros sin rostro tratando de hacer saltar los muros y abrir las compuertas del futuro.

Ahora existe una militarización del ciberespacio, en el sentido de una ocupación militar. Cuando te comunicas a través de internet, cuando te comunicas a través del teléfono móvil, que ahora está entrelazado a la red, tus comunicaciones están siendo interceptadas por organizaciones de inteligencia militar. Es como tener un tanque en tu dormitorio. Es un soldado que se interpone entre tú y tu mujer cuando os enviáis mensajes. Todos estamos bajo una ley marcial en lo que respecta a nuestras comunicaciones, simplemente no podemos ver los tanques, pero están […] Pero internet es nuestro espacio…
Julian Assange

Fuentes citadas

Assange, Julian 2019 *Cypherpunks. La libertad y el futuro de internet* (DEUSTO) e-book. Appelbaum, Jacob, Müller-Maguhm, Andy y Zimmermann, Jérémy colaboradores.

DARPA (Defense Advanced Research Projects Agency) 2003 Strategic plan, in <http://www.arpa.mil/body/strategic.html>, February.

Foucault, Michel 1992 (1977) *La microfísica del poder* (Madrid: La Piqueta).

Kaiser, Robert, 2015 "The birth of cyberwar" en *Political Geography* 46, pp. 11-20.

Snowden, Edward 2019 *Vigilancia permanente* (Planeta) e-book.

Las corporaciones militares y el gran negocio de la guerra

Raúl Ornelas

Es un lugar común señalar que aun en el capitalismo decadente, la guerra impulsa la acumulación de capital y produce enormes ganancias para quienes participan en ella. Sin embargo, el tránsito desde las guerras mundiales y los conflictos de la guerra fría hacia las llamadas guerras asimétricas, introdujo cambios significativos en las relaciones entre las corporaciones, los estados y las instituciones que participan en los conflictos bélicos. Estos cambios pueden ordenarse en torno a dos ejes:

> En primer lugar, la guerra "desborda" sus antiguos límites marcados por conflictos territoriales con enemigos identificados y generalmente organizados bajo la forma de fuerzas armadas, para convertirse en una práctica de "espectro completo" en la que los estrategas y comandantes militares no reconocen límites territoriales ni distinguen entre combatientes y población civil.
>
> En segundo lugar, el estado y las instituciones ceden buena parte de sus actividades bélicas a las corporaciones privadas: de manera similar a lo que sucede en otros sectores de la actividad productiva, las tareas de defensa, y no solo la producción de armamentos, pasan a manos de empresas privadas.

Raúl Ornelas es Investigador Titular del Instituto de Investigaciones Económicas de la UNAM e integrante de OLAG. Coordinador del Laboratorio de Empresas Transnacionales (LET).

El desplazamiento del estado como instancia del ejercicio legítimo de la violencia representa una transformación crucial para la cohesión del capitalismo. El que corporaciones privadas, independientes de los controles institucionales y de las leyes del régimen liberal, realicen actividades de seguridad e incluso de guerra, socava uno de los pilares de la legitimidad del capitalismo. La privatización del ejercicio de la violencia produce cuantiosas ganancias, al tiempo que refuerza las tendencias a la disgregación social y hace frágiles los regímenes políticos al poner en cuestión la hegemonía cultural y política del liberalismo y sus instituciones; todo esto estimula las tendencias más autoritarias tanto del sistema como de grupos y sujetos sociales cada vez más afectados por la violencia. El recurso generalizado a la represión, al control social e incluso a las acciones militares, explica la expansión de las corporaciones militares privadas, que en forma progresiva, ganan terreno y juegan, cada vez más, un papel estratégico en las acciones bélicas.

Relaciones empresa-estado

En los años recientes, asistimos al surgimiento y a la consolidación de corporaciones dedicadas a proveer servicios ligados a la seguridad y a las actividades militares. Este tipo de corporación es el sujeto típico de las nuevas relaciones empresa-estado: en su interior conjunta los intereses de militares, empresarios y políticos, al tiempo que desarrolla y se apropia de las tecnologías bélicas de punta, incluyendo tres de las más mortíferas: las armas

autónomas, la "inteligencia", y las operaciones especiales. Presentamos aquí una caracterización de las corporaciones que realizan actividades de defensa y de seguridad.

De acuerdo con el Stockholm International Peace Research Institute, las ventas de las 100 mayores corporaciones productoras de armas pasó de 201 a 398 mil millones de dólares (mmd) entre 2002 y 2017, un crecimiento de 98%. En este universo, las corporaciones con sede en Estados Unidos concentran la mayor parte de las ventas: 128 mmd (64% del total) en 2002, y 226 mmd (57% del total) en 2017, un crecimiento de casi 77% de las ventas en ese periodo. En 2017, solo las ventas de corporaciones estadounidenses representan 13% del gasto militar mundial, estimado en 1.7 billones de dólares por la misma fuente, proporción que indica la importancia de las corporaciones en la actividad militar global. Es preciso señalar que esta fuente no proporciona información sobre las corporaciones militares con sede en China, a pesar de que reporta el segundo gasto militar más alto del mundo en 2017, 228 mmd, cifra equivalente a las ventas de armas de las corporaciones con sede en Estados Unidos. El gasto en defensa de la potencia líder alcanzó 610 mmd.

Evasión de las leyes de guerra

En este amplio mercado podemos distinguir 4 segmentos principales:

1. Logística: se trata de empresas que realizan tareas de retaguardia como provisión de alimentos, avituallamiento, construcción y mantenimiento de las instalaciones militares, incluso en teatros de guerra (modelo Halliburton).
2. Operaciones de combate, generalmente operaciones especiales y protección de personas o posiciones estratégicas (modelo Blackwater).
3. Capacidades de comunicación y de defensa, defensa y ataque de las infraestructuras de comunicación, tareas de espionaje y de vigilancia que permiten obtener información para la guerra y el control social (modelo Booz Allen Hamilton).
4. Seguridad fuera de los teatros de enfrentamiento físico, en dos vertientes complementarias: la llamada lucha antiterrorista y el control social *in situ*; es decir, control de multitudes, combate al crimen organizado, pacificación de la contestación social, combate en megalópolis, etcétera (modelo G4S).

Estas actividades eran realizadas por instancias y personal ligados al estado, no siempre de las fuerzas armadas, pero sí bajo el control estatal; tal es el caso de las agencias de inteligencia que existen en muchos países. La transformación en curso, por tanto, no sólo implica la complementariedad entre el estado y las corporaciones privadas (que es la justificación de gobernantes y estrategas militares para privatizar las actividades), sino la cesión de tareas estratégicas a las instituciones privadas, que aúnan un alto impacto en la trayectoria de los conflictos con la evasión de las leyes de guerra y los controles gubernamentales e internacionales. A través de esta cesión, los estados rompen con uno de los principios de la seguridad nacional: el control de los aspectos estratégicos de la defensa nacional, que al ser controlados por entidades privadas, generan vulnerabilidades para los gobiernos y las fuerzas armadas. La tríada Manning – Assange – Snowden logró poner en evidencia tanto la extensión de las actividades de los contratistas privados militares como la gravedad de los crímenes que cometen de manera cotidiana y en total impunidad. No obstante, el nuevo sentido común de gobernantes y militares habla de complementariedad y afirma que el cometido esencial de las corporaciones privadas militares y de seguridad es la realización del "trabajo sucio" que implican todos los conflictos que enfrentan con la mayor eficiencia y el menor costo posibles.

Para ilustrar la importancia de estas corporaciones, ofrecemos dos botones de muestra.

En primer lugar, destaca el peso creciente de los contratistas privados en las fuerzas estadounidenses de ocupación durante las invasiones en Afganistán e Irak. De acuerdo con el Servicio parlamentario de investigación del Congreso de

Estados Unidos, en 2008, año en que se alcanzó el máximo histórico de la participación de personal de corporaciones privadas, se reportaron más de 188 mil elementos de las fuerzas armadas contra más de 201 mil contratistas, de los cuales 168 mil eran contratistas locales y de países terceros, una proporción de uno a uno. Si consideramos únicamente el personal destinado a Afganistán, esa proporción se eleva a 1.8. En 2016, el personal de las fuerzas armadas estadounidenses se redujo de manera significativa a 13 887 personas, en tanto que los contratistas fueron más de 28 mil elementos, una proporción de 2 a 1. Por lo que toca al presupuesto asignado para financiar las operaciones en esos países, se estima en 1.5 mil millones de dólares durante el periodo de auge de las operaciones militares en esos países, de 2001 a 2008. Estos datos parecen indicar que la privatización de la guerra llegó para quedarse. Los contratistas constituyen ejércitos privados con todo tipo de capacidades para hacer frente a todo tipo de conflictos bélicos, y por esa vía, apuntalan la posición hegemónica de Estados Unidos al crear grandes asimetrías militares.

En segundo lugar, podemos mencionar el caso de las empresas de seguridad. Entre las corporaciones más importantes de esta actividad están: G4S (Reino Unido) que en 2018 tuvo ingresos de 9.5 mmd resultado de sus operaciones en más de 90 países, con más de 546 mil empleados, es uno de los principales empleadores del mundo; Securitas AB (Suecia) que reportó ingresos por 10.5 mmd, más de 370 mil empleados y actividades en 58 países; y Allied (Estados Unidos), con ingresos de 5.8 mmd y 200 mil empleados. Estas corporaciones realizan tareas de vigilancia y protección de instalaciones, de eventos públicos, transporte de dinero y de personas e incluso acciones armadas y de administración de prisiones. Una de sus actividades más controvertidas son las misiones de "mantenimiento de la paz", contratadas por organismos multilaterales como Naciones Unidas, y en las que han cometido diversos crímenes y violaciones a las leyes de guerra entre los que se cuentan: dos escándalos por tráfico de personas y prostitución organizada cometidos por la empresa Dyncorp en Bosnia (1999) y en Afganistán (2009); 6 empleados de CACI y Titan, que trabajaron como interrogadores y traductores en la prisión de Abu Ghraib en 2003 fueron acusados por actos de tortura contra prisioneros; la masacre cometida por empleados de Blackwater contra civiles iraquíes, con un saldo de 17 muertos y 20 heridos en septiembre de 2007; el mismo año, empleados de Triple Canopy y Aegis fueron denunciados por disparar contra civiles en Irak, acción que fue filmada por los mercenarios; Aegis fue acusada de emplear a ex-niños soldados provenientes de Sierra Leona como una forma de reducir sus costos de operación.

Una ventaja estratégica

Las corporaciones privadas militares y de seguridad tienen en común el recurso a tecnologías de vanguardia, así como la creación de sistemas de vigilancia y procesamiento de la información que les permiten tener una ventaja estratégica sobre las empresas e instancias estatales que no pueden acceder a tales medios de producción. Muchas de ellas han sido fundadas y emplean a ex-militares con alta capacitación, lo que en principio ofrece tres tipos de ventajas: 1. ahorros al no pagar la formación de su personal de mayor preparación, mismo que puede transmitir su saber-hacer a menores costos que las formaciones disponibles en el mercado; 2. el cumplimiento adecuado de las tareas contratadas; 3. contar con relaciones en las esferas militares y gubernamentales que permiten la expansión de sus negocios; aunque el mercado es extenso, sin duda, los mayores contratos, tanto en monto como en duración, son los asignados por los gobiernos.

El auge del autoritarismo y la adopción de políticas militaristas y securitarias han creado un campo fértil para la expansión de las corporaciones militares y de seguridad. Tanto para los movimientos contestatarios como para el pensamiento crítico, el estudio de estos actores es de gran importancia, puesto que no será posible hacer frente y eventualmente desmontar los dispositivos de control social sin entender la fusión progresiva entre actividades militares y actividades de seguridad, así como el retiro paulatino del estado de tales tareas.

Guerra híbrida: orígenes y usos políticos

David Barrios Rodríguez

La guerra es, por lo tanto, no solo de carácter camaleónico, porque cambia su color en algún grado en cada caso particular, sino que también, en su conjunto, está en relación con las tendencias predominantes que hay en ella.
Carl Von Clausewitz

Invocando la "guerra híbrida"

La alocución "guerra híbrida" se ha puesto en boga en años recientes para describir fenómenos bastante diversos. Habiendo estado asociada en un primer momento a la combinación y actuación en el campo de batalla de fuerzas regulares y actores no estatales, posteriormente ha sido relacionada con ciberataques, tareas de espionaje, propaganda e información, campañas de desestabilización para deponer gobiernos (como ocurre con las llamadas Revoluciones de Colores) así como con el uso de herramientas no militares para promover extraterritorialmente los intereses de los Estados que las emplean (guerra económica, presión diplomática, formas de penetración cultural, entre otras). En el presente texto se hará una distinción entre los elementos conceptuales del término y su uso con fines propagandísticos, mismos que hacen parte de una disputa que tiene como principales protagonistas a Estados Unidos y Rusia, pero con ramificaciones a distintas regiones del planeta.

David Barrios forma parte de OLAG, donde se dedica a estudiar las formas de militarización contemporáneas, especialmente en América Latina y el Caribe.

Si bien el concepto fue acuñado en 2002 en la tesis de maestría de William J. Nemeth (Escuela Naval de Posgrado), su utilización por el General James Mattis y el Teniente Coronel Frank Hoffman (ambos de la Marina de Estados Unidos) durante los primeros años del lanzamiento de la llamada "Guerra contra el Terrorismo" lo colocó en el debate de los estrategas militares. Tratándose en verdad de una síntesis de varias aproximaciones, destacan las recuperaciones de la *Three Block War* (General Charles Krulak), guerra irrestricta o guerra más allá de los límites (Coroneles del Ejército Popular de Liberación chino Quang y Wang), guerra compuesta (Thomas H. Huber) o Guerra de Cuarta generación (William S. Lind). En ese momento, se hacía énfasis en la convergencia operacional de Estados con actores no estatales y se puntualizaban algunos de sus elementos: "La gama completa de diferentes modos de guerra, incluidas capacidades convencionales, tácticas y formaciones irregulares, actos terroristas que incluyen violencia y coerción indiscriminada, así como desorden criminal" (Hoffman, 2007). Es decir que se ponía de relieve la imbricación entre formas y actores de guerra convencional o tradicional y aquellos pertenecientes a las manifestaciones de la guerra irregular, en la que se volvía difusa la frontera de actuación entre unos y otros, aun en los niveles a ras del campo de batalla; además de incluir como elemento central las modalidades de actuación del "terrorismo" islámico.

Un elemento a resaltar sobre la noción, es que se han ido agregando y enfatizando algunos de sus componentes a partir de eventos concretos. La Guerra del Líbano de 2006 y

en especial la actuación de Hezbollah apoyada por los gobiernos de Siria e Irán, hizo que el planteamiento cobrara mayor notoriedad por los estragos que esta organización logró asestar a las Fuerzas de Defensa de Israel. En especial, fue destacada la combinación de formas de organización descentralizada, con la creación y utilización de infraestructura y armamento más sofisticado para llevar a cabo la campaña (misiles anti tanque y anti buque, sistemas avanzados de comunicación, creación de túneles y refugios antiaéreos), al mismo tiempo que se llevaron a cabo ataques sorpresa y fue establecida una exitosa campaña mediática promoviendo los resultados de la estrategia de Hezbollah. En esta vertiente, se destacó el hecho de que en una confrontación asimétrica, un actor armado de menor calado, aprovechara avances tecnológicos-informáticos, así como el apoyo de formaciones estatales para ofrecer batalla a uno de los ejércitos más poderosos de su región.

Guerra de "nuevo tipo"

A partir de 2014, se generalizó la enunciación como "nuevo tipo" de guerra, con posterioridad a la anexión de Crimea por Rusia. Desde entonces la acepción incorporó con mayor fuerza la disputa en el terreno de la información a partir de eventos relacionados con la difusión de noticias falsas (especialmente en las redes sociales), propaganda, o guerra psicológica; lo cual da cuenta de otro rasgo que ha sido subrayado sobre estos escenarios: la centralidad que adquiere la población como objetivo de estas operaciones en la medida en que se busca crear descontento social o generar adversarios al interior de los Estados rivales.

Desde el otro extremo del tablero, el interés de Rusia en el concepto surgió de la teorización producida desde Occidente y que a partir de ésta se tradujo al ruso como *gibridnaya voyna*. El objetivo de dicha incorporación habría sido interpretarla a la luz su propio contexto, más que asumirla de manera mecánica (Fridman, 2017). Esto hizo que fueran recuperados los aportes en torno a la "guerra de subversión" (*myatezh voyna*), propuesta desde la década de los años sesenta del Siglo XX, por un ex Coronel del Ejército imperial ruso (y anticomunista furibundo) Evgeny Messner. Bajo esa conceptualización, se refirió a las actividades de la URSS y China respecto a las "democracias" occidentales y los países del Tercer Mundo en el marco de la Guerra Fría. Dicho planteamiento consideraba ya la creciente fusión entre la guerra regular e irregular (en un sentido amplio y no fundamentalmente operacional), así como la preeminencia de la guerra psicológica y la importancia de la población en los conflictos venideros:

> Mientras que el concepto occidental de guerra híbrida se centra principalmente en actividades tácticas y operativas militares 'dirigidas y coordinadas dentro del espacio de batalla principal para lograr efectos sinérgicos', la *gibridnaya voyna* rusa gira en torno a ideas más amplias e 'involucra todas las esferas de la vida pública: política, economía, desarrollo social, cultura'... esta idea está fuertemente basada en el concepto de 'guerra de subversión' de Messner (Fridman, 2017: 43)

Otro elemento a considerar es que, mientras la definición surgida en Estados Unidos pone especial énfasis en la actuación de actores no estatales, las preocupaciones de los académicos rusos que han recuperado a Messner, se centran en los esfuerzos de Estados por socavar gobiernos y sociedades enemigas. En esa línea de ideas es que Andrew Korybko ha establecido que la guerra no convencional y las Revoluciones de Colores son los dos componentes de las guerras híbridas actuales, en este caso entendidas como un método novedoso de guerra indirecta por parte de Estados Unidos (Korybko, 2015).

Lo señalado hasta ahora nos permite observar que lo que se presenta como "guerra híbrida" no es en realidad una forma novedosa de en-

frentar a los enemigos ya que la fusión entre la guerra tradicional o convencional y la de tipo irregular, así como la incorporación de mecanismos no estrictamente militares, resultan prácticas que se actualizan, pero que pueden ser rastreadas desde tiempos inmemoriales. A las objeciones que se han planteado al término, relacionadas con lo hasta ahora expuesto, considero pertinente agregar que la propia conceptualización nos permite observar el carácter performativo de la enemistad contemporánea, de la redefinición constante de amenazas.

El *intervallum* de las guerras actuales

La oscilación entre estrategias tradicionales e irregulares para hacer la guerra es en la actualidad parte constitutiva de la doctrina militar de Estados Unidos (JCOS, 2017) y como expresan las aproximaciones mencionadas al comienzo de este texto, otras características –como la proliferación de guerras internas, la generalización de las operaciones especiales, el resurgimiento y generalización de actores armados no estatales, la importancia que han adquirido las tareas de información y propaganda, o el papel preponderante que tienen las poblaciones civiles en los conflictos actuales– resultan elementos que, operando de manera conjunta, acompañan a nuestras sociedades desde las últimas décadas del siglo pasado.

Es por ello posible afirmar que, tanto Rusia como Estados Unidos, apelan al carácter híbrido de las amenazas y la guerra como una manera de describir al enemigo sin llevar a cabo una autodescripción de su proceder (Ssorin-Chaikov, 2018), eludiendo incluso retomar formalmente el concepto en sus doctrinas, aunque en su repertorio existen formulaciones que bien podrían ponerse en relación o albergar dicha noción. Tal es el caso tanto de las "guerras de nueva generación" o "nuevo tipo de guerra" (Thomas, 2017; Gerasimov, 2019), como la "dominación de espectro completo" (JCOS, 2000).

Si prestamos atención a los elementos señalados, éstos han estado presentes en otros momentos de la historia, e inclusive formaron parte de los conflictos bélicos durante el Siglo XX, incumpliendo con ello las normatividades acordadas para llevar a cabo la guerra. Lo que ocurre es que algunos de estos rasgos se generalizaron con el lanzamiento de la "Guerra contra el Terrorismo". Por ejemplo, a través de las incursiones militares en países sin que haya de por medio declaraciones formales de inicio de hostilidades, la implementación de centros de detención como Abu Grahib o Guantánamo, el incremento exponencial de las Operaciones Especiales o la proliferación del uso de vehículos no tripulados (UAV) que han permitido llevar a cabo ataques a distancia, así como asesinatos encubiertos. Es por ello que, al mismo tiempo que se ha instaurado un "espacio panóptico global" (Gusterson, 2016) a través de las tecnologías de vigilancia o de la generalización del uso de drones, no se percibe una correlativa adaptación de las reglas del juego, sino que distintos actores disponen ahora de esos mismos mecanismos de intervención y ataque.

Lo característico de la época en que vivimos es que los conflictos contemporáneos se desarrollan en una zona gris entre la paz y la guerra (Almäng, 2019). Ese intersticio o zona de indefinición abarca aspectos espaciales, temporales y, por último, pero no menos importante, posibilita la producción de sentidos sociales en los que se diluye el ámbito civil y militar, así como la experiencia de conflictividad bélica que se normaliza en la cotidianidad. Entre otras cosas, esto obedece al resquebrajamiento del orden interestatal y su legitimidad, si bien remite a una experiencia acotada a un par de centurias (a lo sumo) y que en amplias regiones de África, Asia y América Latina y el Caribe tuvo un carácter claramente distinto a la prédica Occidental.

Lo que se amplifica es la conformación de formas de conflictividad permanentes detrás de las cuales es notoria una militarización generalizada y que penetra todos los ámbitos de la vida social, al mismo tiempo que es relanza-

da la disputa de porciones del planeta, como ocurrió durante la Guerra Fría. En esta dinámica tiene un lugar destacado la difusión de propaganda que abarca aspectos diversos y que en lo sucesivo no hará sino profundizarse. Entre los elementos que de manera cualitativa actualizan fenómenos ya presentes, destacan innovaciones tecnológicas y en especial la centralidad/dependencia que nuestras sociedades comportan respecto al mundo informático y la internet.

Por último, es preciso señalar que la capacidad de llevar adelante una estrategia que al mismo tiempo se desarrolle en ámbitos de información, inteligencia, operaciones especiales, propaganda, formas de guerra económica y penetración cultural, e incluya la activación o utilización de actores armados no estatales o paramilitares (*proxy wars*) está acotada a los Estados en la disputa hegemónica.

En lo que respecta a América Latina y el Caribe, en donde también se ha importado este concepto de moda, no debemos perder de vista que las estrategias de desestabilización y socavamiento de nuestras sociedades están presentes desde hace décadas, si bien sus mecanismos de intervención se actualizan y perfeccionan. Esto incluye, tanto el *aggiornamiento* de la contienda en el terreno de la propaganda y la información (que incluye ahora las redes sociales), como el recurrir a fenómenos diversos de privatización de la seguridad y la violencia.

Fuentes consultadas

Almäng, J., 2019, "War, vagueness and hybrid war", *Defence Studies*, Routledge, 1–16.

Fridman, Ofer, 2017, "Hybrid Warfare or Gibridnaya Voyna?", The RUSI Journal, 162:1, 42-49

Gerasimov, Valery (traducido del ruso por Harold Orenstein), 2019, "2018 Presentation to the General Staff Academy «Thoughts on Future Military Conflict»", *Military Review online exclusive*, enero.

Gusterson H, 2016, *Drone: Remote Control Warfare*, Cambridge, Massachusetts, MIT Press.

Hoffman, Frank, 2007, *Conflict in the 21st Century: The rise of hybrid wars*, Potomac Institute for policy studies, Virginia.

Joint Chief of Staff, 2017, *Joint Publication I Doctrine for the Armed Forces of the United States*, Washington.

----------, 2000, *Joint Vision 2020*, Washington.

Korybko, Andrew, 2015, *Hybrid Wars: The indirect adaptative approach to regime change*, Institute for Strategic Studies and Predictions, Moscú.

Nikolai Ssorin-Chaikov, 2018, "Hybrid Peace: Ethnographies of War", *Annual Review of Anthropology*.

Nemeth, William J., 2002, "Future war and Chechnya : a case for hybrid warfare", Naval Postgraduate School Monterey, California.

Thomas, Timothy (Teniente Coronel retirado), 2017, "The Evolving Nature of Russia's Way of War", *Military Review* (julio-agosto), Kansas.

La ciberguerra en la disputa intercapitalista

Adriana Franco

El ciberespacio se ha configurado como un dominio estratégico tanto para la reproducción del sistema capitalista como para la resistencia. Así, a pesar de que la génesis de este espacio se dio en las entrañas del sujeto hegemónico –Estados Unidos–, ciertos actores y acciones han puesto en riesgo el dominio estadounidense sobre este medio. El hackeo es la principal amenaza en este espacio, debido a que es una actividad que busca eludir la vigilancia del sistema, oponerse a las normas establecidas, quebrantar las estructuras de poder, así como mantener y potenciar la capacidad de actuar en este dominio.

El control de internet

Internet –que está formado por un conjunto de redes, cables, servidores, sistemas de comunicación, entre otros– es la base material del ciberespacios. A pesar de que este es un medio asequible para quienes tienen los recursos económicos y tecnológicos para incursionar en él, es un campo que está coordinado por un sector privado denominado Internet Corporation for Assigned Names and Numbers (ICANN), el cual favorece a Estados Unidos, ya que "Washington conserva la autoridad de supervisión y su Comité Asesor Gubernamental, compuesto por delegados de otras naciones, no tiene poderes reales" (Cukier, 2005: 7). Asimismo, en la red de redes hay un dominio de nombres para determinar la ubicación de los servidores, un código para que las máquinas puedan ser reconocidas por las demás, servidores matrices y estándares técnicos que regulan el tráfico de datos (Cukier, 2005: 8-9).

De acuerdo con ICANN, actualmente hay 13 servidores matriz. Diez de estos están controlados por Estados Unidos: cinco por empresas (dos por Verisign, uno por Cogent Communications, otro por ICANN y uno más por Internet System Consortium Inc.), dos por universidades (University of Southern California y University of Maryland) y tres por agencias o departamentos (Departamento de Defensa, Ames Research Center de la NASA y el Laboratorio de Investigación del Ejército). Los demás están regulados por Netnod, Suecia; el Centro de Coordinación de Redes IP europeas, Ámsterdam; y otro por Wide Project, Japón.

Los ciberataques como reposicionamiento a la asimetría de poder

En el ciberespacio las y los enemigos son los hackers. Un ciberataque implica la generación de un código que daña las estructuras y sistemas computacionales del enemigo. Para Estados Unidos, el ciberespacio es un medio lleno de incertidumbre que se ha configurado como un dominio de competencia con enemigos altamente calificados. (Nieto 2014: 105). Por esta razón, en 2009, el Departamento de Defensa creó un subcomando conjunto de combate para hacer frente a las amenazas de los hackers: CYBERCOM, el cual está vinculado con la Agencia Nacional de Seguridad (NSA) (Nieto 2014: 98).

Adriana Franco es maestra en Estudios de Asia y África, integrante de OLAG y Secretaria Técnica de Investigación del Centro de Relaciones Internacionales de la UNAM.

El ciberespacio es el quinto dominio de la guerra (Desforges, 2014: 75-76). El general Paul M. Nakasone, comandante del CYBERCOM, considera que su control es fundamental para la hegemonía estadounidense, debido a que en este espacio sus adversarios pueden realizar ataques en contra de sus intereses estratégicos dificultando la posibilidad de una respuesta directa (Nakasone, 2019). Un ciberataque puede afectar esencialmente tres elementos: las tecnologías de la información, lo cual atentaría contra las capacidades combativas en tierra de las fuerzas armadas; las tecnologías operacionales, que pueden dañar los software y hardware desde los cuales opera la infraestructura militar y económica del sujeto hegemónico; y las plataformas y sistemas de armas (William, 2018), incluyendo las nucleares. El ejemplo más significativo de un ataque de este tipo se dio en 2010 con *Stuxnet*, el malware con el que se dañaron las centrifugadoras de Natanz en Irán (Bommakanti, 2018: 3-7).

Este ciberataque fue realizado por la Agencia de Nacional Seguridad (NSA) de EE.UU. y por la Unidad Secreta Israelí 8200. El programa para desarrollar el malware inició en 2007 y su nombre era "Olympic Games" (Gates, 2012). De acuerdo con los análisis de seguridad que se han hecho, el ataque en Natanz entró en el sistema de control industrial de las instalaciones infectando computadoras y sistemas en el complejo de enriquecimiento de uranio, lo que generó daños a las centrifugadoras. Antes de 2010, el Departamento de Defensa estadounidense ya había demostrado la posibilidad de acceder a computadoras que controlaban redes eléctricas con el ejercicio "Eligible Receiver". Sin embargo, *Stuxnet* logró superar el air-gapping[1] y entrar a una red cerrada (Porche, Sollinger, McKay, 2011: 1).

Stuxnet es considerada la primera arma digital y a partir de su utilización el ciberespacio se ha convertido en un dominio de suma importancia para la disputa intercapitalista, pero también para los esfuerzos por eliminar

1 Es una estrategia que implica el desvinculamiento de una red de computadoras de un circuito más amplio por medio del cual se podría realizar un ataque (Bommakanti, 2018: 3-7).

Servidores matriz en el mundo

País	*Control*	*Nombre*
Estados Unidos	Empresa	Verisign (2) Cogent Communications ICANN System Consortium Inc.
	Universidades	University of Southern California University of Maryland
	Agencias o Departamentos	Departamento de Defensa Ames Research Center de la NASA Laboratorio de Investigación del Ejército
Suecia	Organización de infraestructura de internet	Netnod
Países Bajos	Organización de infraestructura de internet	Centro de Coordinación de Redes IP Europeas
Japón	Institutos y universidades	Wide Project (Keio University, Tokyo Institute of Technology, The University of Tokyo)

Cuadro realizado con base en información de ICANN

el sistema de vigilancia, control y explotación en el que vivimos. De acuerdo con informes de la Corporación de Investigación y Desarrollo (RAND), China y Rusia están destinando cada vez más recursos para la guerra de información con Occidente. Ese mismo reporte considera que a pesar de que estas herramientas y estrategias están en un periodo inicial, ya han generado efectos negativos significativos para la hegemonía estadounidense (Mazarr & Demus, 2019).

El ciberespacio en la disputa intercapitalista: capacidades y estrategias

La NSA y el CYBERCOM fueron unidos desde el nacimiento del segundo. Sin embargo, en los últimos años, las funciones del CYBERCOM se han vinculado más con el ataque a redes enemigas para alcanzar metas militares y no tanto para desarrollar misiones de espionaje (Greenberg, 2018). De acuerdo con Nakasone, los principales Estados que ponen en riesgo la ciberseguridad estadounidense son Rusia, China, Irán y Corea del Norte. Sin embargo, quienes cuentan con mejores capacidades y estrategias son los dos primeros.

El enfoque central del gobierno chino en este ámbito es mantener una presencia significativa para garantizar su seguridad nacional, preservar la estabilidad social y asegurar la información crítica, concentrándose más en el control interno de su población que en algún ataque al exterior (Jinghua, 2019). No obstante, las capacidades cibernéticas que China está desarrollando podrían reducir las asimetrías en el campo físico de batalla. Asimismo, China tiene la PLA's Unit 61398, que es la oficina central militar de operaciones de red cibernética del gobierno. China ha sido identificada como una de las principales fuentes de tráfico de ciberataques, empero, esto no significa que desde esta espacio se originen las irrupciones, ya que las y los hackers pueden enrutar el tráfico en otras vías para atribuir la procedencia del ataque a un espacio geográfico diferente (Richards, 2014: 46-48).

Por su parte, Rusia no utiliza el concepto ciberguerra, sino guerra de información, el cual incluye operaciones de redes computacionales, de información, psicológicas, así como la guerra electrónica. Este gobierno utilizó sus capacidades cibernéticas como una fuerza habilitadora en Georgia y Ucrania (Connell & Vogler, 2016). Asimismo, Rusia tiene una unidad de elite militar que se encarga de llevar a cabo operaciones de espionaje de alto riesgo en el ciberespacio (Oliphant, 2018) y en los últimos años, el gobierno ruso ha estado reclutando programadores con el objetivo de crear un equipo de elite de hackers (Kramer, 2016).

Por esta razón, EE.UU. está desarrollando tecnologías para no permitir que sus adversarios logren sus objetivos en el ciberespacio, por medio de estrategias defensivas y capacitación especializada para oficiales en Fort Gordon (Sheftick, 2019). Una de las principales preocupaciones de EE.UU. es que gran parte de su infraestructura y economía se basa en la digitalización y autonomización, lo que hace que su régimen sea vulnerable en las dinámicas del ciberespacio. Durante la administración Trump, se señaló que el CYBERCOM había logrado entrar en las instalaciones eléctricas de Rusia con un malware capaz de interrumpir su red eléctrica. Rusia mencionó que sus sistemas eran inmunes a esos ataques, pero que si Estados Unidos intervenía en su infraestructura esto generaría una guerra cibernética entre ambos Estados (Sanger & Perlroth 2019).

En términos generales, el ciberespacio es un medio que permite reducir asimetrías, como en el caso de China, pero también es un dominio que posibilita la reproducción hegemónica liderada por EE.UU. Actualmente, el país con mejores capacidades en este espacio es EE.UU., sin embargo, Rusia y China están invirtiendo tiempo y dinero para mejorar su competencia en este medio. A pesar de que en las narrativas securitarias estadounidenses, se resalta la amenaza que representa China para la seguridad nacional del país, el Estado con el que ha tenido mayores encuentros en este domino es Rusia.

El ciberespacio para la creación de mundos alternativos

El ciberespacio no sólo es un dominio ocupado por las grandes potencias, también es un medio en el cual diversos actores sociales tiene capacidad de actuación y movimiento. Asimismo, no todas las agresiones van dirigidas a infraestructura de redes y comunicaciones, los ciberataques también pueden manipular a la población y modificar sus opiniones y decisiones a través de campañas en las cuales se difundan rumores u otras ideas en las redes o medios de comunicación. Entonces, el control del ciberespacio puede garantizar la reproducción hegemónica –a partir de la difusión de los valores e ideas capitalistas– o transformar las relaciones sociales en las que se sustenta el sistema dominante.

El poder económico y tecnológico de los Estados ha hecho que estos actores sean los ejes centrales en la disputa cibernética, sin embargo, figuras no estatales también han desafiado al sujeto hegemónico a través de la filtración de documentos estratégicos, como lo ejemplifican los casos de Edward Snowden, Julian Assange, Wikileaks y Anonymous. La principal amenaza a la reproducción sistémica no viene de los Estados sino de los individuos o colectivos que han incursionado e irrumpido este espacio a través del hackeo.

"Hackear un sistema requiere conocer sus normas mejor que la gente que lo ha creado o que lo gestiona, y vulnerar la distancia que exista entre el funcionamiento que esa gente haya pretendido darle al sistema y el funcionamiento que muestra el sistema de verdad, o que alguien puede hacer que muestre" (Snowden, 2019: 52). Así, aunque aún nos hacen falta herramientas y estrategias, el ciberespacio es un dominio que la sociedad puede utilizar para modificar la hegemonía en el ámbito de la reproducción, es decir, la ocupación y apropiación del ciberespacio pueden ayudarnos a romper las relaciones de poder imperante por medio de la inhabilitación de los sistemas que garantizan el predominio de los sujetos que reproducen la hegemonía, de la transmisión de perspectivas de vida diferentes, de la actuación en colectivo y, por lo tanto, de la transformación de las relaciones sociales dominantes para crear un mundo diferente.

Fuentes consultadas

Bommakanti, K. 2018 "The Impact of Cyber Warfare on Nuclear Deterrence: A Conceptual and Empirical Overview", *ORF Issue Brief* 266: 1-15.

Connell, M. & Vogler, S. 2016 *Russia's Approach to Cyber Warfare,* CNA Analysis & Solutions.

Cukier, K. N. 2005 "Who Will Control the Internet? Washington Battles the World", *Foreign Affairs* 84, 6: 7-13.

Greenberg, A. 2018 "The Next NSA Chief Is More Used to Cyberwar Than Spy Games" *The Wired*.

Hérodote 2014 *Cyberspace: enjeux géopolitiques,* no. 152-153, primer y segundo trimestre.

Jinghua, L. 2019 "What Are China's Cyber Capabilities and Intentions?" *Carnegie Endowment for International Peace*.

The New York Times: Kramer, Andre E. 2016 "How Russia Recruited Elite Hackers for Its Cyberwar" / Sanger, David E. & Perlroth Nicole (2019) "U.S. Escalates Online Attacks on Russia's Power Grid".

RAND Corporation: Porche, I. R., Sollinger, J. M., McKay, S. 2011 *A Cyberworm that Knows No Boundaries* / Mazarr & Demus 2019 "Hostile Social Manipulation by Russia and China a Growing but Poorly Understood Threat".

Nakasone, P. M. 2019 "A Cyber Force for Persistent Operations" *Joint Force Quarterly* 92: 10-14.

Oliphant, R. 2018 "What is the Unit 26165, Russia's elite military hacking centre?" *The Telegraph*.

Richards, J. 2014 *Cyber-War: The Anatomy of the Global Security Threat,* Palgrave Macmillan.

Sheftick, Gary 2019 "Cyber Teams Safeguard National Security" *U.S. Department of Defense*.

Snowden, Edward 2019 *Vigilancia permanente,* Planeta.

Aplicaciones militares de la inteligencia artificial

Ana Katia Rodríguez Pérez

La lucha por la superioridad tecnológica juega un papel fundamental en la disputa por la hegemonía mundial entre Estados Unidos, China y Rusia, en donde la inteligencia artificial (IA), el *machine learning* y la conducción autónoma se han vuelto campos estratégicos para la supremacía en la guerra. Al obtener el control de la tecnología se define la capacidad hegemónica de los capitales y de los Estados, siendo una herramienta esencial de la competencia. De esta manera, la búsqueda por la superioridad en inteligencia artificial está alimentando una carrera armamentista en la que se busca desarrollar aplicaciones tecnológicas que confieran una ventaja sobre adversarios y competidores en diversos dominios de la guerra (Hoadley, 2019: 34).

La primera definición de inteligencia artificial fue acuñada por John McCarthy en 1956, quien a partir de un proyecto denominado *Dartmouth Summer Research Project on Artificial Intelligence* buscó desarrollar varios conceptos alrededor de lo que él y sus colaboradores consideraban que eran *thinking machines* o máquinas pensantes. Actualmente, las definiciones se centran en que la IA es un sub-campo de la informática que busca aprender cómo es que las máquinas pueden imitar la inteligencia humana (Marr, 2018). En este sentido, la inteligencia artificial es la búsqueda por realizar tareas generalmente reservadas a la cognición humana, como lo son reconocer patrones, predecir resultados y tomar decisiones complejas (Lee, 2018).

Sin embargo, cabe señalar que es una tecnología que procesa una gran cantidad de información sobre un campo específico, con el fin de tomar una decisión en un caso determinado a partir de un objetivo particular. Es decir, la inteligencia artificial funciona en dominios únicos, por lo que no es capaz de generalizar la información o de tener sentido común. Por ello, donde la IA puede tener dificultades es cuando se encuentra con una situación más allá de su experiencia o modelo aprendido, puesto que puede tener problemas para pensar más allá de su base de datos o programación. Además, la IA necesita un objetivo para trabajar, por lo que se vuelve necesario mantener una colaboración entre humano y máquina para llevar a cabo sus tareas. En este modelo de trabajo en equipo, los humanos determinan los objetivos y proporcionan la creatividad, mientras que la IA brinda experiencia autodidacta, habilidades de pronóstico y eficacia (Cain, 2017: 33).

Para lograr su objetivo es necesario el uso de algoritmos, los cuales permiten que las computadoras perciban e interpreten el mundo para tomar decisiones por sí mismas. Ello se logró a raíz del desarrollo del *deep learning*, un modelo inspirado en el cerebro humano, donde las redes del sistema están programadas por seres humanos a partir de grandes cantidades de datos etiquetados. De este modo, utilizan lo que han aprendido para seleccionar matemáticamente ciertos datos, reconocer patrones dentro de la vasta cantidad de información y desarrollar las tareas de manera

Ana Katia Rodríguez tiene una Licenciatura en Relaciones Internacionales de la Facultad de Ciencias Políticas y Sociales (FCPyS) de la UNAM y es miembro del proyecto PAPIIT Economía y guerra en el siglo XXI de OLAG (UNAM).

más eficiente (Lee, 2018). Para realizar sus análisis, se requiere de grandes conjuntos de datos para programarlos y una gran capacidad computacional para procesarlos, de forma que la información, la creación de infraestructura y el desarrollo de algoritmos se vuelven factores estratégicos para la guerra (The Economist, 2018a).

En este sentido, un grupo considerable de expertos señala que la IA tiene el potencial de cambiar la naturaleza misma de la guerra (The Economist, 2018a). Los defensores de esta posición argumentan que el mundo ha pasado de la era industrial de la guerra a la era de la información, en la que la recopilación, el análisis y la difusión de datos será el aspecto más importante en las operaciones de combate (Hoadley, 2019: 35). En la búsqueda por mantener la superioridad tecnológica, cobra relevancia la capacidad de reunir e interpretar información en tiempo real, en donde la supremacía en este campo se traduce en poder de combate a partir de una mejor reacción ante cualquier situación que se pueda enfrentar (Ceceña, 2006: 18). Es así como Estados Unidos, China y Rusia han comenzado a desarrollar avances en inteligencia artificial con aplicaciones militares.

Con IA: decisiones y respuestas más rápidas

En 2014, el Pentágono anunció la *Third Offset Strategy*, la cual busca recuperar una ventaja militar por medio del aprovechamiento de una gama de tecnologías, incluidas la inteligencia artificial, sistemas autónomos, la robótica y el *big data,* mediante las cuales pueda actuar de manera más rápida y efectiva (The Economist, 2018b). Frente a esto, China lanzó en 2017 su *New Generation of Artificial Intelligence Development Plan* que incorpora a la IA como la tecnología transformadora que sustentará los poderes económico y militar, utilizando una estrategia de fusión militar-civil. Por su parte, Vladimir Putin estableció que la inteligencia artificial es el futuro y quien se convierta en el líder en esta esfera, se convertirá en el gobernante del mundo (The Economist, 2018a). A pesar de que Estados Unidos cuenta con una ventaja tecnológica considerable, China está empezando a posicionarse como un competidor real frente a los avances estadounidenses, mientras que Rusia continúa rezagado en esta disputa.

Así pues, la IA está siendo incorporada a la guerra a través de aplicaciones relacionadas con operaciones de inteligencia, vigilancia y reconocimiento, así como en logística y procesos de toma de decisiones, operaciones del ciberespacio y de información, comando y control, vehículos semiautónomos y autónomos y sistemas de armas letales autónomos (LAWS, por sus siglas en inglés) (Hoadley, 2019: 9). Aunado a ello, el impacto potencial que la IA tendrá en el futuro de la guerra estará en función de diversos factores, incluidos la tasa de inversión comercial, el impulso para competir con rivales internacionales, la capacidad de la comunidad de investigación para avanzar en el estado de la IA, la actitud general de los militares hacia su aplicación en las operaciones de guerra y el desarrollo de conceptos específicos para su empleo en combate (Hoadley, 2019: 34).

De esta manera, a partir del desarrollo e implementación de esta tecnología, un Estado podrá obtener una ventaja informativa y temporal con la cual tendrá una mejor comprensión de los factores que afectan un entorno estratégico y podrá generar respuestas de manera casi instantánea frente a las operaciones de sus adversarios. La capacidad de automatizar el análisis de datos a través de múltiples dominios, les permitirá recortar el proceso de toma de decisiones y facilitará la capacidad de respuesta en eventos en los que los humanos no puedan reaccionar lo suficientemente rápido, como puede ser el caso de un ataque cibernético o el despliegue de misiles supersónicos. En particular, en la guerra cibernética se hace uso de sistemas de inteligencia artificial a partir de la búsqueda de vulnerabilidades en la red para atacar, por lo que el diseño de softwares con habilidades de autonomía pueden aprender de los ataques para advertir

a los planificadores cuando las suposiciones ya no son válidas o si hay una oportunidad para mejorar los planes y generar una mejor respuesta (The Economist, 2018a).

Vehículos y armas autónomos

Por su parte, los vehículos semiautónomos y autónomos son otro campo en el que se puede aplicar la IA en la guerra, en donde los vehículos pueden percibir el entorno, reconocer obstáculos, fusionar datos, planificar la navegación, comunicarse con otros vehículos, interferir amenazas electrónicas y portar armas (Hoadley, 2019: 12-13). Igualmente, el empleo de la inteligencia artificial en este ámbito ha introducido el despliegue de vehículos autónomos de manera simultánea, lo que comúnmente es conocido como enjambre o *swarm*, con el fin de abrumar a las defensas del enemigo y generar una mayor coordinación, inteligencia y velocidad en la guerra (The Economist, 2018a). En el caso de los sistemas de armas letales autónomos o "robots asesinos", la IA permitirá la creación de sistemas capaces de identificar un objetivo y tomar decisiones de manera independiente sobre si atacar y destruir a dicho enemigo. No obstante, su aplicación ha presentado importantes problemas éticos, legales, políticos y prácticos en los que se cuestiona la autonomía de esta innovación y su capacidad de matar.

De este modo, el surgimiento de la inteligencia artificial ha implicado el desarrollo de múltiples innovaciones que han permitido su aplicación en diferentes ámbitos militares, teniendo un impacto importante en el reposicionamiento tecnológico necesario para la supremacía en la guerra. Sin embargo, su aplicación sugiere ciertos cuestionamientos, especialmente sobre la forma en la que pueden librarse los conflictos en un futuro y sobre cómo los humanos deben de interactuar con máquinas que son capaces de tener diversos grados de autonomía. Así, se presenta un ambiente de incertidumbre en el cual es posible que se generen riesgos vinculados a la capacidad de las máquinas de funcionar sin supervisión humana, llegando a amenazar todas las condiciones de vida.

Fuentes consultadas

Cain, C. B. (2017), "*Go* and Artificial Intelligence: Potential for Strategic Decision-Making" en Samuel R. White Jr., *Closer Than You Think: The Implications of the Third Offset Strategy for the U.S. Army*, Estados Unidos: Strategic Studies Institute y U.S. Army War College Press.

Ceceña, A. E. (2006), "Sujetizando el *objeto de estudio*, o de la subversión epistemológica como emancipación" en Ana Esther Ceceña (comp.), *Los desafíos de las emancipaciones en un contexto militarizado*, Buenos Aires: CLACSO.

Hoadley, D. S. (2019), *Artificial Intelligence and National Security,* Estados Unidos: Congressional Research Service.

Lee, Kai-Fu (2018), "The Four Waves of A.I." [en línea], *Fortune,* 22 de octubre. Disponible en: https://bit.ly/2nSqFnX [Consultado: 13 de agosto de 2019].

Marr, B. (2018), "The Key Definitions of Artificial Intelligence (AI) That Explains Its Importance" [en línea], *Forbes*, 14 de feb rero. Disponible en: https://bit.ly/2mg4Qyx [Consultado: 11 de agosto de 2019].

The Economist (2018a), "War at hyperspeed. Getting to grips with military robotics. Autonomous robots and swarms will change the nature of warfare" [en línea], *The Economist*, 27 de enero. Disponible en: https://econ.st/2mpGUZr [Consultado: 20 de agosto de 2019].

The Economist (2018b), "The new battlegrounds. The Future of war" [en línea], *The Economist*, 25 de enero. Disponible en: https://econ.st/2ng8vwn [Consultado: 20 de agosto de 2019].

Las superarmas del futuro

Yetiani Romero Rebollo

Las innovaciones tecnológicas han venido a cambiar las reglas de la guerra desde la propia existencia de la humanidad. Estos avances también han producido efectos cada vez más destructivos hasta llegar a los sistemas de armas nucleares en el siglo pasado, con la capacidad de destruir a la humanidad entera.

En la actualidad existen nuevos desarrollos tecnológicos en el campo de las armas, algunas de las cuales tienen el potencial de cambiar el curso de la guerra. Las principales nuevas armas en las que las grandes potencias militares han puesto todos sus esfuerzos son:

A) Armas de energía directa (directed energy wepons). También conocidas como armas láser, este tipo de arma produce energía electromagnética concentrada a partir del uso del espectro electromagnético, lanzando un rayo de energía concentrado (láser).

Existen dos tipos principales:

1. Los laser de alta energía (High Energy Lasers, HELs), que producen rayos de luz monocromática, los cuales concentran energía en un punto designado;
2. Los de microondas de alto poder (High Powered Microwaves, HPMs), que usan la electricidad para hacer funcionar un generador que emite pulsos de radiación microonda.

Las armas láser tienen el potencial de cambiar las reglas de la guerra en dos sentidos:

1. Al tratarse básicamente de rayos de luz, pueden viajar a la velocidad de la luz (300,000 km/s), lo que siendo aplicado a la defensa antimisiles, convierte en ineficientes a los misiles balísticos intercontinentales (ICBMs), pues estos podrían ser interceptados por el láser mucho antes de alcanzar su objetivo;
2. Los láser microondas pueden ser usados como armas electrónicas, es decir, pueden tener como objetivo dispositivos electrónicos (computadoras, centros de control, o cualquier dispositivo que funcione en el espectro electromagnético), los cuales quedarían temporal o permanentemente inservibles después de ser alcanzados por un pulso electromagnético.

El alcance de esta tecnología aún está en discusión, pues su desarrollo implica muchos desafíos técnicos como sus limitaciones relacionadas al clima y al comportamiento de la luz en la atmosfera.

B) Armas hipersónicas. Se trata de misiles capaces de alcanzar una velocidad hipersónica. La velocidad hipersónica debe distinguirse de otras categorías de velocidades relacionadas al sonido. Las velocidades sónicas se miden bajo el sistema de referencia mach, donde mach 1 significa una vez la velocidad del sonido (343,2 m/s aprox.), mach 2 son dos veces la velocidad del sonido, y así sucesivamente. Hay tres categorías: la velocidad subsónica, cercana pero menor a la del sonido (mach 1); la velocidad supersónica que está entre mach 1 y mach 5; y la velocidad hipersónica, mayor a mach 5 (cinco veces la velocidad del sonido).

Hay dos tipos de misiles hipersónicos: 1. Los Hypersonic glide vehicles (HGV), lanzados desde cohetes de misiles balísticos pero sin salir de la atmosfera y sin seguir una trayectoria balística. Caen hacia su objetivo desde altitudes de entre 40 y 100 km. Aunque no tienen un sistema

Yetiani Romero Rebollo es tesista de Estudios Latinoamericanos, Facultad de Filosofía y Letras de la Universidad Nacional Autónoma de México.

de propulsión propio, pueden tener pequeños propulsores que les permiten cambiar su trayectoria de manera impredecible, es decir, a diferencia de un misil balístico intercontinental (ICBM) que sigue una trayectoria balística (en forma de parábola) la cual no puede cambiar, el misil HGV puede cambiar de curso y objetivo en cualquier momento de su vuelo a voluntad del operador. 2. Misiles crucero hipersónicos (Hypersonic cruise missiles, HCM). Pueden ser lanzados desde tierra, aviones y barcos. Tienen un sistema de propulsión propio que acelera y mantiene la velocidad hipersónica además de cambiar su trayectoria en cualquier momento también de forma impredecible y puede volar a altitudes de entre 20 y 30 km.

El desarrollo de estas armas cambia totalmente la capacidad de disuasión, ya que debido a su velocidad y su capacidad de maniobra dejan completamente obsoletos los sistemas de defensa antimisiles, que no pueden interceptar, por ahora, un misil hipersónico. Además, un misil hipersónico puede llevar una carga explosiva convencional, múltiples cabezas nucleares e incluso no llevar carga explosiva y solo actuar con la energía cinética, la cual debido a su velocidad conserva una alta capacidad destructiva.

C) Cañón de riel electromagnético (Electromagnetic railgun). Es un cañón que usa energía electromagnética en lugar de propulsores explosivos para lanzar un proyectil. Funciona como un enorme circuito eléctrico hecho de metales conductivos. Al igual que los misiles hipersónicos, el interés en este tipo de arma es su velocidad. El cañón electromagnético es capaz de lanzar proyectiles a velocidades hipersónicas con una gran precisión. A diferencia de los misiles, estos proyectiles no tienen carga explosiva y su capacidad destructiva se las brinda la energía cinética que se alcanza con velocidades superiores a mach 5.

D) Armas cibernéticas. En general, un arma cibernética o digital es aquella capaz de dirigir un ataque cibernético contra sistemas computacionales con el uso de software maligno (malware). Un ataque cibernético comúnmente tiene como objetivo el robo o destrucción de información importante del adversario. Pero un ataque cibernético tiene un potencial más amplio, por ejemplo, un software (virus) puede estar diseñado para tomar control remoto de infraestructura crítica como una planta de energía, una red ferroviaria o el sistema de vigilancia de una ciudad, lo que implica un potencial destructivo ampliado contra el enemigo.

La disputa hegemónica en el campo de las armas

Las armas descritas aquí son desarrolladas por las grandes potencias militares, esencialmente Rusia, China y por supuesto Estados Unidos. El avance ruso y chino pone en entredicho la conservación de la superioridad militar estadounidense.

Respecto a las armas de energía directa, en Rusia se han desarrollado armas de microondas que pueden destruir sistemas de navegación en aviones tripulados y no tripulados y en misiles de precisión guiados. Además, Rusia tiene la capacidad de interrumpir señales GPS y destruir equipo de radio y satélites. China ha logrado construir un sistema láser no letal dirigido a individuos para neutralizarlos, además de tener sistemas capaces de destruir aviones no tripulados y satélites lanzando un láser desde la tierra. (Feickert, 2018: 14)

Pero la amenaza a la superioridad estadounidense es más clara respecto a los misiles hipersónicos. Hoy Rusia tiene en jaque los sistemas de defensa estadounidenses. En 2018 fueron presentados los misiles Kinzhal y Avengard, convirtiendo a Rusia en el primer país del mundo en contar con misiles hipersónicos entre su arsenal. El Kinzhal es un HCM que se lanza desde aviones de combate furtivos como el Mig-31 o el Su-57. Viaja a mach 10 y puede llevar carga nuclear o convencional. El Avengard, por su parte, es un HGV que puede alcanzar una velocidad de mach 20. China también ha logrado desarrollar un misil del tipo HGV que alcanza una velocidad de mach 10. Se sabe que desde 2014 los chinos trabajan en las armas hipersó-

nicas y recientemente se han realizado pruebas con un misil balístico que lleva el HGV mencionado (Lague, 2019). China, además, ha logrado construir un cañón de riel electromagnético el cual fue mostrado a inicios de 2019 montado sobre un barco (Sharman, 2019).

En lo referente a las armas cibernéticas, aunque hay varios países con capacidades de ataque cibernético, la disputa se da esencialmente entre Rusia y Estados Unidos. Se sabe que cada uno de estos países cuenta con una oficina en la que trabajan piratas informáticos, militares, hackers, programadores, etc., que dirigen ataques cibernéticos contra sus respectivos contrincantes. A pesar de esto, la mayoría de la información al respecto se mantiene en secreto y lo que sabemos se lo debemos en gran parte a filtraciones y reportes de prensa que ocurren después de un ataque cibernético (por ejemplo, recientemente contra Irán).

La permanencia de la superioridad estadounidense

A pesar de la disputa mencionada, Estados Unidos se mantiene como el actor hegemónico militar. Aunque pueda parecer que lleva un atraso respecto a sus rivales, mantiene inversiones y desarrollos en todos los campos tecnológicos, no solo enfocándose en el desarrollo de un arma o un sistema.

Su mayor avance es respecto a las armas láser. Actualmente cuenta con un arma láser basada en aire que puede derribar misiles y morteros. También cuenta con un sistema llamado Active Denial System, un arma no letal que neutraliza a individuos por medio del calor que genera el láser. Además, entre el 2020 y 2022 se incorporarán a sus arsenales varios sistemas de hasta 100 kilowatts capaces de destruir misiles, cohetes, artillería y aviones no tripulados.

En el campo de las armas hipersónicas es donde mantiene un gran retraso respecto a Rusia y China. Sin embargo, sus programas sobre tecnologías hipersónicas son múltiples, especialmente en la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA), que incluyen misiles y vehículos. Por otro lado, después de que Rusia dio a conocer sus misiles hipersónicos, Estados Unidos aceleró el paso con un contrato multimillonario con la empresa Lockheed Martin, la cual ha quedado encargada de construir armas hipersónicas en un tiempo relativamente corto. Recientemente, en junio de 2019, dio a conocer por primera vez el prototipo de un misil HCM, reduciendo la distancia respecto a Rusia y China (Macias, 2019)

Además, el interés en el cañón de riel electromagnético es fundamental en el desarrollo de programas relacionados a velocidades hipersónicas. Actualmente hay un contrato entre la marina (U.S. Navy) y la empresa BAE Systems, la cual ha desarrollado un cañón que está en fase de pruebas y se planea equiparlo en barcos para defensa aérea, alcanzando a China en el desarrollo de esta arma.

Finalmente, la Agencia Nacional de Seguridad (NSA) mantiene una oficina llamada Tailored Access Operations, la cual mantiene a un grupo de hackers que recolectan información, roban datos y monitorean comunicaciones. Aunque se sabe poco de esta oficina, gracias a Edward Snowden y al grupo de hackers conocido como The Shadow Brokers conocemos su existencia, además de las actividades y alcances que tienen sus programas informáticos, como su capacidad de espiar a cualquier individuo en cualquier lugar del planeta mediante dispositivos digitales.

Fuentes consultadas

Feickert, Andrew 2018 *U.S. Army Weapons-Related Directed Energy (DE) Programs: Backgrounds and Potential Issues for Congress* (Washington: Congressional Research Service) 30 pp.

Macias, Amanda 2019 “US successfully flies its newest hypersonic missile on B-52, Lockheed Martin says” *CNBC*

Lague, David 2019 “China leads U.S. on potent superfast missiles” *Reuters*

Sharman, Jon 2019 “Chinese navy ship equipped with futuristic hypersonic railgun that can fire at nearly 6,000 mph” *The Independent*

En el umbral de la autonomización de la guerra:

Los sistemas de armas autónomos

Cristóbal Reyes Núñez

De las múltiples transformaciones (tecnológicas y organizativas) por las que atraviesa la guerra en la actualidad, una de las más importantes es el desarrollo de los sistemas de armas autónomos (en adelante, SAAs).

El Departamento de defensa de Estados Unidos define a un SAA como aquel que "una vez activado, puede seleccionar y enfrentarse a objetivos sin mayor intervención por un operador humano".[1] Aunque algunos sistemas de armas semi-autónomos (como los drones o el "robot centinela" de Samsung ubicado en la frontera entre las dos Coreas) aún cuentan con operadores o supervisores humanos a distancia, es importante señalar que ya existen las condiciones tecnológicas para poner en funcionamiento sistemas de armas completamente autónomos y que algunas armas con funciones autónomas (como los sistemas de defensa aérea) se utilizan desde hace décadas.

La particularidad de los SAAs no es que se activen sin validación humana previa (pues algunas armas como las minas antipersonales se activan de manera automática) sino su capacidad para identificar objetivos y la autonomía decisional para enfrentarse a ellos.

Aunque hay armas que han tenido autonomía en algunas funciones (por ejemplo, de movimiento o de navegación) desde las décadas de 1960 y 1970, la aplicación de la inteligencia artificial (IA) en años recientes ha hecho posible que los SAAs puedan identificar objetivos, adaptarse a situaciones cambiantes y modificar sus planes a partir del análisis y procesamiento de grandes cantidades de datos. Esto representa un cambio cualitativo en las tecnologías de guerra.

A diferencia de lo que sucedía con las armas preexistentes (desde el arco y la flecha hasta los aviones de combate), para las cuales la efectividad del ataque dependía de la pericia del humano que las manipulaba, con los SAAs los procesos están automatizados y mejorarán paulatinamente sus capacidades, lo que permitirá superar ampliamente y en aspectos específicos las capacidades humanas. Los SAAs constituyen la cúspide del proceso de automatización, abstracción y autonomización en las actividades militares.

La utilización de los SAAs amenaza con cambiar significativamente la manera en que se hace la guerra. Además, por el conjunto de tecnologías involucradas en su desarrollo (IA, robótica, entre otras), estos sistemas son uno de los espacios más importantes de la carrera armamentista en curso y una de las áreas clave en la disputa por la supremacía militar.

1 https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf, p. 13.

Cristóbal Reyes Núñez es maestrante en el Posgrado en estudios latinoamericanos de la UNAM y miembro del Laboratorio de estudios sobre empresas transnacionales.

Condiciones tecnológicas clave para el desarrollo de los SAAs

La mutación tecnológica y organizativa que anuncian los SAAs ha sido posible por la digitalización de las armas y por la aplicación de los avances en tecnologías como las comunicaciones satelitales, la IA y la robótica en el campo de la guerra. De entre las múltiples condiciones que hacen que ya sea tecnológicamente posible el funcionamiento de los SAAs, destacan:

- Los sensores, cámaras, dispositivos electroópticos y otras tecnologías que sirven para recolectar enormes masas de datos variados a gran velocidad sobre las características y contexto del teatro de operaciones militares, los objetivos a atacar, etc.
- El software especializado y los algoritmos que analizan las enormes masas de datos para ordenarlas y hacerlas inteligibles.
- Los sistemas con IA mediante los cuales los sistemas de armas autónomos identifican objetivos, interpretan su entorno y contexto, se adaptan a situaciones cambiantes y "toman la decisión" de atacar sin validación inmediata por los humanos.[2]
- Los sistemas de comunicaciones e infraestructuras por los cuales se transmite la información entre los dispositivos interconectados.
- Los dispositivos físicos digitalizados (ruedas, motores, armas) que ejecutan las decisiones.

Todas ellas son tecnologías de vanguardia que pueden tener uso civil y militar. Las condiciones de la supremacía en el ámbito militar están estrechamente imbricadas con las que están en la base del liderazgo económico y la hegemonía mundial.

2 Más allá de las armas autónomas, la IA se utiliza ampliamente en los sistemas militares en tareas como el reconocimiento facial, la vigilancia y el análisis y procesamiento de datos. Como hemos dicho, lo que distingue el uso de la IA en las armas autónomas es la autonomía decisional.

Los sujetos detrás de los sistemas de armas autónomos

Como afirma Ana Esther Ceceña[3], el sujeto hegemónico en la sociedad contemporánea es un sujeto desdoblado, que aunque asume la forma diferenciada de estados y corporaciones, actúa bajo una lógica unitaria orientada a garantizar las condiciones materiales y simbólicas de la hegemonía. La carrera por la producción de SAAs es impulsada por la disputa geopolítica entre estados y por la competencia entre las corporaciones tecnológicas y armamentistas. Los SAAs son un instrumento de poder mediante el cual los estados y las grandes corporaciones buscan garantizar la acumulación incesante de ganancias y la concentración en el ejercicio del poder.

En un estudio de 2017, el Instituto de Estudios para la Paz de Estocolmo (SIPRI, por sus siglas en inglés) identificó que en el mundo ya existen varios sistemas militares con funciones autónomas: 277 sistemas con autonomía de movimiento; 154 con capacidad para identificar objetivos de manera autónoma; 56 sistemas con "autonomía para la inteligencia" (análisis y procesamiento de información, planeación a partir de la información analizada, generación de mapas, evaluación de amenazas); y 55 sistemas con interoperabilidad autónoma (sistemas de armas capaces de ejecutar misiones o tareas en cooperación con otros sistemas).

En el mismo estudio, SIPRI registró los siguientes sistemas de armas con múltiples funciones autónomas que están en funcionamiento: 56 sistemas de defensa aérea; 17 "sistemas de protección activa" (sistemas de armas diseñados para proteger vehículos blindados contra misiles o cohetes); 3 torretas robóticas armadas; y 26 tipos de municiones de permanencia en vuelo [*loitering*] (proyectiles que pueden modificar el rumbo para impactar con su objetivo).

Estados Unidos es un ejemplo paradigmático

3 Ceceña, Ana Esther (2016), "La territorialidad de las corporaciones", en Las corporaciones y la economía-mundo, Siglo XXI, México.

de la mancuerna existente entre estados y corporaciones. Según información de SIPRI, entre 2016 y 2020 el Departamento de defensa de Estados Unidos planea invertir 18 mil millones de dólares en investigación y desarrollo de SAAs. Aunque una parte de ese presupuesto lo ejerce la Agencia de proyectos de investigación avanzados de defensa (DARPA), la mayor parte está destinada al pago a las corporaciones tecnológicas y armamentistas como contratistas militares. Adicionalmente, mucha de la investigación en tecnologías de vanguardia financiada de manera privada por las corporaciones puede ser utilizada tanto para fines civiles como militares (uso dual). El resultado de esta dinámica es que el estado estadounidense y sus corporaciones actualmente son los mayores productores de sistemas de armas autónomos y semi-autónomos.

No obstante, Estados Unidos no es el único país donde se invierte intensamente en la investigación y desarrollo de estos sistemas de armas.[4] Otros estados con grandes presupuestos militares y una industria armamentista con amplias capacidades tecnológicas que están impulsando la investigación e implementación de SAAs son: Rusia, China, Alemania, Francia, Reino Unido, Italia, Israel y Corea del Sur. Aunque las posiciones políticas entre esos estados difieren en torno a los márgenes y regulación del uso de este nuevo armamento, ninguno dejará de invertir en el desarrollo de las armas autónomas *so pena* de quedar rezagados en un área que representa el futuro de la guerra y que será clave para la supremacía militar.

Las principales corporaciones que desarrollan sistemas de armas autónomos son: BAE Systems (Reino Unido), Israel Aerospace Industries (Israel), KBP Instrument Design Bureau (Rusia), Leonardo (Italia), Lockheed Martin (Estados Unidos), Rafael (Israel), Raytheon (Estados Unidos), Rheinmetall (Alemania) y Samsung (Corea del Sur). Aunque no hay información disponible sobre los ingresos y ganancias que la venta de los SAAs genera o generará a estas corporaciones, todo indica que se trata de un negocio multimillonario en el que hay también abundante financiamiento estatal.

Algunos riesgos

Al excluir la intervención humana y funcionar con complejos algoritmos de IA, los SAAs plantean nuevos riesgos. Por ejemplo, pueden tener un mal funcionamiento porque hay errores en la escritura de su código o pueden ser objeto de ciberataques. Esto podría traer consigo la pérdida de control en su funcionamiento o un escalamiento del conflicto tan acelerado que no haya tiempo para que los humanos respondan. Además, los SAAs pueden interactuar de forma impredecible para los humanos.

A lo anterior hay que añadir que debido a que la tecnología que hace posible el funcionamiento de las armas autónomas sería generalizada y fácilmente transferible, grupos armados no estatales (algunos de ellos considerados como "terroristas") podrían tener acceso a la utilización de sistemas de armas autónomos, lo que haría más complejos y letales los conflictos.

Reflexiones finales

Con los sistemas de armas autónomos, nos encontramos en el umbral de una mutación en la naturaleza de la guerra y sus tecnologías. Los SAAs y las tecnologías que los hacen posibles son claves en la competencia por el liderazgo tecnológico, en la pugna por la supremacía militar y en la disputa por la hegemonía mundial.

Los SAAs no son una anomalía en el curso de la sociedad moderna. Por el contrario, representan un resultado plenamente compatible con las tendencias que la rigen. Por ello, es necesario inscribir el cuestionamiento de los SAAs en una crítica de la lógica que está detrás suyo: la de la guerra y la acumulación incesante de capital como principios que organizan un mundo que se enfila a la catástrofe.

4 Debido a los pocos detalles que los estados ofrecen sobre su inversión en investigación militar, no hay información disponible para presentar un comparativo internacional que ponga de relieve el financiamiento estatal a la investigación y desarrollo de sistemas de armas autónomos.

Guerra siempre, guerra por doquier

Ana Esther Ceceña, David Barrios y Alberto Hidalgo

Los estrategas estadounidenses han identificado claramente dos ejes del mal. El primero concierne a los países que tienen capacidad potencial de poner en riesgo la hegemonía de Estados Unidos sobre el proceso de reproducción tanto de las relaciones de poder como del sistema. El desafío mayor consiste en afianzar su superioridad, particularmente en los campos tecnológico y económico, frente a China, Rusia e Irán –Corea del Norte en menor medida–, para inhabilitar una posible coalición que podría resultar cada vez más difícil de enfrentar. Ya las competencias en varios campos de tecnología militar muestran grietas en el monolito estadounidense, pero las dimensiones globales aún distan de anunciar la caída del imperio. Si bien con distintos estilos y dinámicas, es evidente que ambos lados deben apresurarse para definir posiciones.

Geográficamente, uno de los espacios que marca los términos de la disputa es América Latina, donde por cierto se ubica el segundo eje del mal conformado por Venezuela, Cuba y Nicaragua, de acuerdo con los documentos militares estadounidenses, y dibujándose un poco en las sombras, Bolivia.

La apuesta aquí es distinta. Nadie en esta región tiene condiciones de disputar el liderazgo mundial. Lo que sí se asoma son proyectos de organización sistémica no capitalistas que, aunque en ciernes, coartan la libertad del hegemón para disponer de territorios, poblaciones, riquezas y voluntades. Peor aún, las tensiones generadas y las piezas en juego han acercado las posiciones de los integrantes de ambos ejes y el espacio históricamente monopolizado por Estados Unidos ahora alberga proyectos de infraestructura, de comunicación, económicos, tecnológicos y culturales prescindiendo de la participación de la potencia del *tío Sam*. América Latina adquirió capacidad para disputar narrativas mediante la creación de Telesur, en alianza con HispanTV y Russia Today, y a la vez es una ventana para vislumbrar las visiones no *americanas* del mundo.

La construcción de sistemas de comunicación lo más independientes posible, y el blindaje del espacio cibernético han sido parte de los campos de trabajo conjunto que buscan evitar ataques financieros o a las infraestructuras críticas.

La ciberguerra y la guerra sobre terreno

En este contexto, es interesante observar algunos de los movimientos y de las declaraciones del Comando Sur de las Fuerzas Armadas de Estados Unidos. En sus propios términos, la definición de los desafíos a enfrentar, de acuerdo con el documento *Estrategia del Comando Sur* actualizado en mayo de este año, se identifica con el creciente papel que tienen

Ana Esther Ceceña, David Barrios y Alberto Hidalgo son Investigadores integrantes del Observatorio Latinoamericano de Geopolítica, Instituto de Investigaciones Económicas, UNAM.

sus competidores más cercanos, pero también otros países y amenazas no estatales.

> …China está aumentando rápidamente su comercio e inversión, y ahora es el mayor acreedor de la región […] ha expandido su iniciativa *One Belt, One Road* en América Latina y el Caribe a un ritmo que algún día podría eclipsar su expansión en el Sudeste asiático y África. Rusia e Irán han aumentado contra Estados Unidos esfuerzos de información en la región, e Irán ha exportado su apoyo estatal al terrorismo en este hemisferio […] China emplea las mismas prácticas de préstamos extranjeros depredadores y opacos que ha implementado en todo el mundo para ejercer influencia política y económica en este hemisferio. El control de China de los puertos e infraestructura de aguas profundas asociados con el Canal de Panamá mejora su postura operativa global. Sus inversiones en telecomunicaciones y el acceso a instalaciones de rastreo espacial ponen en riesgo las operaciones militares, la propiedad intelectual y los datos privados. China y Rusia también apoyan a sus aliados autoritarios en Cuba, Venezuela y Nicaragua, a menudo a través de propaganda y otras herramientas relacionadas con la información. Rusia difunde la información para sembrar la desunión, recolecta inteligencia y despliega activos estratégicos como buques de guerra y bombarderos con capacidad nuclear en la región para demostrar su alcance global […] El representante de Irán, el Hezbolá libanés, mantiene redes de facilitación y recauda fondos en el hemisferio, a menudo a través del tráfico de drogas y el lavado de dinero. Irán sigue siendo el patrocinador estatal más importante del terrorismo en todo el mundo. (Southcom, 2019)

Al hegemón le preocupan los 56 acuerdos portuarios que, de acuerdo con sus estimaciones, China tiene en la región como parte de su estrategia de desarrollo denominada *One Belt, One Road* y que ponen en riesgo su posición de dominio. Pero además de ello, se señalan insistentemente las inversiones del gigante asiático en tecnología e infraestructura informática y de información para "conseguir ampliar su influencia" a la que atribuye una clara dimensión militar. En el mismo sentido, son señalados los esfuerzos de Rusia e Irán por construir plataformas de comunicación, en articulación con Telesur, que logren contrarrestar el relato hegemónico.

A este discurso en torno a la pérdida de control sobre el área, subyace una lógica que aunque actualizada, remite al mismo viejo imperialismo de Estados Unidos. Esto quedó patente en el discurso pronunciado por el Mayor Daniel Walrath, jefe de las fuerzas de tierra del Comando Sur desde julio pasado:

> [En tanto América Latina constituye el área de responsabilidad del Comando Sur], es nuestro vecindario, y la misión del Ejército del Sur es dirigirse hacia los retos de seguridad en común en cooperación con nuestros socios, lo que representa la versión actual de la Doctrina Monroe. (Dotson, 2019).

No obstante, el trabajo regional ha ido quedando bajo la responsabilidad de los aliados locales. Muchos de los países del área participan en distintos intercambios, ejercicios, convenios y entrenamientos con Estados Unidos, pero las actividades conjuntas con Colombia, Chile, Honduras y Brasil han tenido un carácter más de socios corresponsables. Colombia resalta por su protagonismo en la guerra con Venezuela y por el papel que tiene al entrenar a las fuerzas de otros países del área, en este caso, a partir del *U.S.-Colombia Action Plan for Regional Security Cooperation*. De acuerdo con información del Ministerio de Defensa del país andino, entre 2013 y 2017, Colombia entrenó a 16,997 efectivos, de los cuales el 85% provenían de países de Centroamérica (Beittel, 2019).

Operaciones Especiales

Las modalidades de guerra contemporánea, en muchas ocasiones sin la participación de ejércitos explícitos, han llevado a la proliferación y generalización de las Operaciones Especiales. Entre otras razones porque éstas, que parten de un principio de clandestinidad, permiten intervenir en escenarios en los que no se puede o desea actuar de manera abiertamente militar. Es decir que se trata de formas de intervenir que pueden apuntalar discretamente el proceso de derechización o de conformación de regímenes y sociedades afines con los intereses del hegemón.

En nuestra región, el seguimiento que de manera permanente hacemos sobre distintas actividades militares nos permite señalar que en lo que va del año se han llevado a cabo 7 intercambios, ejercicios y entrenamientos dedicados a este tipo de tareas.[1] En marzo se realizó en Tolemaida un curso de dos y tres semanas de duración en este tipo de tácticas dirigido a suboficiales colombianos, mismo que fue replicado en el mes de septiembre en Canto Norte, Bogotá. En esos mismos días un entrenamiento en Operaciones Especiales facilitado por el componente aéreo de la Fuerza de Tarea Conjunta Bravo (Base de Soto Cano en Honduras) se llevó a cabo en El Salvador, dedicado especialmente a lanzamientos en paracaídas aire-tierra y en escenarios anfibios. También en marzo el Comandante Militar Adjunto del Southcom Michael Plehn, visitó Colombia, donde sostuvo reuniones con la División de Operaciones Especiales del país. Otro intercambio de este tipo se dio en Goiânia en el mes de abril, entre el Ejército brasileño (que cuenta con el primer batallón de Operaciones Psicológicas de la región) y el Comando Sur. Específicamente fueron abordados temas relacionados con Operaciones de apoyo de información, mismas que son definidas como:

> …planificadas para transmitir información e indicadores seleccionados a audiencias extranjeras para influir en sus emociones, motivos, razonamiento objetivo y, en última instancia, el comportamiento de gobiernos, organizaciones, grupos e individuos extranjeros de manera favorable a los objetivos de quien las origina. También son conocidas como MISO (DOD, 2019).

En junio se llevó a cabo el ejercicio Fuerzas de Operaciones Especiales-Fuerzas Comando, en esta ocasión en Chile con participación de 20 países. Los "juegos de competencia" son acompañados de seminarios entre militares con mayor perfil con el objetivo de fortalecer las alianzas y alcanzar la "seguridad regional". Finalmente en lo que corresponde a lo que va de este 2019, se llevó a cabo un Entrenamiento de Intercambio Combinado Conjunto sobre Operaciones Especiales de carácter bilateral en Paraguay.

Como se ve, si bien las Operaciones Especiales regularmente se asocian con la introducción de grupos de acción específica y acotada, lo que propicia crecientemente el uso de mercenarios, para desestabilizar los escenarios de la guerra, esas actividades van orientándose cada vez más hacia intervenciones cibernéticas, o de manejo de información y contrainformación para la contaminación o fabricación de narrativas.

Fuentes consultadas

Beittel, S., June, 2019, "Colombia: Background and U.S. Relations" (actualización a febrero de 2019), *Congressional Research Service*

Dotson, Ashley, 2019, "U.S. Army South Welcomes New Commander", Southcom, 16 de julio.

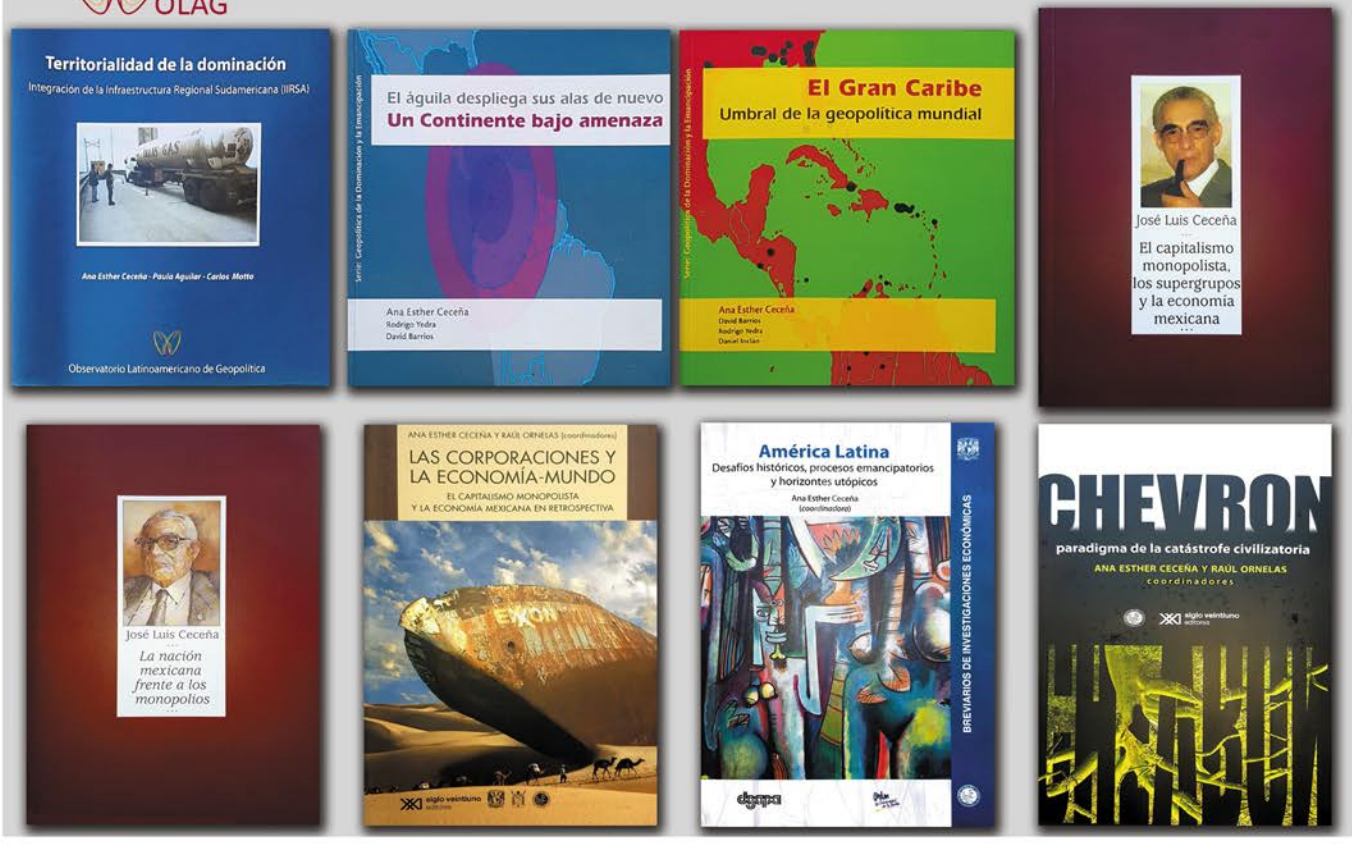
Department of Defense, 2019, *DOD Dictionary of Military and Associated Terms*, enero.

Southcomm, 2019, "Southern Command Strategy: «Enduring promise for the Americas»", Florida.

1 Las referencias a las actividades del Comando Sur fueron consultadas en todos los casos en el sitio electrónico www.southcom.mil

OLAG

Publicaciones del Observatorio Latinoamericano de Geopolítica



Encuentro **Antimperialista** de Solidaridad por la Democracia y contra el **Neoliberalismo**

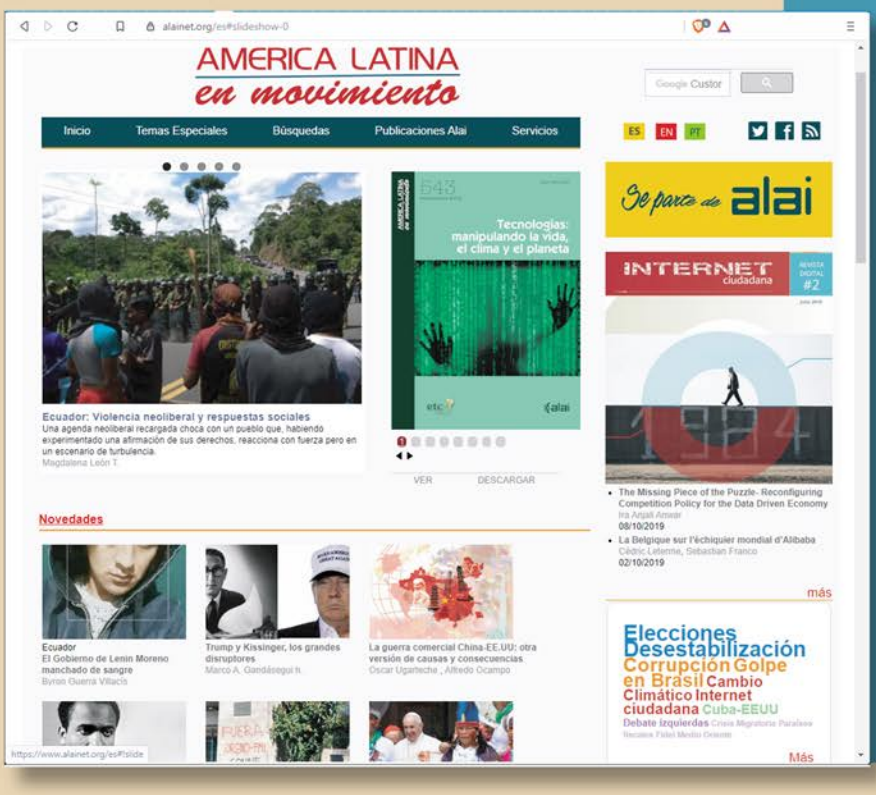
Del 1ro al 3 de noviembre de **2019**
La Habana, Cuba

"Los Pueblos seguimos en lucha"

#NoMásBloqueo #SeguimosEnLucha #JornadaContinental #SoyAntimperialista

Dossier

www.alainet.org/es/dossier/china-eeuu



www.alainet.org

- realidad regional actualizada diariamente
- dinámicas sociales
- noticias, opinión y análisis
- más de mil documentos clasificados
- búsquedas por tema, autor, fecha, país, palabra clave