GlobalResearch
Center for Research on Globalization

EE.UU. y Rusia: De la Guerra Fría a la guerra cibernética

By William de Jesús Salvador
Global Research, January 15, 2017
Katehon en Español 12 January 2017

"La guerra cibernética es el conjunto de acciones llevadas por un Estado para penetrar en los ordenadores o en las redes de otro país, con la finalidad de causar prejuicio o alteración" . Richard Clarke, especialista en seguridad del gobierno de EE.UU.

El gobierno norteamericano de manera categórica ha acusado formalmente a Rusia de interferir en su proceso electoral a través de robos de correos electrónicos y documentos que fueron publicados por WikiLeaks, DCLeaks, y GUccifer 2.1.

El Presidente Barack Obama reaccionó muy enfadado con el Presidente Vladimir Putin, lo ha responsabilizado del 'hackeo' a las comunicaciones del jefe de la campaña del Partido Demócrata, John Podesta, y a la Fundación Hillary Clinton durante las campaña electoral norteamericana.Moscú rechazó las acusaciones de intromisión en elecciones EEUU y Dmitry Peskov dijo que Estados Unidos debería "dejar de hablar de ello o producir alguna evidencia, de lo contrario todo comienza a parecer impropio."

Las revelaciones de este 'hackeo' dejó al desnudo la alianza estratégica y aproximación de la candidata demócrata con los grupos financieros de Wall Street -aunque su discurso de campaña en ocasiones manejaba una retórica distante- además los correos dejaron saber la estratagema o urdimbre que tejió contra Bernie Sanders quien fuese el rival de Hillary Clinton.

El Gobierno estadounidense ha aplicado sanciones diplomáticas a Rusia, que consisten en la expulsión de 35 diplomáticos rusos y sus familias, seis de ellos acusados de espionaje, el cierre de dos centros de operaciones en Nueva York y Maryland; además de sanciones a tres empresas rusas establecidas en los Estados Unidos.

> ¿Cómo los ciberdelincuentes rusos robaron los correos electrónicos e influyeron de manera tal en el resultado electoral que el FBI abrió una nueva investigación a la candidata del Partido Demócrata Hillary Clinton?

Los principales medios de comunicación el 30 de diciembre 2016, como los Hackers penetraron a las computadoras demócratas para producir la sustracción maliciosamente de informaciones sensibles:

Las informaciones hechas públicas ayer por el FBI y el Departamento de Seguridad Interior (DHS), establece que dos equipos de hackers informáticos mercenarios del gobierno ruso habrían robado información de los ordenadores de los cobradores a Hillary Clinton.

Los especialistas en espionaje cibernético establecen que siempre quedan trazas de las actividades cibercriminales, y que esto fue lo sucedido: A mediado del año 2015, el grupo "hackers" denominado como APT29, entró a las redes del partido Demócrata de Estados Unidos. Su 'modus operandi' fue mandar mensajes de correo con un enlace malicioso a miles de personas relacionadas con todo el entramado de Hillary Clinton, solo bastaba que uno solo abriese los correos con los documentos adjuntos infectados y efectivamente los delincuentes lograron cuando una persona lo hizo, abriendo paso al código malicioso en su ordenador.

En el primer cuatrimestre del 2016, otro grupo de 'hackers' conocidos como APT28, utilizando la misma ciber estrategia para infiltrarse al mismo partido político, remitieron mensajes de correo a un considerable número de personas, esta vez, usaron las webs legítimas con agujeros de seguridad para alojar allí páginas-trampa que pedían a los afectados que introdujesen sus credenciales. Estas credenciales llegan directas al 'banco' de los ciberdelincuentes.

Con las credenciales robadas, APT28 entró en las redes del partido y filtraron las informaciones de múltiples miembros 'senior'. Pero, a diferencia de APT29, no la guardó si la hizo públicas por vía de la prensa. El director de la CIA, John Brennan confirmó la información del ciber espionaje, James Comey Jefe del FBI y James Clappers Director de Inteligencia Nacional han compartido todo lo relacionado a este tema, y están asegurando que el gobierno ruso actuó de manera intrusa en el proceso electoral para perjudicar a Clinton y favorecer a Donald Trump, quien ha descalificado y poniendo en dudas las competencias de los organismos de seguridad norteamericanos.

Las relaciones entre el gobierno de Obama y Putin, están en un punto muerto después de las sanciones aplicadas unilateral por EE.UU, ya que el gobierno ruso no aplicó medidas recíprocas de orden diplomáticas, simplemente cerraron la escuela de hijos de diplomáticos, a la vez que el Presidente Putin prefirió esperar que el Presidente Trump asuma la jefatura de Estado, cuyas relaciones parecen ser excelentes.

Revisemos las guerras cibernéticas que se han desarrollado y que están reseñadas por Wikipedia con el título de Guerra informática

En el año 1999 en Guerra de Kosovo, casi medio millar de especialistas en asuntos informáticos con el Capitán Dragan se introducen en los ordenadores militares aliados, los ordenadores dela OTAN, la Casa Blanca y el portaaviones norteamericano Nimitz.

En este siglo en el 2003 , Taiwán recibió un ataque sin precedentes de denegación de servicio (DDoS), incluyó virus y troyanos la culpa recayó en los jefes de estrategias china.

En el año 2007, Estonia sospecha de Rusia por un Serie de ataques que trastornaron a medios de comunicación, bancos e instituciones del gobierno.

Medio Oriente en mayo de 2012, es descubierto uno de los Malware más dañinos hasta la fecha llamado Flame o sKyWIper, el cual se especula que está diseñado para propósitos de Cyber-espionaje. Entre los países que se ven más afectados están Irán, Israel, Sudán, Siria, Líbano, Arabia Saudí y Egipto.

Anterior a la intromisión de los hackers en las elecciones de EE.UU, debemos recordar el conjunto de tropelías que filtró documentos diplomáticos de los Estados Unidos el 28 de

noviembre de 2010 por el portal WikiLeaks. Esto creó un gran trastorno internacional al gobierno de Obama con aliados y contrarios.

El derecho internacional avanza para establecer castigado a los delitos de espionaje cibernético, no está contemplado en un ningún tratado y paradójicamente los Jefes de Estados se reúnen en Cumbres donde pasan revista a los asuntos de interés global. Hay que recordar que en los años 2011 y 2012 Ley SOPA presentada por Lamar S. Smith, desató una reacción movimiento de grandes empresas y usuarios contrarios, podemos citar Google, Facebook, Twitter, Youtube, y Wikipedia. La organización de hackers Anonymous desplegó todas sus fuerzas intimidando a los auspiciadores de la Ley Sopa.

En un informe de la ONU el 16 de octubre del 2014 condena el ciberespionaje masivo por violar derechos establecidos. "La tecnología de acceso a granel es indiscriminadamente corrosiva de la privacidad online y afecta a la propia esencia del derecho" garantizado en tratados internacionales, afirma un documento oficial presentado en las Naciones Unidas.
El relator especial sobre contra terrorismo y derechos humanos de Naciones Unidas, Ben Emmerson, presentó un informe formal ante la Asamblea General en el que condena al ciberespionaje masivo en Internet por violar el derecho a la privacidad, garantizado en tratados y convenciones internacionales.

La vigilancia masiva es un grave problema y atenta contra los derechos individuales, El texto del relator indica que esta vigilancia masiva viola en principio el Pacto Internacional sobre Derechos Civiles y Políticos, un tratado aprobado por la Asamblea General en 1966, que en su Artículo 17º garantiza el derecho a la privacidad de las personas al establecer que "los individuos tienen derecho a compartir información e ideas con otros sin la interferencia del Estado, con la certeza de que sus comunicaciones serán leídas sólo por sus destinatarios"

La intromisión y robos de informaciones, así como las alteraciones de datos de la base de cualquier programa es una actividad criminal que debe ser castigada, tengo un amigo y que trabajamos en el área diplomática en Alemania, que había servido en los organismos de seguridad o tal vez seguía en esas labores, me dijo reiteradamente: "Yo no uso tarjeta de crédito, ni celular, usó tarjeta de débito y la uso solo para sacar dinero, hago mis transacciones cotidianas en efectivo y las importantes por transferencia, el teléfono celular te hace un preso de confianza y nada es más público que cualquiera de los servicios de internet." Lo consideraba obsoleto y paranoico. Hoy el tiempo me confirma que era un hombre ilustrado en esos menesteres.

Con la reacción de las agencias de investigación y seguridad de EE.UU, la CIA, FBI y de Seguridad Nacional , es muy probable que se inicie el proceso para establecer acuerdos multilaterales destinados a castigar estos delitos cibernético, que son capaz de crear amenazas a la seguridad de los países en materia energética, la banca, las bolsas, agua, nuclear y militar. Ahora hasta los procesos electorales un verdadero atentado a la democracia global. La humanidad pasa de la Guerra Fría a la Guerra Cibernética. Estamos ante la amenaza sin precedentes de una Guerra Mundial Cibernética.

William de Jesús Salvador

William de Jesús Salvador: *Diplomático y analista político dominicano.*

Articles by: **William de Jesús Salvador**