OBSERVATORIO DE POLÍTICA INTERNACIONAL

El Pentágono y su estrategia de ciberseguridad

Mayo 2021

Josefina Pighin[1]

En un mundo tan interconectado regido por el paradigma de la globalización, y reconociendo la importancia y el papel preponderante de la tecnología en nuestra vida.

En el extremo norte de América se encuentra el tan emblemático Estados Unidos, país en donde nació Internet en 1968, con el conocido nombre de ARPANET en plena Guerra Fría. Alberga más de la mitad de los gigantes tecnológicos que toman las riendas del plano internacional en 2021, entre ellos podemos nombrar, Apple, Amazon, Samsung, Microsoft, Intel, IBM, Facebook, Google, y muchas otras, que, a su vez, compiten con Tencent Holdings, Alibaba y Baidu de origen chino.

Otro dato para entender el lugar de la tecnología en nuestra era, es que seis de las diez empresas más valiosas del mundo, son de tecnología. Además es el sector estrella dentro de la economía estadounidense, de aquí derivamos a unos cuantos datos importantes para analizar. La balanza tecnológica estadounidense hace unos cuantos años está en positiva, este término hace alusión a la capacidad que tiene un país de exportar tecnología y de utilizar su propia producción, una relación directa entre mayor dan los números de la balanza tecnológica, mayores son los esfuerzos de un estado en materia de Investigación y Desarrollo. Y casualmente, Estados Unidos lidera el grupo de países que más invierten en estos campos.

En el presente artículo trataremos la creciente importancia de la tecnología a nivel mundial, haciendo foco en Estados Unidos, adentrándonos en a forma en que la ciberseguridad se convirtió en el plano principal de atención para los gobiernos.

Un dato a tener en cuenta es que según la Revista Forbes, el valor de mercado de Microsoft actualmente es de 1.400 billones de dólares, seguido por Apple, para dimensionar el capital y los ingresos que tienen estas empresas estadounidenses y el lugar que ocupan en el PBI nacional.

En los últimos años se experimetno una desaceleración de la producción china en esta materia, pero observamos según las estadísticas que la influencia de la tecnología en la economía global continuó creciendo con un récord de 161 compañías. Frente a este

[1] Estudiante avanzada de Relaciones Internacionales. Miembro del Observatorio de Política Internacional de la Facultad de Derecho y Ciencia Política de la Universidad Católica de Santa Fe.

panorama de inmensurable incremento tecnológico y de las conocidas TICs a nivel mundial, analizamos que el único actor capaz de hacerle frente a Estados Unidos de forma tan pareja, menester resaltar que es su adversario hace ya unos años en la famosa “guerra comercial”. China, el gigante asiático con un crecimiento exponencial de su población y producción en masa, ya no más de calidad china, sino que competitivos en el mercado. Podemos ver una tendencia generalizada en cuando a China, cuanto más espacio gana a nivel internacional, la Casa Blanca disminuye su participación en el mismo.

No podemos dejar de pensar en la estrategia del Pentágono en materia de ciberseguridad, como se esperaban es un tema de controversia para este artículo. Obama es el primer mandatario que pone sobre la mesa el tema de la ciberseguridad, logró entender hace ya varios años, que Internet entraba en su auge.

En 2015, por primera vez, luego de varios ciberataques, se habla de esta realidad como hechos tangibles y desestabilizadores del sistema estadounidense. "Las amenazas cibernéticas son urgentes y un peligro creciente" destaco Obama en un breve discurso en el Centro Nacional de Ciberseguridad, a las afueras de Washington. “El ataque a Sony, la cuenta de Twitter [del Ejército] pirateada por simpatizantes de yihadistas islámicos demuestran que el sector público y privado tienen que hacer mucho más trabajo en fortalecer nuestra ciberseguridad”. (FAUS, 2015) Durante el mismo año y frente a este panorama la Casa Blanca propuso una legislación en materia de ciberseguridad, la cual fue aprobada por la Cámara de los Representantes, pero en el Senado no causo mucho entusiasmo. Como podemos ver, la ciberseguridad dejaba de ser un tema meramente privado, y se insta por la cooperación entre los ámbitos públicos y privados trabajen juntos para la protección de los datos de los ciudadanos. Esto género bastante controversia, ya que, el gobierno se puso su propio limite frente a la monitorización total de las personas y su gran acceso a la información privada.

Tal y como nos indica la historia estadunidense, se desarrolló dentro de los servicios de inteligencia y dentro del mismo gobierno un sentimiento de temor frente a un nuevo 11S cibernético. Es complejo nombrar “un nuevo 11S”, por el impacto social que genero este ataque alrededor del globo, pero para explicarlo mejor, hace referencia a un hecho inesperado causante de mucho daño y perdida de popularidad y legitimidad del “policía del mundo” en un nuevo ámbito en donde el estado puede ser objeto de amenazas.

Otra de las emblemáticas propuestas de esta ley fue la aprobación para el Presidente de declarar una “emergencia cibernética”, esto consistía en que se puedan “desenchufar” las redes privadas y "desconectar" los sitios de internet que son considerados como una

amenaza a la seguridad nacional. Esto dio mucho que hablar ya que generaba una clase de superponer del gobierno, y como sabemos, el poder y atribuciones sin límites no son buenas. Como en todo dilema hay partes en contra y partes a favor, en este plano encontramos a la Electronic Frontier Foundation una ONG con sede en San Francisco defensora de los derechos digitales, expreso en ese mismo año la incomodidad generado por las nuevas propuestas, "El presidente tendría un poder sin límites para determinar cuáles servicios pueden estar conectados al internet o incluso que tipo de contenido podría diseminarse en una emergencia cibernética", explica el abogado de EFF, Kevin Bankston, en una entrevista con el sitio web especializado en tecnologías de la información CNet, "nuestras inquietudes no han cambiado".

Lo propuesto es que el gobierno de los Estados Unidos de América reaccionara a las amenazas y ataques cibernéticos de la misma forma en que lo hace en otros campos, esto genera mucha incomodidad a nivel internacional, porque como ya sabemos, si bien la Casa Blanca es el primer actor que enarbola los valores de la paz y democracia, es el también el primero en enviar tropas a Afganistán luego del 11S, y de respaldar dictaduras en Latinoamérica para evitar la intromisión soviética.

Fruto de la filtración de datos personales de más de 22 millones de personas de la Oficina de Administración de Personal de Estados Unidos en julio de 2015. Genero una gran preocupación y entrada en acción del gobierno, ya que entendían que no sólo era una amenaza al estado en sí, sino a los sistemas financieros y de salud que operan en redes conectadas a través de Internet.

Hace un año, el policía del mundo pensando que tenía todo bajo control, se desayunó con uno de los ciberataques más importantes de su historia, más de 18.000 agencias del Gobierno y empresas fueron hacheadas, si bien es imposible determinar los culpables, se sabe cuál fue es blanco preciso de estos ataques: Departamento de Energía, y, dentro de éste, la Administración Nacional de Seguridad Nuclear, cuya misión es el mantenimiento y mejora de las aproximadamente 5.800 bombas atómicas que oficialmente tiene Estados Unidos. Lo que sorprende es que la magnitud del ataque es desmesurado, y llega hasta España. Todo esto se vuelve más grave, al incorporar la variable que dentro del ciberespacio se puede paralizar a un estado, como lo hizo Rusia con Estonia en 2007, sin estar en un marco de hostilidades. Otro factor a tener en cuenta es la poca mediatización del hecho, el gobierno no lanzo ningún informe sobre la situación, y el entonces presidente Donald Trump, se limitó en su cuenta de Twitter a hablar sobre el tema.

Cuando pensamos que era suficiente, en el trascurso del 2021 el Pentágono sufre otro nueva ciberataque de una inmensidad avasallante, el día domingo nueve de mayo fue el elegido por el gobierno para declararse en estado de emergencia regional, desencadenado por un ciberataque a la más grande red de oleoductos del país.

Los hackers autores del desastre lograron robar más de 100MG de información sobre esta red que transporta más de 2,5 millones de barriles por día, el 45% del suministro de diésel, gasolina y combustible que consumen los aviones de la costa este. Esto no fue todo lo negativo, sino que la inactividad de la red por toda la noche del viernes de esa semana, según expertos, generara un aumento del 2% al 3% de los combustibles, pero si estos apagones se dan con mayor frecuencia, la situación se agravara. Podemos analizar como la inactividad cuesta más que un daño físico. La única información que se tiene es que los autores son un grupo de hackers llamados Dark Side, antes del hecho, su líder expreso en sus redes sociales que el objetivo era económico y negó estar vinculado con ningún gobierno. Esto es llamativo, ya que se piensa que algunos, todos o sólo uno de los participantes de este grupo se encuentra en Europa del Este, si bien China está en la mira, el Kremlin no queda atrás y los servicios de seguridad culpan a este.

En el ciberespacio, el atacante normalmente tiene la ventaja de encontrar nuevas formas de entrar en un sistema antes de que el defensor pueda cerrar esa grieta. Si tenemos algo en claro, es que la ciberseguridad es un campo en que todavía no fue conquistado por nadie, además supone dificultades mucho mayores que en cualquier otro, lo más dificl es rastrear a los responsables, su ubicación geográfica y, creemos los peor de todo, cual es la gravedad de la situación con la información robada.

Todavía hay mucho que trabajar en este momento de la humanidad, pero si algo estamos convencidos, es que Internet es un nuevo campo de batalla, y que Estados Unidos pierde su preponderancia cada vez que China gana espacio a nivel internacional. Estamos atentos de cómo seguirá

Finalmente como reflexión personal, destacamos que la información hoy cotiza mucho más que acciones en cualquier empresa multinacional, construye la credibilidad de un gobierno, con imágenes políticas, en resultados de lecciones y en la forma en que fluctúan las redes financieras mundiales. Así como lo valoriza, lo puede tirar todo en un sólo segundo.

“La idea más destacada del siglo XXI es que los organismos son algoritmos, y que los algoritmos pueden piratear a los organismos.” (ABC Cultural, 2018) dice Yuval Noah Harari en una entrevista.

Bibliografía

ABC Cultural. (Septiembre de 2018). Obtenido de https://www.abc.es/cultura/cultural/abci-yuval-noah-harari-tecnologia-podra-sustituir-gente-completo-201809020113_noticia.html

BBC, R. d. (16 de Diciembre de 2016). *BBC News Mundo*. Obtenido de https://www.bbc.com/mundo/noticias-internacional-38336691

Corera, G. (Diciembre de 2020). *BBC News Mundo*. Obtenido de https://www.bbc.com/mundo/noticias-internacional-55381892

Cosoy, N. (Junio de 2011). *BBC News Mundo*.

FAUS, J. (Enero de 2015). *EL PAIS*. Obtenido de elpais.net: https://elpais.com/internacional/2015/01/13/actualidad/1421180628_845380.html

LABORDE, A. (Febrero de 2021). *EL PAIS*. Obtenido de https://elpais.com/internacional/2021-02-23/ee-uu-prepara-sanciones-contra-rusia-por-el-ciberataque-masivo-a-agencias-federales-y-el-caso-navalni.html

Prado, P. (18 diciembre 2020). *EL MUNDO.* Obtenido de ELMUNDO.ES : https://www.elmundo.es/internacional/2020/12/18/5fdd06d6fdddff6a158b45df.html