EL CIBERESPACIO, NUEVO ESCENARIO DE CONFRONTACIONES.

Por: Rodrigo Bernardo Ortega. 01/12/2020

Foto: *http://www.cubadebate.cu/noticias/2017/11/13/the-new-york-times-ciberataque-sacude-cimientos-de-la-agencia-de-seguridad-nacional-de-eeuu/#.X8Va-WhKjIU*

Hasta hace muy poco tiempo se conoció de un ciberataque dirigido en contra de las Naciones Unidas en el verano de 2.019. Aunque intentó mantenerse en el anonimato, se pudo conocer que los servidores de la red informática de la ONU en Ginebra y Viena sufrieron sendos ataques cibernéticos, en particular las oficinas dedicadas a la protección de los derechos humanos y el departamento de recursos humanos.

El representante de la organización, Stéphane Dujarric, dijo con muchos titubeos que no se informó a la opinión pública del suceso pues no se logró determinar con precisión los alcances de las acciones. Sin embargo, hay mucho por esclarecer en esta circunstancia y suena más a excusa que cualquier otra cosa las declaraciones del alto funcionario. Al margen del acontecimiento, el ataque a la ONU, habla de una nueva dinámica a la que estaremos abocados en los próximos años: un escenario de confrontación cibernética. Por supuesto, este tipo de temáticas despierta suspicacias por parte de diversos actores, entre ellos, el gobierno de los Estados Unidos, siempre tan atento en la reconfiguración de escenarios de disputa geopolítica.

https://www.muyseguridad.net/2020/01/10/puede-iran-ganar-una-ciberguerra-a-estados-unidos/

En efecto, el ciberespacio constituye hoy por hoy un nuevo instrumento de influencia política en el sistema internacional. Los grandes poderes mundiales pugnan por establecer su dominio en diversas zonas de influencia. El propósito de este tipo de estrategias ha sido articular espacios de control que generen un ambiente de constante dependencia a la tecnología y la ciberseguridad. Este escenario es muy similar a las descripciones realizadas por el teórico argentino Raúl Prébisch sobre la *teoría de la dependencia* en el marco de sus reflexiones como Secretario Ejecutivo de la Comisión Económica de las Naciones Unidas para América Latina y el Caribe (CEPAL). De acuerdo con Prébisch y los cepalinos, existe una dinámica entre centro y periferia en la cual los Estados industrializados explotan recursos y medios de producción que son llevados a sus naciones, transformados y vendidos como bienes y servicios a los países emergentes desde donde se extrajeron dichos recursos. De esa manera, se genera un círculo vicioso de dependencia en donde los países del centro aseguran su subsistencia mediante el domino y la explotación de las naciones periféricas.

En las actuales circunstancias está sucediendo algo similar: el control del

ciberespacio por parte de poderosos gobiernos como el de Estados Unidos, busca construir en torno suyo un conjunto de Estados leales y subalternos a sus caprichos.

Esta nueva dinámica daría origen al “cibervasallaje” en el que Washington puede prolongar su dominio histórico, por ejemplo, en países como Colombia. Así pues, ya no sólo se utilizaría el territorio mediante la ocupación de facto con el establecimiento de bases y mandos militares, sino además con la creación de centros de espionaje cibernético para llevar a cabo ataques sorpresivos a naciones enemigas del imperio norteamericano. De hecho, no debe perderse de vista como declara Daniel Markuson (experto en tecnologías digitales) que en este año 2.020 habrá más de 80 elecciones en todo el mundo, por lo cual no es difícil predecir que tanto políticos como hackers tratarán de entrometerse en la elección de los votantes.

En el caso norteamericano, esto aplica no solamente en las elecciones en su propio territorio, sino en las elecciones que pueda llegar a tener influencia. Nuevamente, encontramos a Colombia, en donde el hastío del pueblo a la clase política tradicional ha llegado a niveles importantes, de ahí que las elecciones de 2.022 tengan el foco de poderes internacionales por un posible viraje a un gobierno progresista. En todo caso, debe considerarse que la Casa Blanca no perderá fácilmente su poder sobre uno de sus Estados vasallos más leales.

En consecuencia, a causa del pobre desarrollo tecnológico que tiene una nación como Colombia, puede llevar a convertirla en presa fácil de las ambiciones de Washington. Por tanto, sumado al servilismo económico y político de vieja data (que inició incluso con la declaración de independencia de España), ahora se suma una subordinación en términos cibernéticos que traería nefastos resultados para el interés nacional colombiano. No obstante, es tradicional esa noción servil y rastrera con la que la élite política de Bogotá ha servido a los intereses de sus jefes del norte. Ahora bien, el peligro inmediato que puede derivarse de una circunstancia como aquella es que a mediano y largo plazo puede llevar a la desestabilización de gobiernos que contravengan las órdenes de Washington y generar una situación de autoritarismo tecnológico. Haciendo un parangón con otras épocas, la influencia del Pentágono puede llevar a crear nuevos escenarios de control sobre América Latina al estilo de las truculentas dictaduras de mediados del siglo XX.

https://es.wikipedia.org/wiki/Cibercomando_de_Estados_Unidos#/media/Archivo:2010-05-14-USCYBERCOM_Logo.jpg

La situación más preocupante es la ausencia de regulación internacional del ciberespacio, por lo cual ningún país puede sentir salvaguardadas sus redes informáticas gubernamentales. No en vano, uno de los miedos más radicales de Whasington es el inicio de una posible ciberguerra con Irán, pues la nación persa puede realizar ataques híbridos en los que se combine sabotajes y ataqueshaciendo uso de drones para arremeter en contra de las instalaciones petroleras desocios de Estados Unidos como Israel o Arabia Saudita. No debe olvidarse, sinembargo, que el primer saboteador del mundo duerme en la Casa Blanca y que, porello, las redes informáticas de infraestructura crítica y militar de otros países, estánen riesgo por las ambiciones de ese gobierno. El gran cambio que se ha generadoen las dinámicas actuales es el hecho de pensar en otros escenarios de guerra en elcual ya no enfrentan dos ejércitos convencionales, sino un grupo de hackers quepueden generar devastación a poblaciones enteras.

Es claro que Washington ve el ciberespacio como un territorio de guerra en el que cualquier país puede convertirse eventualmente en un competidor informático y agresor potencial de ese país. En este escenario, Estados Unidos está promoviendo un sistema de seguridad informático internacional bajo la égida de la ONU, estrategia que tiene dos intenciones:

Por una parte, asegurarse el control internacional, eliminando la injerencia de “pequeños países”, pues todo ello se gestionaría desde el Consejo de Seguridad y, en segunda medida, ponerse en situación de paridad con otros grandes poderes mundiales como China o Rusia y así evitar ataques sorpresa.

En este sentido, la regulación internacional del ciberespacio será determinante para que Estados Unidos pueda erigirse como un actor relevante dentro del concierto internacional. Es oportuno recordar en esta circunstancia que la carrera armamentista está siendo progresivamente reemplazada por otro tipo de competencia global. Estamos asistiendo a una nueva Guerra Fría en la que los diferentes Estados se disputan posiciones estratégicas, pero en territorios etéreos y deslocalizados.

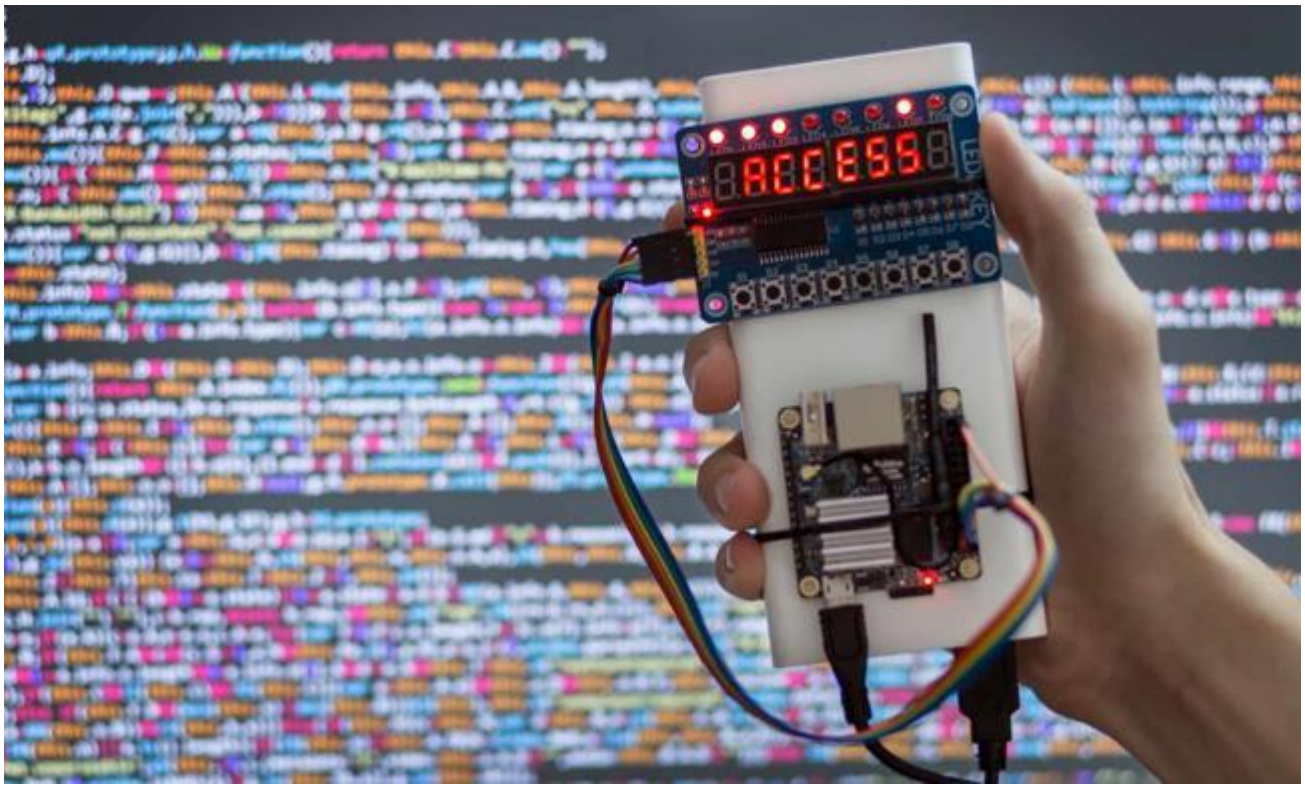
http://www.juventudrebelde.cu/suplementos/informatica/2017-02-22/el-nuevo-universo-y-la-intimidad-cero

Para ilustrar lo anterior, tenemos el caso de la guerra comercial entre Estados Unidos y China que inició a mediados de 2.019 y que tuvo como telón de fondo el origen y propagación de la tecnología 5G, carrera que la Casa Blanca se niega a perder. El aumento de aranceles por un supuesto desbalance comercial sólo fue la excusa impulsada por la administración Trump al ver cómo el gigante chino Huawei se adelantaba definitivamente en la consecución de una tecnología móvil capaz de ofrecer mayor velocidad, menor tiempo de latencia y mayor cantidad de equipos que pueden conectarse a una misma base. De manera que las recientes decisiones

adoptadas por el magnate-presidente son tan sólo pataletas de ahogado frente al imparable ritmo de la tecnología china. Ahora, el gobierno Trump va detrás del gigante de compras online Alibaba tras despacharse contra la aplicación Tik Tok, según se dijo por “razones de seguridad”. El problema es que Washington buscará influenciar a sus gobiernos vasallos para que persigan su misma directriz. El mensaje es claro: “el único que puede espiar al mundo y generar guerras cibernéticas es Estados Unidos”.

Por esa razón, es fundamental destacar las palabras de Roberto Uzal, director de la maestría en ciberdefensa y ciberseguridad de la UBA en Argentina: “entre países no hay amigos ni enemigos: sólo hay intereses compartidos y muy acotados en el tiempo”. Esta frase resume en buena medida el fenómeno al que nos estamos enfrentando.

Mientras el gobierno de Colombia, liderado por un pseudopresidente cree y repite ser un “socio estratégico” de Washington, la realidad es que es un simple servidor de los intereses del imperio del magnate-presidente. Pero no debe escatimarse el hecho de que Estados Unidos está siendo consciente de su debacle internacional. En efecto, la pandemia del coronavirus ha puesto en evidencia el poco nivel de respuesta que tiene la Casa Blanca para gestionar una situación de estas dimensiones, por lo que entregar el estandarte de líder mundial es algo que se avizora en un futuro cercano (Ver Coronavirus e Imperios). Sin embargo, el Pentágono peleará con las fuerzas del herido para continuar siendo un importante referente mundial, de ahí que la ciberguerra se configure como un posible escenario de renacimiento de los poderes imperiales.



https://www.muyseguridad.net/2020/07/20/ciberguerra-ataque-iran-israel/

Otro de las profundas consecuencias que se pueden derivar del actual fenómeno es el ciberpatrullaje. So pretexto de mantener información diáfana en torno al número de contagios por coronavirus, los servicios de inteligencia de varios países han estado patrullando y extrayendo información de la ciudadanía en diversas partes del mundo. Como si se tratara de gobiernos autoritarios, el propósito de estas acciones es ejercer control a como dé lugar. En este punto ya debe sonar familiar la estrategia del Pentágono después de los atentados a las torres gemelas, donde se promovió un ambiente de “salvaguardar la seguridad internacional”, algo que derivó en la persecución e invasión de países en Medio Oriente. Pues bien, actuando de manera similar, Washington busca promover una campaña de persecución por diversos medios empleando la tecnología para eliminar a sus adversarios.

A manera de epílogo podemos mencionar que las ciberguerras no son un asunto de ciencia ficción. Por el contrario, son confrontaciones muy reales que permitirán a ciertos Estados (re)posicionarse en el plano internacional. Esta circunstancia ha surgido como un nuevo camino de disputa y ha recordado las carreras tecnológicas propias de la Guerra Fría. Por esa razón, Estados Unidos como poder en decadencia está llamado a reconfigurar sus estrategias para evitar perder su poder

de influencia en el mundo. El objetivo central de la Casa Blanca será articular una compleja red de influencias capaz de crear en torno suyo una serie de “cibervasallos” desde donde espera seguir ejerciendo control del destino político del mundo. Nunca en la historia de la humanidad había existido un Estado tan terco a la hora de aceptar su debacle como potencia, razón por la cual, los Estados libres del mundo deben estar atentos para no perder su independencia informática en detrimento de las más odiosas ambiciones imperiales.

Fecha de creación
2020/12/01