Comentarios UNISCI

Transición Cibernética: de Barack Obama a Donald Trump
Análisis comparado de las Órdenes Ejecutivas sobre Ciberseguridad

Manuel Gazapo Lapayese
UNISCI

23 Julio 2017

1 Introducción

Tanto Donald Trump como antes Barack Obama han operado con Executive Orders (EO) para poder llevar a cabo sus políticas en materia cibersecuritaria. Una revisión de las EO puestas en marcha por los presidentes Obama y Trump con respecto a la cuestión de la seguridad virtual, nos permitirá detectar cuales son las líneas de actuación tomadas y advertir si existe o no un continuismo entre ambas administraciones en torno a un tema vital para EEUU dentro del panorama internacional: la ciberseguridad.

Para crear el marco de análisis, hemos de retroceder en el tiempo y trasladarnos a 2009. Barack Obama fue el primer presidente de los EEUU en dedicar una atención destacada al problema de la seguridad cibernética. Al llegar a la Casa Blanca, reunió a un equipo para evaluar los esfuerzos de administraciones anteriores con el objetivo de crear un marco estratégico que ayudara a EEUU a hacer frente a los ciberataques que estaban apareciendo en el panorama internacional.

Durante su primer mandato, entre 2009 y 2012, por lo que se conoce de forma abierta, el mundo sufrió una serie de ciberataques de inmensa magnitud: por ejemplo, en marzo de 2009 tuvo lugar la operación *Ghostnet*, perpetrada desde China, que supuso el robo de datos procedentes de organizaciones como la OTAN y países de gran peso geoestratégico como EEUU; en diciembre de 2009 la entidad financiera americana CityBank sufrió un grave ciberataque; en enero de 2010 WikiLeaks sacó a la luz los controles de la Agencia Nacional de Seguridad de EEUU; en Julio de 2010 se acusó a EEUU de estar detrás del virus Stuxnet infiltrado en las plantas nucleares de Irán; y en Octubre de 2012 tuvo lugar el ciberataque denominado Octubre Rojo, que robo información de infraestructuras críticas de EEUU y otros países afectados.

Durante su segundo mandato, el mundo siguió sufriendo de forma progresiva ciberataques tremendamente sofisticados y alumbrando ciberfiltraciones cada vez más comprometidas : en enero de 2013 se destapó el ciberespionaje del gobierno chino a EEUU;

en junio de 2013 las filtraciones del analista de la NSA, Edward Joseph Snowden; en junio de 2014 el ciberataque a JP Morgan Chase, victima supuestamente de un ataque cibernético ruso; y, finalmente, la intromisión de Rusia en el sistema electrónico de votación de EEUU en junio de 2016.

Inmerso en un contexto global donde habían saltado las alarmas sobre un nuevo tipo de guerra, la guerra cibernética, Obama inició su segundo mandato redactando una orden ejecutiva sobre Ciberseguridad, la EO 13636 , "Improving Critical Infrastructure Cybersecurity". Firmada en febrero de 2013, se planteó como respuesta a la batería de ciberataques sufridos por EEUU en los últimos cuatro años. Sus disposiciones se ampliarían en la orden ejecutiva de abril de 2015, la EO 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". Barack Obama finalizó su mandato con la EO 13757, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities", del 28 de diciembre de 2016, como reacción al ciberataque masivo en la campaña a las elecciones presidenciales.

Estos hechos, arriba mencionados, determinan la forma y el contexto con el que Donald Trump accedía a la Casa Blanca en enero de 2017. La atmosfera era sumamente turbulenta debido al cuestionamiento de la legitimidad del proceso democrático a consecuencia de la injerencia cibernética del gobierno ruso en las elecciones presidenciales de EEUU. Ante este panorama, Donald Trump, al igual que hiciera Barack Obama, solicitó a su gabinete un periodo de revisión en torno a las cuestiones de ciberseguridad.

Es en ese momento, cuando el diario Washington Post filtró un primer borrador de lo que se suponía iba a ser su primera EO sobre ciberseguridad. Sin embargo, el texto no vio la luz en ese momento y la EO de Ciberseguridad estuvo detenida pendiente de aprobación hasta mayo 2017. El 11 de mayo del citado mes, finalmente salió a la luz la "Cyber EO" de la era Trump, la EO-13800, "Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", que ponía énfasis en dos cuestiones, la ciberseguridad de la red federal y la vulnerabilidad de sus infraestructuras críticas. No debe olvidarse que, con motivo del retraso en la firma de la EO, y para que no quedara un vacío legal, el 1 de abril de 2017 Trump dirigió una carta al Congreso solicitando la extensión temporal de la EO de Obama, de forma que se garantizaba que el Gobierno seguía teniendo una serie de poderes especiales para realizar

detenciones y revisiones en cuestiones cibersecuritarias.

Ante un panorama cibernético que ha seguido evolucionado y aumentando exponencialmente la complejidad y los tipos de ciberamenazas en la red, cabe preguntarse si el texto de la nueva EO de Donald Trump mantiene la misma hoja de ruta trazada por Obama, o si, por el contrario, el nuevo presidente está tomando un nuevo rumbo ante este tema de crucial importancia para EEUU. La respuesta, como veremos a continuación, es que por mucho que se potencie el eslogan *"Make America Safe Again"*, atendiendo a los títulos de las órdenes ejecutivas, parece advertirse una cierta continuidad en el camino a seguir.

2. Análisis de las Executive Orders

La primera orden ejecutiva sobre ciberseguridad de Barack Obama, la EO 13636 , "Improving Critical Infrastructure Cybersecurity" del 12 de febrero de 2013, estaba encaminada a poder implementar las cuestiones de ciberseguridad que afectaban a las infraestructuras críticas, como resultado de la serie de ciberataques acontecidos hasta la fecha que dejaban en evidencia la vulnerabilidad de dichas infraestructuras en EEUU.

Al igual que en épocas anteriores se dejaron desasistidas las infraestructuras terrestres como la red de carreteras estatales y la red de trenes, en ese momento estaba repitiéndose el mismo escenario, pero esta vez con las infraestructuras críticas virtuales, por lo que éstas se presentaban tremendamente vulnerables ante cualquier ataque cibernético. Para solucionarlo, se debía producir un aumento de la colaboración entre los actores implicados, tanto públicos como privados, y, a la vez, garantizar la privacidad y las libertades civiles. "In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks."

La segunda EO sobre ciberseguridad de Obama, la EO 13694, " Blocking the Property of of Framework for improving Critical Infrastructure Cybersecurity Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" del 1 de abril de 2015, enfocaba su campo de acción en la necesidad perseguir a todos los actores que estuvieran realizando actividades delictivas en el entorno cibernético. Esta EO permitía a las agencias del gobierno el bloqueo

de la propiedad y la imposición de sanciones a las personas o actores que estuvieran implicados en acciones ciberdelictivas como el ciberespionaje industrial o las filtraciones de información sensible procedentes del ámbito comercial o securitario.

Tras la firma de la orden ejecutiva, se siguió trabajando en el tema de forma intensa, y en octubre de 2015 la administración de Obama sacó adelante la Estrategia Nacional de Ciberseguridad y el Plan Estratégico, (CSIP) y, en febrero de 2016, el Plan Nacional de Seguridad Cibernética (CNAP).

La tercera y última orden ejecutiva sobre ciberseguridad de Obama, la EO 13757, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities", del 28 de diciembre de 2016, nace forzada por el ciberataque ruso al proceso electoral de EEUU y avalada por el informe JAR "*GRIZZLY STEPPE – Russian Malicious Cyber Activity*" desarrollado por el Departamento de Seguridad Nacional (DHS) y el FBI. Cabe apuntar que el propio título de esta tercera EO anticipa que ésta va a ser un elemento adicional destinado a perfeccionar la ya citada EO 13694 de 2015. La EO 13757 pone el énfasis en penalizar los actos ciberdelictivos a través de las reformas necesarias que velen por la legitimidad de los procesos democráticos. Asimismo, se apuesta por ampliar la severidad de las sanciones.

La primera orden ejecutiva de Donald Trump, la EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", del 11 de mayo de 2017, se centra en incrementar la ciberseguridad de la Red Federal Norteamericana y de las infraestructuras críticas, pero no hace ninguna referencia al ciberataque preelectoral sufrido. La EO 13800 contiene tres líneas de acción fundamentales **claramente continuistas** en la línea de Obama: La primera línea es la ciberseguridad de las Redes Federales; la EO insta a incorporar a todos los departamentos vinculados de una u otra forma con el tema y solicita una modernización de dicha red federal. La segunda línea es la ciberseguridad de las infraestructuras críticas. La tercera línea de acción se dedica a la ciberseguridad de la Nación, trabajando desde varios frentes: desde la disuasión y protección hasta la cooperación internacional, pasando por la educación en ciberseguridad.

Como advertían los analistas del Washington Post, Karen DeYoung y Philip Rucker, estamos ante una EO que revisa las áreas ya puestas en marcha por la administración de Obama en materia cibersecuritaria: "There is little apparent controversy in the draft executive

order to strengthen cybersecurity, a six-page document that in tone and substance could have been written by the Obama administration. It calls for no bold initiatives but rather for review of areas Trump's predecessor had already scrutinized."

3. Conclusión ¿Continuismo en la transición Cibernética?

Se hace evidente que hasta ahora **Trump está continuando la labor de Obama**, al menos sobre el papel, con respecto a las líneas generales a seguir en lo que se refiere a cuestiones cibersecuritarias. Las órdenes ejecutivas sobre ciberseguridad, hasta ahora aprobadas por ambos presidentes, mantienen un propósito claro de proteger las infraestructuras críticas del país ante el riesgo de sufrir nuevos ciberataques tanto por actores estatales, como por no estatales. Pero también se ha hecho evidente que, si bien Trump ha mantenido las políticas iniciadas por Obama, existe un asunto en el que Trump parece no ha mantenido la misma hoja de ruta: el asunto de la intromisión rusa en las elecciones norteamericanas a través de la ventana del ciberespacio. Algo que sí había iniciado Obama en su última EO 13757 y que Trump en su EO 13800 no profundiza de forma explícita. En estos últimos meses, el escenario ha seguido evolucionando y volviéndose más complejo en lo que se refiere al asunto de la EO 13757 de Obama: El Presidente Trump ha destituido al director del FBI, James Comey; el FBI está investigando las injerencias de Rusia en las elecciones de EEUU con un fiscal independiente; y el Consejero de Seguridad Nacional, Michael Flynn, se ha visto forzado a dimitir en relación a unos encuentros con el embajador ruso en Washington. Estos asuntos de importancia estructural demuestran que el ciberespacio es el nuevo escenario de luchas de poder y que el caso de las injerencias rusas en las elecciones presidenciales, a pesar de ser un ataque a la línea de flotación del sistema democrático norteamericano, no es una prioridad para Trump. El inquilino de la Casa Blanca tiene una perspectiva diferente a Obama en lo que respecta al ciberataque ruso. El 7 de julio de 2017, en la Cumbre del G-20, Trump ha hecho unas declaraciones al respecto, antes de su primer encuentro con Putin, alegando que el ciberataque podría haber sido ruso o podría haber sido de otro país. Igualmente, el Secretario de Estado de EEUU, Rex Tillerson, afirmó que quieren olvidar el tema de las injerencias rusas en las elecciones para centrarse en cuestiones de futuro, como la ciberseguridad y el terrorismo. Tras el encuentro con lider ruso, Donald Trump lanzó un tweet el 9 julio de 2017: "Putin & I discussed forming an impenetrable Cyber Security unit so that election hacking, & many other negative things, will be guarded."

Todo esto nos hace entender que, una vez más, queda sin penalizarse un acto bélico en el ciberespacio. Tenía razón Obama cuando ya advertía en Stanford en 2009 que el ciberespacio es como el nuevo "*wild west*".