CIENCIA Y TECNOLOGÍA / MUNDO

El uso de armas cibernéticas de USA desde 1982 sobre Rusia y el Mundo

El Ciudadano · 20 de diciembre de 2016

Ru

20/12/2016.- Leer y escuchar tantas falsedades y desinformaciones sobre Siria para tratar de ocultar una enorme derrota geoestratégica en el Oriente Medio, ver tanto desatino y obsesión en llevar el mundo a una peligrosa confrontación entre Estados Unidos y sus aliados con Rusia, seguir las "noticias" fabricadas para crear falsas acusaciones contra Vladimir Putin sobre el supuesto "hackeo" de los correos electrónicos del Consejo Nacional Demócrata (CND), todo eso hace hervir la sangre de este viejo periodista que sabe, documento de la CIA a la mano (1), que si hay un gobierno que inventó el sabotaje y pirateo informático, el "hackeo" en sus diversas formas y lo puso en práctica en 1982 -cuando Internet estaba en pañales y en la "cuna" del Pentágono-, para ejecutar un sabotaje de enormes dimensiones contra la economía de la Unión Soviética, ese es bien el gobierno de Washington. Que el gobierno soviético no supiera entonces el origen de ese sabotaje, y que se lo considerara como un "accidente" y por lo tanto quedase impune, nos salvó de una guerra nuclear.

Como la hipocresía no tiene límites en esta patética y peligrosa decadencia imperial, recordemos que bastan unos minutos en Internet para encontrar que la experiencia con el sabotaje informático del gasoducto transiberiano sirvió para otros sabotajes en países "enemigos", el más conocido es el llevado a cabo contra

las centrifugadoras nucleares de Irán con el sofisticado "virus" Stuxnet, obra de informáticos estadounidenses e israelíes (2). Y si se tratara de hackeo para acceder a documentos o para espiar conversaciones, Edward Snowden nos ha mostrado que nadie está a salvo de las intromisiones y escuchas de la National Security Agency, o del "hackeo" israelí, como lo muestra la operación "Duqu" contra Irán durante las conversaciones entre Washington y Teherán, como en su momento reportaron el Wall Street Journal y Haaretz (3).

Ahora, a menos de un mes de finalizar su mandato el presidente Barack Obama amenazó con tomar represalias contra Rusia por el supuesto pero no probado "hackeo" del CND, pero el periodista David Sanger escribe en el New York Times (4) que por diferentes razones (y entre ellas la falta de pruebas, evidentemente) no parece haber consenso en la Administración, aun cuando EEUU dispone de un enorme "arsenal cibernético" a su disposición.

Esos planes, según Sanger, podrían desplegar un arsenal de primera clase mundial de armas cibernéticas ensambladas a un costo de miles de millones de dólares bajo el mandato del señor Obama, para exponer o neutralizar los instrumentos favoritos de hackeo de los espías rusos, (o sea) el equivalente digital de un ataque preventivo. Pero la selección de objetivos por los estadounidenses y la precisión de esa represalia *pueden también exponer los 'implantes'* (caballos de Troya) *de software que Estados Unidos ha pacientemente insertado y mantenido en buena forma en las redes de Rusia, para el caso de futuros ciber-conflictos*.

Siendo un poco lógicos al seguir lo que Sangers nos dice, el dilema es que EEUU ya "hackeó" los sistemas informáticos rusos –como ya lo había hecho con los soviéticos- y ya puso sus caballos de Troya, y que esa estratégica ventaja militar no puede ser utilizada y por lo tanto puesta en peligro a menos que se trate de un asunto muy grave, del tipo que puede llevar a una guerra total entre ambas naciones.

Más adelante Sanger nos recuerda que "el señor Obama es el presidente que, en su primer año del mandato, buscó obtener las más sofisticadas ciber-armas del planeta para pulverizar partes de las instalaciones del plan nuclear de Irán. Ahora, al final de su presidencia, se encuentra frente a un desafío diferente en el terreno de la guerra con armas cibernéticas. El Presidente ha llegado a dos conclusiones, según reportan altos funcionarios*: La única cosa peor que no usar un arma es usarla de manera inefectiva. Y si escoge la represalia, él insiste en mantener lo que se llama una 'posición dominante', o sea asegurarse la habilidad de concluir el conflicto en sus propios términos".*

No es de extrañar que desde hace algún tiempo Rusia y China impulsan la creación de sistemas informáticos y de componentes electrónicos en sus países, evidentemente para liberarse de los "caballos de Troya" y las "puertas secretas" que desde 1982, es decir desde el comienzo de la informática sofisticada y de su interacción con las telecomunicaciones, EEUU y sus empresas vienen introduciendo en sus productos, y

que muy probablemente afectan tanto los que son producidos para el propio país como para los exportados hacia el resto de países.

El papel de las armas cibernéticas en la guerra económica.

Si hay una constante en las formas de agresión de los imperialistas pasados y presentes contra los pueblos que deciden asumir sus destinos haciendo cambios para recuperar sus soberanías, o haciendo una revolución socialista, esa es la guerra económica, en todas las esferas posibles de la economía, en el comercio, las finanzas y las monedas, y en los intercambios que impliquen transferencias de procesos, tecnologías y ciencias necesarias para el desarrollo de las fuerzas productivas.

En definitiva, el objetivo es de hambrear esos pueblos impidiéndoles desarrollar sus fuerzas productivas, para desestabilizar la vida política de esas naciones y obligarlas a tomar medidas de racionamiento, entre otras más que no serían necesarias en el marco de relaciones normales de intercambio comercial internacional.

Esta es una forma de guerra que los países imperialistas han utilizado desde 1919 (5), comenzando con el "cordón sanitario" contra la naciente Unión Soviética, continuada mediante bloqueos y controles de exportación, como el CoCom, y toda la panoplia de embargos y sanciones extraterritoriales para asfixiar las economías de los pueblos que no se someten al imperio. Desde entonces esta guerra económica estuvo acompañada de agresiones militares directas o fomentadas con aliados locales o foráneos –como la Operación Gladio en Europa- para llevar a cabo sabotajes de todo tipo, invasiones -como la de Playa Girón-, bloqueos económicos con sanciones de aplicación extraterritorial, golpes de Estado (demasiados para hacer una lista), operaciones clandestinas y creación de grupos terroristas o de fanáticos religiosos para desestabilizar gobiernos –como la creación de Al Qaeda para debilitar a la URSS, y del ISIS para destruir el Estado secular de a Siria-, y muchos etcétera más.

Nuestra América es testigo de la guerra económica más prolongada de la historia moderna, como nos recuerda el periodista cubano Manuel E. Yepe: la fundamentación original del bloqueo la dio el seis de abril de 1960 Lester D. Mallory, Vice Secretario de Estado Asistente para los Asuntos Interamericanos, en un memorándum secreto del Departamento de Estado desclasificado en 1991, que fue incluido en la página 885 del Volumen VI del Informe del Departamento de Estados de Estados Unidos de 1958 a 1960 que textualmente dice: *"La mayoría de los cubanos apoyan a Castro… el único modo previsible de restarle apoyo interno es mediante el desencanto y la insatisfacción que surjan del malestar económico y las dificultades materiales… hay que emplear rápidamente todos los medios posibles para debilitar la vida económica de Cuba… una línea de acción que, siendo lo más habilidosa y discreta posible, logre los mayores avances en la privación a Cuba de dinero y suministros, para reducirle sus recursos financieros y los salarios reales, provocar hambre, desesperación y el derrocamiento del Gobierno"* (6).

Es por eso mismo que si en la historia moderna hubo un líder político que durante más de cinco décadas conoció y luchó denodadamente contra la guerra económica del imperialismo estadounidense ese ha sido Fidel Castro. Y es por eso mismo que en septiembre del 2007, en su artículo titulado "Mentiras deliberadas, muertes extrañas y agresión económica mundial" (7), escribía que un ejemplo claro del uso de la ciencia y la tecnología con los mismos fines hegemónicos se describe en un artículo del ex oficial de Seguridad Nacional de Estados Unidos Gus W. Weiss, aparecido originalmente en la revista Studies in Intelligence, en 1996 (8), aunque con real difusión en el año 2002, titulado "Engañando a los soviéticos". En él Weiss se atribuye la idea de hacerle llegar a la URSS los softwares que necesitaba para su industria, pero ya contaminados con el objetivo de hacer colapsar la economía de aquel país.

Fidel se refiere ahí a la Operación Farewell, que tuvo lugar en los años 80 y cita el documento redactado por Gus Weiss, quien ocupó los cargos de Asistente especial del Secretario de la Defensa, y de consejero científico en el Pentágono y en el Servicio de Inteligencia durante el gobierno del Presidente James Carter, y puestos claves en el Consejo de Seguridad Nacional de EE.UU. bajo las presidencias de Richard Nixon, Ronald Reagan y Gerald Ford.

Sobre ese sabotaje de 1982 Fidel escribía que "la producción y transporte de petróleo y gas era una de las prioridades soviéticas. Un nuevo gasoducto transiberiano debía llevar gas natural desde los yacimientos de gas de Urengoi en Siberia a través de Kazajstán, Rusia y Europa oriental hasta los mercados de divisas de Occidente. Para automatizar la operación de válvulas, compresores e instalaciones de almacenaje en una empresa tan inmensa, los soviéticos necesitaban sistemas de control sofisticados. Compraron computadoras de los primeros modelos en el mercado abierto, pero cuando las autoridades del gasoducto abordaron a Estados Unidos para adquirir el software necesario, fueron rechazados. Impertérritos, los soviéticos buscaron en otra parte; se envió un operativo de la KGB a penetrar un proveedor canadiense de softwares en un intento por adquirir los códigos necesarios. La inteligencia estadounidense, avisada por el agente del Dossier Farewell, respondió y manipuló el software antes de enviarlo.

Una vez en la Unión Soviética, las computadoras y el software, trabajando juntos, hacían operar el gasoducto maravillosamente. Pero esa tranquilidad era engañosa. En el software que operaba el gasoducto había un caballo de Troya, término que se usa para calificar líneas de software ocultas en el sistema operativo normal, que hacen que dicho sistema se descontrole en el futuro, o al recibir una orden desde el exterior.

Con el objetivo de afectar las ganancias de divisas provenientes de Occidente y la economía interna de Rusia, el software del gasoducto que debía operar las bombas, turbinas y válvulas había sido programado para descomponerse después de un intervalo prudencial y resetear —así se califica— las velocidades de las bombas y los ajustes de las válvulas haciéndolas funcionar a presiones muy por encima de las aceptables para las juntas y soldaduras del gasoducto.

El resultado fue la más colosal explosión no nuclear e incendio jamás vistos desde el espacio. En la Casa Blanca, funcionarios y asesores recibieron la advertencia de satélites infrarrojos de un extraño evento en medio de un lugar despoblado del territorio soviético. El NORAD (Comando de Defensa Aeroespacial Norteamericano) temía que fuera el lanzamiento de misiles desde un lugar donde no se conocía que hubiera cohetes basificados; o quizás fuera la detonación de un dispositivo nuclear. Los satélites no habían detectado ninguna pulsación electromagnética característica de las detonaciones nucleares. Antes de que tales indicios pudieran convertirse en una crisis internacional, Gus Weiss llegó por un pasillo para decirles a sus colegas del CSN (Consejo de Seguridad Nacional) que no se preocuparan, afirma Thomas Reed en su libro (9).

La campaña de contramedidas basadas en el Dossier Farewell fue una guerra económica. Aunque no hubo bajas personales debido a la explosión del gasoducto, hubo un daño significativo para la economía soviética".

Y Fidel señalaba que "no podemos ignorar que durante la Guerra Fría e incluso en el breve período de la 'distensión' entre Washington y Moscú (1962-1975), EEUU y sus aliados trataron por todos los medios de impedir que la URSS y todos los países socialistas pudiesen adquirir legalmente los productos de alta tecnología, utilizando para ello diversos instrumentos creados para tal efecto, como el CoCom.

Sobre la Operación Farewell para desmantelar el equipo soviético que buscaba acceder a tecnologías modernas, Fidel recuerda que "consta en un artículo publicado en The New York Times que la operación utilizó casi todas las armas al alcance de la CIA —guerra sicológica, sabotaje, guerra económica, engaño estratégico, contrainteligencia, guerra cibernética—, todo ello en colaboración con el Consejo de Seguridad Nacional, el Pentágono y el FBI. Destruyó al pujante equipo de espionaje soviético, dañó la economía y desestabilizó el Estado de ese país. Fue un éxito rotundo. De haberse hecho a la inversa (los soviéticos a los norteamericanos), pudiera haberse visto como un acto de terrorismo".

"Del tema se habla también en otro libro titulado Legado de Cenizas, que acaba de ser publicado. En la solapa del libro se expresa que 'Tim Weiner es un reportero de The New York Times, quien ha escrito sobre los servicios de Inteligencia estadounidenses durante veinte años, y obtuvo un Premio Pulitzer por su trabajo sobre los programas secretos de Seguridad Nacional. Ha viajado a Afganistán y otros países para investigar de primera mano las operaciones encubiertas de la CIA. Este es su tercer libro".

"Legado de Cenizas se basa en más de 50 mil documentos, provenientes fundamentalmente de los propios archivos de la CIA, y cientos de entrevistas a veteranos de dicha agencia, incluidos diez directores. Nos muestra un panorama de la CIA desde su creación después de la Segunda Guerra Mundial, pasando por sus batallas durante la guerra fría y la guerra contra el terrorismo iniciada el 11 de Septiembre del 2001."

Y el líder cubano cita el artículo de Jeremy Allison, y los de Rosa Miriam Elizalde (10), en los cuales se denuncian estos hechos, destacando la idea de uno de los fundadores del software libre, quien señaló que "a medida que se complejizan las tecnologías será más difícil detectar acciones de ese tipo".

Y agrega que "Rosa Miriam publicó dos sencillos artículos de opinión de apenas cinco páginas cada uno. Si lo desea, puede escribir un libro de muchas páginas. La recuerdo bien desde el día en que, como periodista muy joven, me preguntó ansiosa, nada menos que en una conferencia de prensa hace más de 15 años, si yo pensaba que podríamos resistir el período especial que nos caía encima con la desaparición del campo socialista.

"La URSS se derrumbó estrepitosamente. Desde entonces hemos graduado a cientos de miles de jóvenes en el nivel superior de enseñanza. ¡Qué otra arma ideológica nos puede quedar que un nivel superior de conciencia! La tuvimos cuando éramos un pueblo en su mayoría analfabeto o semianalfabeto. Si lo que se desea es conocer verdaderas fieras, dejen que en el ser humano prevalezcan los instintos. Sobre eso se puede hablar mucho".

Y Fidel, que es inmortal en sus análisis e ideas, nos señalaba en 2007 que "en la actualidad, el mundo está amenazado por una desoladora crisis económica. El gobierno de Estados Unidos emplea recursos económicos inimaginables para defender un derecho que viola la soberanía de todos los demás países: continuar comprando con billetes de papel las materias primas, la energía, las industrias de tecnologías avanzadas, las tierras más productivas y los inmuebles más modernos de nuestro planeta".

Notas

1.- https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm ; Ante el impedimento de obtener los productos de alta tecnología mediante comercio legal, la URSS buscó obtenerlos de manera encubierta, creando la llamada "operación Line X", revelada en 1981 a los servicios de contrainteligencia de Francia por el oficial de la KGB que coordinaba la operación, el Coronel Vladimir I. Vetrov, codificado por los franceses como Farewell. En 1981, durante la Cumbre del G7 en Ottawa, el Presidente francés François Mitterrand transmitió al Presidente Ronald Reagan una copia de la lista de agentes y objetivos de la "operación Line X". Con esa información la CIA efectuó en 1982 el primer acto de sabotaje de la era informática, en el gasoducto Transiberiano (http://fcw.com/Articles/2004/04/26/Tech-sabotage-during-the-Cold-War.aspx?sc_lang=en&Page=2), inaugurando así el terrorismo telecomandado y la acción de los "hackers" en los sistemas informáticos. Ver también The Farewell Dossier, William Shafire, NYT 02-02-2004 http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?_r=0

2.- http://www.haaretz.com/israel-news/report-israel-tested-iran-bound-stuxnet-worm-in-dimona-nuclear-plant-1.337276 Report: Israel Tested Iran-bound Stuxnet Worm in Dimona Nuclear Plant: El retirado jefe de la agencia de inteligencia de Israel, Mossad, Mair Dagan, dijo recientemente que el programa nuclear iraní ha sido retrogradado y que Teherán no será capaz de construir una bomba atómica hasta al menos 2015. Funcionarios estadounidenses, incluyendo la Secretaria de Estado Hillary Clinton, no disputaron lo que dijo Dagan. (*The retiring chief of Israel's Mossad intelligence agency, Meir Dagan, said recently that Iran's nuclear program had been set back and that Tehran would not be able to build an atomic bomb until at least 2015. U.S. officials, including Secretary of State Hillary Clinton, have not disputed Dagan's view).* Stuxnet: How USA and Israel created anti-Iran virus, and then lost control of it https://nakedsecurity.sophos.com/2012/06/01/stuxnet-usa-israel-iran-virus/)

3.- Haaretz: Israel Spied on Iran Talks by Planting Computer Virus at Hotels, WSJ Reports http://www.haaretz.com/israel-news/1.660544 ; en el WSJ: http://www.wsj.com/articles/spy-virus-linked-to-israel-targeted-hotels-used-for-iran-nuclear-talks-1433937601

4.- David E. Sanger, 12-17-2016: "Obama Confronts Complexity of Using a Mighty Cyberarsenal Against Russia" ; http://www.nytimes.com/2016/12/17/us/politics/obama-putin-russia-hacking-us-elections.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=0

5.- Uno de los acuerdos del Tratado de Versalles de 1919 entre las grandes potencias occidentales que derrotaron a Alemania en la primera Guerra Mundial fue el de establecer un "cordón sanitario" para "impedir que la peste comunista se expanda por Europa" y, en realidad, aislar a la naciente República de los Soviets, impidiéndole relaciones comerciales y políticas con el mundo, lo que explica que al mismo tiempo se le haya negado su incorporación en la Sociedad de Naciones. Al comienzo de la Guerra Fría, en 1949, Estados Unidos crea la Organización del Tratado del Atlántico Norte (OTAN) y establece el Comité de Coordinación Multilateral para el Control de Exportaciones (CoCom) con sede en Paris y destinado a impedir cualquier exportación de tecnología avanzada hacia la URSS y demás países socialistas en Europa y Asia. Después del derrumbe de la URSS el CoCom fue reemplazado por los "Acuerdos de Wassernaar" con sede en Viena y con el mandato de controlar las exportaciones de armamentos y tecnología de "doble uso" (http://www.wassenaar.org/)

6.- Manuel Yepe, El verdadero alcance del bloqueo contra Cuba http://www.alainet.org/es/articulo/182450

7.- Fidel Castro, "MENTIRAS DELIBERADAS, MUERTES EXTRAÑAS Y AGRESIÓN A LA ECONOMÍA MUNDIAL" http://www.fidelcastro.cu/es/articulos/mentiras-deliberadas-muertes-extranas-y-agresion-la-

economia-mundial ; en inglés: http://www.globalresearch.ca/deliberate-lies-strange-deaths-and-aggression-to-the-world-economy/6861

8.- https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass y https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm

9.- AT THE ABYSS: An Insider's History of the Cold War http://www.publishersweekly.com/978-0-89141-821-4m ; Old Trick Threatens the Newest Weapons http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=1&ref=science&pagewanted=all ;The Hunt for the Kill Switch http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

10.- Rosa Miriam Elizalde escribió sobre el tema varios y muy buenos artículos en 2006 y 2007: Cómo la CIA hizo estallar un gasoducto en Siberia. Dossier Farewell https://www.rebelion.org/noticia.php?id=56005 ; Comando del Ciberespacio de la Fuerza Aérea de EEUU: No apto para aficionados http://www.rebelion.org/noticia.php?id=51104 ; Y vale mencionar, como lo hizo Fidel, el artículo de un especialista, de Jeremy Allison: La CIA modificó software para causar graves daños a la Unión Soviética. Computación «confiada» http://www.rebelion.org/noticia.php?id=33610 ; Otros lazos de interés: Operación Farewell, fuentes de información y resumen: http://en.wikipedia.org/wiki/Vladimir_Vetrov ; Farewell Dossier – Wikipedia, the free encyclopedia; https://fcw.com/Articles/2004/04/26/Tech-sabotage-during-the-Cold-War.aspx?sc_lang=en&Page=1&p=1 ; https://nsarchive.wordpress.com/2013/04/26/agent-farewell-and-the-siberian-pipeline-explosion/ ; https://nsarchive.wordpress.com/2013/04/26/agent-farewell-and-the-siberian-pipeline-explosion/#_ednref2 ; http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html

– ***Alberto Rabilotta*** es periodista argentino-canadiense.

URL de este artículo: http://www.alainet.org/es/articulo/182485

Fuente: El Ciudadano