>> Jorge Dávila

Lo llamaban disuasión

Los Estados Unidos acaban de publicar su nueva Estrategia Nacional de Ciberseguridad y en ella remarcan cuáles van a ser sus objetivos en este conflictivo medio. Además de mostrar su convencida propiedad casi exclusiva de esta 'dimensión', la administración Trump opta por erguir los Carnyx[1] de guerra y amenaza con tomar medidas frente aquellos que les molesten en su camino. Lo quieren llamar "disuasión", pero no está claro si tal cosa puede existir en un medio como internet. En cualquier caso, siempre es inteligente analizar lo que preparan los poderosos para nuestro futuro a medio plazo

Como colofón de la estación estival, los funcionarios de la Casa Blanca han optado por, entre otras cosas, sacar en septiembre su nueva Estrategia Nacional de Ciberseguridad[2]. Al igual que muchos otros grandes documentos de cualquier administración, no sólo de la norteamericana, el documento está lleno de grandes palabras y unas frases un tanto manidas. Sin embargo, en todos estos documentos de referencia siempre hay algo de verdad y conviene hacer el esfuerzo de leérselos con espíritu indagador y, a poder ser, crítico para intentar ver lo que se nos viene encima.

Para empezar, la administración Trump reconoce directa y explícitamente que el ciberespacio es un componente esencial de todos los aspectos de la vida norteamericana, además de la de su economía y defensa, y por ello debe asegurarse de preservar como tal ese ciberespacio para las nuevas generaciones (las de ellos).

La idea es la de Patria, la de defender sus redes de telecomunicaciones, sus sistemas, las funcionalidades que desempeñan y los datos que albergan, procesan y deducen. La nueva política de Ciberseguridad de los EE.UU. pretende promover prosperidad del país haciendo crecer una próspera economía digital que sea segura, así como fomentando la innovación interna. A la par, también persigue preservar su paz y seguridad fortaleciendo su capacidad para disuadir y, si es necesario, castigar a aquellos que usan herramientas cibernéticas con fines maliciosos.

En el debate 'redes abiertas o cerradas', debe ser que a los EE.UU. le sale mucho más a cuenta dejar florecer las redes rabiosamente abiertas, ya que un objetivo confeso de esta nueva toma de posición interna y externa que es la estrategia de ciberseguridad, es expandir la influencia estadounidense en el extranjero y extender los principios de una internet abierta, interoperable, confiable y segura.

No sin algo de razón, la Administración Trump recuerda que el auge de internet y la imparable permeación del ciberespacio en todas las facetas del mundo moderno son contemporáneas con "*el auge de los Estados Unidos como superpotencia única del mundo*".

La realidad es que los norteamericanos quieren una Internet libre pero controlada por ellos, de modo que puedan circular todas las ideas, siempre que vayan adecuadamente ponderadas por los secretos algoritmos de Google, y que ellos puedan analizarlas y almacenarlas si procede, como llevan haciendo desde que internet es internet.

Y dice esto para luego quejarse lastimosamente de que "sus competidores" se benefician de la naturaleza abierta de internet mientras que se apresuran a limitar el acceso de sus ciudadanos a ella, a la vez que minan los principios de una Internet Libre en los foros internacionales. La redacción apunta claramente a los "malos oficiales" de esta administración que son Rusia y China, pero quizás también se refiera a esas propuestas inglesas de prohibir el cifrado seguro en internet y dejar que todos vean todo lo que circula en ella.

La realidad es que los norteamericanos quieren una internet libre pero controlada por ellos, de modo que puedan circular todas las ideas, siempre que vayan adecuadamente ponderadas por los secretos algoritmos de Google, y que ellos puedan analizarlas y almacenarlas si procede, como llevan haciendo desde que internet es internet.

Lo más descarado de este documento de la Casa Blanca es que acusa a otros de esconderse detrás del concepto de soberanía para "*violar de manera imprudente las leyes de otros estados al participar en perniciosas actividades de espionaje económico y actividades cibernéticas maliciosas, causando con ello trastornos económicos significativos y daños a individuos, intereses comerciales y no comerciales, y gobiernos de todo el mundo*". Sin embargo, y sin olvidarnos de Rusia y China, hay que recordar que una parte muy significativa, probablemente mayoritaria, del ciberespionaje en internet lleva la marca de los EE.UU. y sus cuatro ojos restantes[3].

La Estrategia de Ciberseguridad de Trump manifiesta su infantil victimismo diciendo que "*ellos ven el ciberespacio como un escenario donde el abrumador poder militar, económico y político de los Estados Unidos podría ser neutralizado y donde los Estados Unidos y sus aliados y socios son vulnerables*". Y por eso…, ¡deben defenderse!

Como en el caso de atacar hay que hacerlo al competidor que tienes más cerca, la administración Trump no desaprovecha la oportunidad de acusar a China de "*estar involucrada en el espionaje económico cibernético y en el robo de billones de dólares en forma de propiedad intelectual*"; lo cual es probablemente cierto, pero convenientemente se les olvida decir que probablemente no haya sido China la única que lo ha hecho.

Para continuar con los tópicos típicos de este tipo de documentos gubernamentales, –no solo los de Trump, sino en los de los demás también–, no se puede resistir a decirle al gran público que también hay actores no estatales, terroristas y delincuentes, que explotan el ciberespacio para "*obtener ganancias, reclutar, hacer propaganda y atacar a los Estados Unidos y sus aliados y socios, con sus acciones a menudo protegidas por estados hostiles*". No sé si documentos como estos los lee el gran público o se lo leen los periodistas que escriben sobre ellos, pero es necesario resaltar el doble rasero que hay en acusar los EE.UU. a otros de "*obtener ganancias, reclutar, hacer propaganda*" cuando es exactamente eso lo que hacen ellos y sus

[1] Ver https://fr.wikipedia.org/wiki/Carnyx
[2] Ver https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[3] Ver https://en.wikipedia.org/wiki/Five_Eyes

empresas desde la internet que creen suya.

Si no me creen, sigan leyendo y lleguen a la fanfarria del Credo en la que no ocultan que "*el enfoque de la Administración respecto del ciberespacio está anclado en los valores estadounidenses perdurables, como la creencia en el poder de la libertad individual, la libre expresión, los mercados libres y la privacidad*." Luego dicen que mantienen su compromiso con una internet "*abierta, interoperable, confiable y segura*" pero…, ¿para quién? ¿para todos o para unos pocos?

Por si había alguna duda, el documento señala claramente cuáles son sus enemigos "*Rusia, China, Irán y Corea del Norte que utilizan el ciberespacio como un medio para desafiar a los Estados Unidos y a sus aliados*". Y dice todo esto como si Alemania, Francia, Reino Unido e Italia no estuviesen también hasta las cejas en esto del espionaje con fines económicos. Si alguien quiere conocer cómo realmente funciona eso de la Geoestrategia[4], que consulte algunos títulos interesantes[5] que hay al respecto.

Objetivos directores

En concreto, los objetivos directores de la Estrategia de Ciberseguridad de Trump son: **1)** la defensa de su patria protegiendo sus redes, sistemas, funciones y datos; **2)** promover la prosperidad estadounidense con una economía digital segura y próspera que fomenta la innovación nacional; **3)** preservar su paz y seguridad fortaleciendo **su capacidad de disuadir y, si es necesario, castigar** a quienes usen herramientas cibernéticas con fines maliciosos; y **4)** expandir la influencia estadounidense y conseguir una internet abierta, interoperable, confiable y segura.

Está claro que los Estados Unidos están dispuestos a ir contra cualquier actividad que consideren contraria a un comportamiento "responsable" en el ciberespacio, y que piensan disuadir tales desviaciones a través de la imposición de costes (sanciones) tanto cibernéticas como no cibernéticas. A diferencia de muchos otros países, los Estados Unidos realmente sí están en posición de utilizar capacidades cibernéticas y físicas para lograr sus objetivos de seguridad nacional.

Frentes concretos

Dejando las grandes palabras atrás, la estrategia aporta frentes concretos en los que habrá que trabajar como son **1)** centralizar la gestión y monitorización de la ciberseguridad federal, **2)** alinear las actividades IT con la gestión de riesgo evitando duplicidades y aumentando la eficiencia, **3)** mejorar la **gestión del riesgo en las cadenas de suministro** de manera que se puedan excluir proveedores, productos y servicios que puedan ser peligrosos, **4)** aumentar la ciberseguridad de las empresas (*contractors*) que trabajan para el estado monitorizándolas e interviniendo en ellas si es preciso, y **5)** protegerse de la amenaza potencial que supondrían los Computadores Cuánticos desarrollando y estandarizando algoritmos de clave pública post-cuánticos como concesión a algo que está de moda.

Otro frente que la Estrategia considera mejorable es la seguridad de las Infraestructuras Críticas. En este caso, se empieza amenazando con perseguir, aplicar sanciones económicas y tomar represalias contra los que las ataquen y sus promotores como parte de una estrategia común de disuasión.

La estrategia aporta frentes concretos en los que habrá que trabajar, como por ejemplo el de protegerse de la amenaza potencial que supondrían los Computadores Cuánticos desarrollando y estandarizando algoritmos de clave pública post-cuánticos como concesión a algo que está de moda.

Acciones prioritarias en IC

Las acciones que marca como prioritarias serían **1)** redefinir roles y responsabilidades en el mundillo de las Infraestructuras Críticas, **2)** utilizar las tecnologías de la información y las comunicaciones como habilitadores de una nueva ciberseguridad, **3)** proteger la democracia en lo que a la implementación de los sistemas electorales se refiere, **4)** incentivar la inversión en ciberseguridad, **5)** priorizar la investigación y desarrollo nacionales, **6)** mejorar la ciberseguridad de la marítima mercante, y **7)** mejorar la ciberseguridad en el espacio exterior donde considera que tiene acceso sin restricciones y con la libertad para operar libremente para promover la seguridad, la prosperidad económica y el conocimiento científico de los EE.UU.

También el cibercrimen tiene cabida en la Estrategia de Ciberseguridad de los EE.UU., ya que se fija como objetivo combatir los delitos informáticos y mejorar los informes sobre incidentes. La Administración norteamericana presionará para garantizar que se cuente con la autoridad legal y los recursos necesarios para combatir el cibercrimen transnacional, incluyendo la identificación y el desmantelamiento de redes de distribución, *dark-markets* y cualquier otra infraestructura utilizada en el delito informático, así como para combatir el espionaje económico.

Para ello las fuerzas del orden público trabajarán con la industria privada para enfrentar desafíos como son las **tecnologías de anonimización y cifrado**, en lo que a la obtención de evidencias y pruebas se refiere. Eso requiere modernizar el código penal y las leyes de vigilancia electrónica de modo que se otorguen nuevas capacidades a las fuerzas de seguridad para obtener pruebas, destruir instalaciones criminales, e imponer las consecuencias pertinentes para los ciber-actores que sean maliciosos según la ley americana. Eso requiere mejorar la capacidad de identificación, detención y extradición de los cibercriminales que se encuentren fuera de las fronteras de los EE.UU.

EE.UU. va animar a que los países se adhieran a nuevas normas de derecho internacional que indiquen lo que es un comportamiento estatal responsable y aceptable en el ciberespacio. Se propone establecer estándares que hagan que el ciberespacio tenga una mayor previsibilidad y estabilidad.

Talento propio

Algo que resalta en este documento es que se hable de construir y mantener un mecanismo de canalización del talento propio a través de la educación universitaria. Así mismo, también incluye el concepto de re-educación o reciclado de trabajadores en temas de ciberseguridad, huyendo de la mera "concienciación" que tanto se menciona a este lado del Atlán-

[4] Ver https://en.wikipedia.org/wiki/Geostrategy

[5] Pedro Baños: "Así se domina el mundo: Desvelando las claves del poder mundial". Noviembre de 2017. Editorial Ariel ISBN-13: 978-8434427174

tico. Para ello la Administración Trump sigue apoyando el programa conocido como **"National Initiative for Cybersecurity Education"** (NICE).

En el apartado "*Preserve Peace through Strength*" se incorpora de forma irreversible el ciberespacio al resto de elementos que componen el poderío de los EE.UU., poniendo como objetivo de la estrategia "*identificar, contrarrestar, interrumpir, degradar y disuadir cualquier comportamiento en el ciberespacio que sea desestabilizador y contrario a los intereses nacionales*", al tiempo que se amplía la presencia de los Estados Unidos en y a través del ciberespacio.

Para ello va animar a que los países se adhieran a nuevas normas de derecho internacional que indiquen lo que es un comportamiento estatal responsable y aceptable en el ciberespacio. Se propone establecer estándares que hagan que el ciberespacio tenga una mayor previsibilidad y estabilidad.

Con ello queda abierta la puerta para establecer lo que no es aceptable en el ciberespacio y así poder hacer que "*todos los instrumentos del poder nacional están disponibles para prevenir, responder y desalentar la actividad cibernética malintencionada contra los Estados Unidos. Esto incluye capacidades diplomáticas, de información, militares (tanto cinéticas como cibernéticas), financieras, de inteligencia, de atribución pública y de aplicación de la ley*".

Estados Unidos opta por construir una Disuasión en el Ciberespacio o Disuasión Cibernética mediante la imposición de consecuencias por parte de EE.UU. y en concierto con países de ideas afines. Para ello se desarrollarán estrategias "a medida" para asegurar que los adversarios entiendan las consecuencias de su comportamiento cibernético malicioso.

Está claro que los planes de Trump son claramente belicosos y que lo hacen en un terreno muy resbaladizo. Por mucho que se empeñen algunos, **la atribución de acciones en el ciberespacio es muy difícil, por no decir que es imposible**. Por lo que todos estos planes pueden acabar siendo acciones de matonismo o gansterismo más que legítimos derechos a la autodefensa. Aunque lo llamen "disuasión" realmente no se trata de tal cosa cuando puedes terminar siendo atacado o aniquilado por acusaciones no probadas ni verificables. Se está disfrazando de disuasión lo que en realidad es coacción mediante la amenaza y el recurso al terror.

En el mundo real hay cientos de casos en los que esas mismas administraciones han manipulado la escena para que parezca lo que no es y acusen a otro de lo que ellas han hecho. Un ejemplo diáfano de ello son los denominadas **"Operaciones de Falsa Bandera"**[6].

Estados Unidos opta por construir una Disuasión en el Ciberespacio o Disuasión Cibernética mediante la imposición de consecuencias por parte de EE.UU. y en concierto con países de ideas afines. Para ello, se desarrollarán estrategias "a medida" para asegurar que los adversarios entiendan las consecuencias de su comportamiento cibernético malicioso.

Las fuerzas del orden público trabajarán con la industria privada para afrontar desafíos como son las tecnologías de anonimización y cifrado, en lo que a la obtención de evidencias y pruebas se refiere. Eso requiere modernizar el código penal y las leyes de vigilancia-e de modo que se otorguen nuevas capacidades a las fuerzas de seguridad para obtener pruebas, destruir instalaciones criminales e imponer las consecuencias pertinentes para los ciberactores que sean maliciosos.

En 2005 la policía iraquí en Basora detuvo a soldados británicos del Regimiento de Reconocimiento Especial que se dedicaban a disparar a las fuerzas de seguridad iraquíes e intentaban colocar bombas simulando ser terroristas. Los soldados fueron liberados a la fuerza por el ejército británico mediante la destrucción de la cárcel donde estaban detenidos.

En relación con los atentados de Bali en 2002, el expresidente de Indonesia Abdurrahman Wahid admitió que policías y oficiales militares indonesios tuvieron un papel destacado en el atentado y en causar 202 muertos, todo ello para poder culpar de ello a los fundamentalistas islámicos de la Jemaah Islamiya.

Si queremos ir más atrás podemos remontarnos al denominado "Incidente del Golfo de Tonkìn" (1964) que fue una invención del presidente Lyndon B. Johnson para implicar a la opinión pública estadounidense en la guerra de Vietnam. Según la versión de la Casa Blanca, varios botes vietnamitas habrían abierto fuego contra el destructor norteamericano USS Maddox, anclado en las costas de Vietnam. Se sabe que esa historia era y es totalmente falsa gracias a documentos posteriormente desclasificados de la NSA. La entrada de los EE.UU. en la guerra de Vietnam fue un proyecto al que se había negado Kennedy, quien fue oportunamente asesinado apenas ocho meses antes de la declaración formal de guerra por parte de Lyndon B. Johnson.

Si queremos otro ejemplo, miremos al incendio del Reichstag el 27 de febrero de 1933 y que fue atribuido por el gobierno electo de Adolf Hitler a los comunistas y socialistas alemanes, pero muy probablemente fue orquestado por los mismos nazis para declarar el "estado de emergencia" y así poder pasar de leyes a decretos, sin la intervención del parlamento.

Todos estos y muchos ejemplos más muestran lo difícil que es atribuir, incluso en el mundo físico, las autorías de cualquier acción cuando los implicados son estados, ejércitos o agencias de inteligencia. Realmente no se va a poder llegar a la atribución de las acciones en el ciberespacio, y todo este discurso no es más que una tapadera para justificar que la administración Trump y otras afines, estén dispuestas a "campar por sus respetos" en el ciberespacio y que la ley del más fuerte impere.

Quizás el ciberespacio termine siendo la "piedra de toque" que ponga de manifiesto esa falacia que se llama Derecho Internacional, y que desde luego no se puede cumplir en el ciberespacio si no hay una atribución previa y verificable de los autores de cualesquiera actos. ■

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

[6] Ver https://washingtonsblog.com/2015/02/41-admitted-false-flag-attacks.html