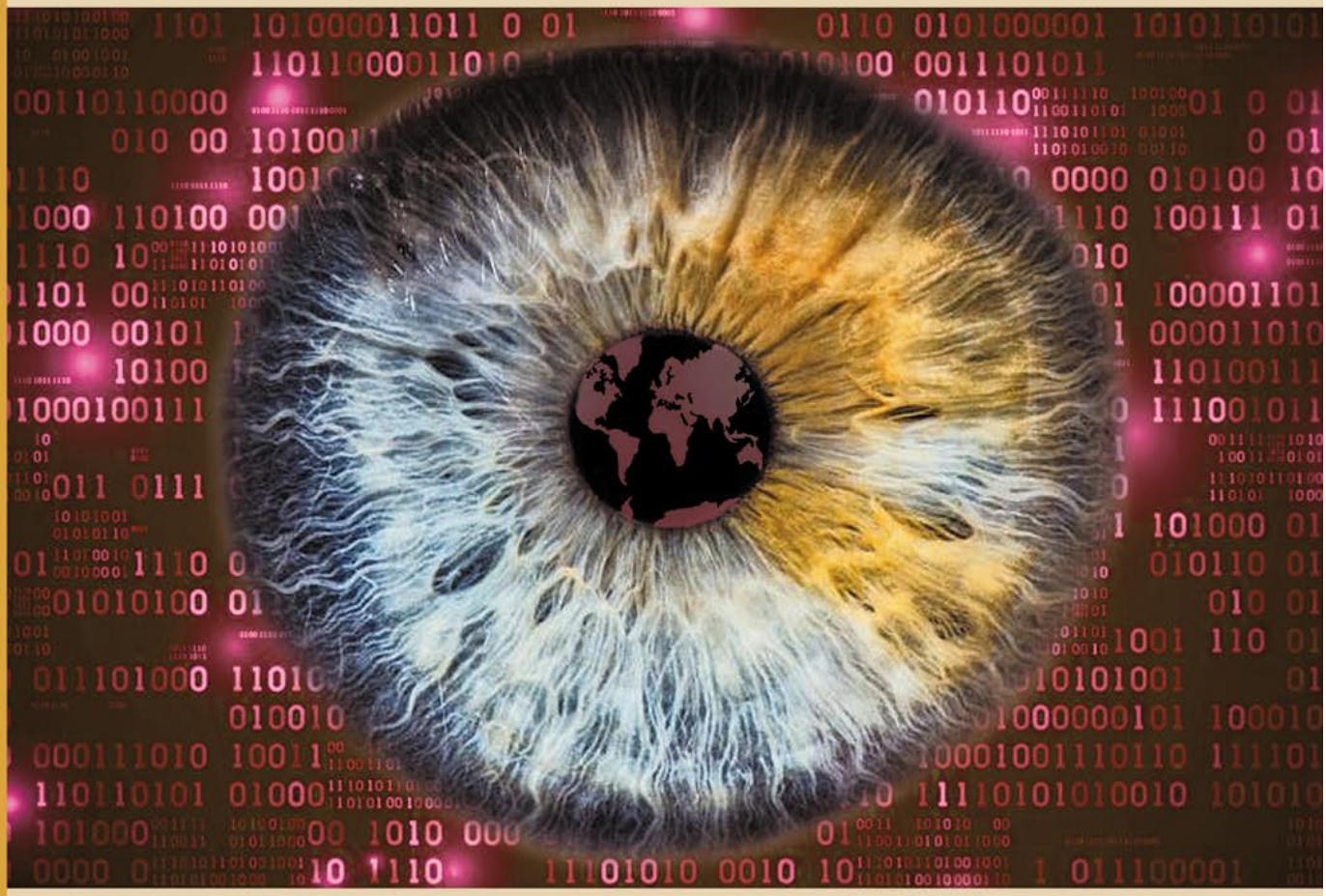
AMERICA LATINA en movimiento

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.