

Guerras cibernéticas: Nuevas formas de guerra

Por: [Leonardo Boff](#)

Globalización, 25 de diciembre 2017

[Cubadebate](#) 22 December, 2017

Tema: [Agenda de guerra EE.UU.-OTAN](#),
[Ciencia](#), [Defensa](#), [Guerra EEUU-OTAN](#)

Conocemos las formas clásicas de guerra, primero entre ejércitos y después de Hitler (con su totaler Krieg = guerra total) de pueblos contra pueblos. Se inventaron bombas nucleares tan potentes que pueden destruir toda la vida. Se dice que son armas de disuasión. No importa. Quien tenga primero la iniciativa gana la guerra, que duraría pocos minutos. La cuestión es que son tan letales que pueden matar a todos, incluso a los primeros que las lanzaron. Se volvieron armas de horror. Pero cuidado, la seguridad nunca es total y no es imposible que algunas de ellas exploten bajo la acción de hackers, poniendo en riesgo a gran parte de la humanidad.

Últimamente se ha inventado otra forma de guerra de la que la mayoría ni siquiera se da cuenta: la guerra cibernética, llamada también guerra informática, guerra digital y ciberguerra.

Esta tiene un telón de fondo que merece ser considerado: hay un exceso de acumulación de capital hasta el punto de que las grandes corporaciones no saben dónde aplicarlo. La agencia de políticas de desarrollo, Oxfam, presente en 94 países y asesorada por científicos del MIT, nos proporcionó este año de 2017 los siguientes datos: **el 1% de la humanidad controla más de la mitad de la riqueza del mundo. El 20% más rico posee el 94,5% de esa riqueza, mientras que el 80% debe conformarse con el 5,5%. Es una profunda desigualdad que traducida éticamente significa una injusticia perversa.**

Esta excesiva concentración no ve sentido en aplicaciones productivas porque el mercado empobrecido no tiene condiciones de absorber sus productos. O continúan en la rueda especulativa agravando el problema o encuentran otras salidas rentables a las aplicaciones. Varios analistas, como William Robinson de la Universidad de California, Santa Bárbara, que publicó un brillante estudio sobre el tema, y también Nouriel Rubini, que previó la debacle de 2007-2008, refieren **dos salidas para el capital ultraconcentrado: invertir en la militarización comandada por el Estado, construir nuevas armas nucleares o invertir en guerras locales, guerra contra las drogas, en la construcción de muros fronterizos, en inventar nuevos aparatos policiales y militares.**

O bien hacer grandes inversiones en tecnología, robotización, automatización masiva y digitalización, cubriendo, si es posible, todos los ámbitos de la vida. Si la inversión en 1980 era de 65 mil millones, ahora ha pasado a 654 mil millones. En esta inversión están previstos servicios de control de las poblaciones, verdadero estado policial y las guerras cibernéticas.

Sobre esto, conviene detallar un poco el análisis. En la guerra cibernética no se usan armas físicas sino el campo cibernético con la utilización de virus y hackers sofisticados que entran en las redes digitales del enemigo para anular y eventualmente dañar los sistemas informáticos. **Los principales objetivos son los bancos, los sistemas financieros o militares y todo el sistema de comunicación. Los combatientes de esta guerra son expertos en informática y en telecomunicaciones.**



Guerras cibernéticas vienen ganando predominio durante años recientes

Este tipo de guerra ha sido probado varias veces. Ya en 1999 en la guerra de Kosovo, los hackers atacaron incluso al portaaviones norteamericano. Tal vez el más conocido fue el ataque a Estonia el 26 de abril de 2007. El país se jacta de poseer casi todos los servicios del país informatizados y digitalizados. Un pequeño incidente, el derribo de la estatua de un soldado ruso, símbolo de la conquista rusa en la última guerra, por civiles de Estonia sirvió de motivo para que Rusia dirigiera un ataque cibernético que paralizó prácticamente todo el país: los transportes, las comunicaciones, los servicios bancarios, los servicios de luz y agua. Los siguientes días desaparecieron los sitios del Parlamento, de las Universidades y de los principales diarios. Las intervenciones venían de diez mil ordenadores distribuidos en distintas partes del mundo. El jefe de Estado de Estonia declaró acertadamente: “nosotros vivíamos en el futuro: bancos en línea, noticias en línea, textos en línea, centros comerciales en línea; la total digitalización hizo todo más rápido y más fácil, pero también creó la posibilidad de hacernos retroceder siglos en segundos”.

Es muy conocido el virus Stuxnet, producido posiblemente por Israel y Estados Unidos, que logró entrar en el funcionamiento de las plantas de enriquecimiento de uranio de Irán, aumentando su velocidad a punto de agrietarse o imposibilitar su funcionamiento.

El mayor riesgo de la guerra cibernética es que puede ser conducida por grupos terroristas, como el ISIS o por otro país, paralizando toda la infraestructura, los aeropuertos, los transportes, las comunicaciones, los servicios de agua y luz e incluso romper los secretos de los aparatos de seguridad de armas letales y hacerlas disparar o inutilizarlas. Y todo esto a partir de cientos de ordenadores operados desde diferentes partes del planeta, imposibilitando identificar su lugar y así hacerles frente.

Estamos, por tanto, frente a riesgos innumbrables, fruto de la razón enloquecida. Sólo una humanidad que ama la vida y se une para preservarla podrá salvarnos.

Leonardo Boff: *Teólogo, filósofo y escritor brasileño. Conocido por su apoyo activo a los derechos de los pobres y marginados dentro del marco de la Teología de la Liberación, y además al movimiento ecologista.*

La fuente original de este artículo es [Cubadebate](#)

Derechos de autor © [Leonardo Boff](#), [Cubadebate](#), 2017

[Comentario sobre artículos de Globalización en nuestra página de Facebook](#)
[Conviértase en miembro de Globalización](#)

Artículos de: [Leonardo Boff](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Center of Research on Globalization grants permission to cross-post original Global Research articles on community internet sites as long as the text & title are not modified. The source and the author's copyright must be displayed. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca