CÁMARA DE DIPUTADOS
LXV LEGISLATURA
40 Aniversario Investigación Parlamentaria
CEDIP
CENTRO DE ESTUDIOS DE DERECHO E INVESTIGACIONES PARLAMENTARIAS

ANÁLISIS GEOPOLÍTICO Y ASUNTOS INTERNACIONALES

ANALÍTICA DE LA BELIGERANCIA RUSO-UCRANIANA PARTE III. INDUSTRIA Y CIBERATAQUES

20 DE MAYO DE 2022

Irving Ilie GÓMEZ LARA[1]

El denominado Complejo Bélico Industrial (CBI) de los Estados Unidos se caracteriza por las sinergias existentes entre un grupo de empresas, sus mandos administrativos, la cúpula militar que toma las decisiones en el Pentágono y una clase política dirigente aglutinada en un sistema político bipartidista en torno a lo que se ha denominado el Triángulo de Hierro.[2] Tal apreciación, surgida desde el basamento teórico de la Sociología del Conocimiento,[3] busca dar cuenta de que el denominado 1% de la población de nuestro vecino del norte[4] toma decisiones a partir de sus intereses particulares como el de garantizar la acumulación y reinversión de la ganancia mediante los principios de maximización de costos y de la operación industrial con capacidad instalada ociosa.[5]

Otro de los principios reinantes en el CBI es el de realizar contratos económicos para la mejora, desarrollo y despliegue de sistemas armamentísticos para hacer frente a amenazas –reales o probables– que puedan vulnerar su seguridad nacional o volverse un obstáculo para el desarrollo pleno de los negocios e intereses de las empresas vinculadas en los contratos. Esto quiere decir que en la entrega de contratos económicos se privilegia a aquellas empresas cuyo poder dominante les permite tomar decisiones al interior del Triángulo de Hierro.[6] Si bien lo anterior no es algo sorprendente, lo relevante es que ocurren impactos supraliminales y subliminales[7] en el conjunto de la población cuando se observa el despliegue de los sistemas de armas en un contexto de situación límite, es decir, cuando son activados los protocolos de guerra.

Tal situación, que ha sido relatada a lo largo de las anteriores entregas de esta serie de boletines sobre el análisis contencioso en Europa oriental, tiene un matiz de primer orden en el ciberespacio, toda vez que fue el primer escenario de beligerancia entre Rusia, Ucrania, Estados Unidos y el conjunto de la Organización del Tratado del Atlántico Norte. Minutos antes de que iniciaran los bombardeos rusos con artillería móvil, destructores y lanzaderas de misiles en territorio ucraniano con movimientos evolventes de las tropas de infantería y los regimientos de fuerzas especiales con el objetivo de destruir los batallones ucranianos –que el gobierno ruso califica de neonazis–, aislar

1 Investigador A adscrito a la Dirección de Estudios Jurídicos del Centro de Estudios de Derecho e Investigaciones Parlamentarias de la Cámara de Diputados, maestro en Estudios Latinoamericanos por la Universidad Nacional Autónoma de México.

2 DOMHOFF, G. William, ¿Quién gobierna Estados Unidos?, México, Siglo XXI editores, 1990, pp. 20-92.

3 MILLS, Charles Wright, *Poder Política Pueblo*, México, Fondo de Cultura Económica, 1973, pp. 3-116.

4 STIGLITZ, Joseph E., *El precio de la desigualdad*, México, Editorial Taurus, 2012, pp. 47-100.

5 Cuando se otorga un contrato para el desarrollo y construcción de un sistema de armas (tanques, aviones, barcos, etc.) se solicita a la empresa que recibirá el contrato por parte del Departamento de Defensa de Estados Unidos que tenga las instalaciones adecuadas para producir la cantidad de armamento estipulado en el contrato y que dichas instalaciones provean, en un escenario de guerra, de los sistemas de armas necesarios para pelear en ella, lo que implica que tengan la capacidad instalada necesaria para aumentar la producción en el corto plazo. *Véase* NADAL EGEA, Alejandro, *Arsenales Nucleares. Tecnología decadente y control de armamentos,* México, El Colegio de México, 1991, pp. 20-111.

6 SAXE-FERNÁNDEZ, John, *La compra-venta de México*, México, Plaza & Janés, 2002, pp. 337-476.

7 *Véase* FROMM, Erich, Ética y Psicoanálisis, México, Fondo de Cultura Económica, 1986, pp. 15-130.

los centros industriales, destruir la infraestructura logística y de aprovisionamiento y cancelar, en el largo plazo, la salida al mar Negro y al mar de Azov, se realizó un ataque informático contra la empresa de comunicaciones satelital Viasat, proveedora de servicios informáticos, de mando y control, de comunicaciones y de rastreo satelital tanto del gobierno como del ejército ucraniano.

El ataque se desplegó mediante el uso del *malware AcidRain contra los módems y enrutadores de Viasat, borrando rápidamente todos los datos del sistema*,[8] con lo que se dejó ciego y sordo al ejército y gobierno de la exrepública soviética. Lo más importante del ciberataque, en un contexto donde no se encuentra regulada la ciberguerra por el derecho internacional, es que se caracteriza como un ataque universal (entendido contra todos los sistemas computacionales existentes en el planeta) porque el *malware* se replica entre los servidores interconectados de las empresas y gobiernos de todo el mundo, creando amenazas probables en el ciberespacio y, por lo tanto, la vulnerabilidad estratégica de toda la información planetaria se devela como objetivo de guerra.

Ahora bien, no sólo los ciberataques contra las entidades estatales son motivo de preocupación, también lo son las violaciones a la privacidad de los ciudadanos que despliegan las grandes empresas que constituyen uno de los mercados oligopólicos más influyentes del mundo: los proveedores de tecnología, servidores y servicios de diferente tipo en el ciberespacio; por ejemplo: El Consejo Irlandés por las Libertades Civiles (ICCL, por sus siglas en inglés) recientemente publicó un reporte donde señala que la empresa *Google* permite que más de 4,600 empresas, de todos los sectores económicos, tengan acceso a lo que *la gente ve en línea y su ubicación en el mundo real 178 billones de veces cada año en EE. UU. y Europa*, una industria, *Real-Time Bidding* (RTB), con un valor de más de 117 mil millones de dólares.[9]

El reporte presentado exhibe la profundidad de esta posible violación de datos, mientras que en Estados Unidos una persona tiene un rango de exposición al RTB del orden de 747 veces al día, en el viejo continente es de 376 veces al día por persona, dichas exposiciones son enviadas por igual a cualquier parte del mundo (incluso Rusia y China) *sin ningún medio para regular lo que se hace con los datos*.[10] En este sentido, es poco favorable la información sobre estos fenómenos en México pero dada la penetración y despliegue relativo de las tecnologías de información y comunicación, su rango de probabilidad de ocurrencia pudiera ser elevado.

Las posibles vulnerabilidades a la seguridad nacional y a la privacidad de la información de los ciudadanos de nuestro país pueden tornarse en asuntos de seguridad ciudadana, estratégica y militar, ya que no poseemos las tecnologías asociadas al ciberespacio que nos permitan cerrar las brechas de seguridad, por ello se vuelve necesario repensar el papel central que juega la investigación y desarrollo en ciencias básicas que se realiza en México. Todo lo anterior aún sin considerar las dimensiones económico-financieras, como la confiscación de activos, congelamiento de cuentas o el posible control extranjero del valor de las acciones de las empresas nacionales, fenómeno que se estudiará en próximas entregas de este boletín Geopolítico y de Asuntos Internacionales.

Finalmente, los retos para México son enormes por lo que la mejora, perfeccionamiento y confección de normatividad jurídica en materia de ciberseguridad es una necesidad que se ha ido atendiendo de forma adecuada por el Congreso. Al mismo tiempo, dada la alta dependencia a las tec-

8 O'NEILL, Patrick Howell, *Una hora antes de la invasión, los hackers rusos ya habían atacado Ucrania*, MIT Tecnology Review, 17 de mayo de 2022, https://www.technologyreview.es//s/14225/una-hora-antes-de-la-invasion-los-hackers-rusos-ya-habian-atacado-ucrania

9 IRISH COUNCIL FOR CIVIL LIBERTIES, *The biggest data breach. ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe*, ICCL, 16 de mayo de 2022, https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf.

10 *Idem.*

nologías cibernético-digitales (servidores, módems, satélites, redes de telecomunicaciones, etc.), resulta esencial que se discuta la posibilidad de crear un ente institucional en el Estado mexicano que coordine, aglutine y establezca planes y programas para hacer frente a los diferentes escenarios polemológicos del siglo XXI.

Asimismo, ante las mejoras y perfeccionamiento potencial de la doctrina de seguridad nacional que establezca cuáles son las amenazas latentes en el ciberespacio y categorice los vectores de ciberguerra, ciberseguridad, ciberataque y ciberdefensa, es prudente que desde la H. Cámara de Diputados se abran espacios de debate público, como parlamentos abiertos, y en consecuencia se pondere crear una legislación que atienda estos fenómenos.

REFERENCIAS

1. *Bibliohemerográficas*

DOMHOFF, G. William, ¿Quién gobierna Estados Unidos?, México, Siglo XXI editores, 1990.

FROMM, Erich, Ética y Psicoanálisis, México, Fondo de Cultura Económica, 1986.

IRISH COUNCIL FOR CIVIL LIBERTIES, *The biggest data breach. ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe*, ICCL, 16 de mayo de 2022.

MILLS, Charles Wright, *Poder Política Pueblo*, México, Fondo de Cultura Económica, 1973.

NADAL EGEA, Alejandro, *Arsenales Nucleares. Tecnología decadente y control de armamentos,* México, El Colegio de México, 1991.

O'NEILL, Patrick Howell, *Una hora antes de la invasión, los hackers rusos ya habían atacado Ucrania*, MIT Tecnology Review, 17 de mayo de 2022.

SAXE-FERNÁNDEZ, John, *La compra-venta de México*, México, Plaza & Janés, 2002.

STIGLITZ, Joseph E., *El precio de la desigualdad*, México, Editorial Taurus, 2012.