ANÁLISIS GEOPOLÍTICO Y ASUNTOS INTERNACIONALES

ANALÍTICA DE LA BELIGERANCIA RUSO-UCRANIANA PARTE II. BATALLAS EN EL CIBERESPACIO

13 DE MAYO DE 2022

Raúl Adrián HUERTA RODRÍGUEZ[1]

Cumpliéndose dos meses de que las tropas rusas comenzaran sus acciones beligerantes en Ucrania y que, como se explicó en el análisis anterior, se trata de un acontecimiento bélico que debe entenderse como una guerra híbrida de envergadura mundial, durante la última semana de abril el *Cooperative Cyber Defence Centre of Excellence* (o simplemente CCDCOE) de la Organización del Tratado del Atlántico Norte (OTAN)[2] realizó la décima edición de uno de los más grandes eventos anuales de juegos de ciberguerra en Tallin,[3] la ciudad capital de Estonia, ubicada a menos de 400 kilómetros de la segunda urbe más importante y poblada de Rusia: San Petersburgo.

Acorde con su sitio web oficial, el CCDCOE se autodefine como *un centro multinacional e interdisciplinario de ciberdefensa* para la investigación, entrenamiento y realización de ejercicios enfocados en cuatro núcleos principales: la tecnología, la estrategia, las operaciones y el derecho. Respecto a este último rubro, y siendo transversal al núcleo tetracompuesto del Centro, destaca el *Manual de Tallin 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas* de 2017, que es un documento ampliado de la primera edición publicada en 2013.[4]

Este Centro fue creado el 14 de mayo de 2008 y acreditado en octubre de ese mismo año como Organización Militar Internacional de la OTAN. Ubicado en Estonia, está financiado e integrado por Austria, Bélgica, Bulgaria, Canadá, Croacia, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Irlanda, Italia, Japón, Letonia, Lituania, Luxemburgo, Montenegro, el Países Bajos, Noruega, Polonia, Portugal, Rumania, Eslovaquia, Eslovenia, Corea del Sur, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos. Desde 2010, ha organizado los llamados *Locked Shields*, que son los ejercicios internacionales más grandes a nivel mundial de ciberdefensa con fuego real.

Hasta este momento, la dimensión ciberdigital todavía no se ha desplegado como una trinchera formal dentro del teatro de operaciones ruso-ucraniano, o al menos no se ha visibilizado tanto como otras formas de beligerancia, pese a que, por un lado, Rusia haya estado sufriendo los más intensos ciberataques de su historia,[5] y por otro, se hayan contabilizado casi cuarenta ciberataques

1 Investigador C adscrito al Centro de Estudios de Derecho e Investigaciones Parlamentarias de la Cámara de Diputados, doctor en Filosofía por la Universidad Iberoamericana, Ciudad de México.

2 Centro de Excelencia de Ciber-Defensa Cooperativa.

3 MCLAUGHLIN, Jenna, *Estonia hosts NATO-led cyber war games, with one eye on Russia*, NPR, 2 de mayo de 2022, https://www.npr.org/2022/05/02/1095008257/estonia-nato-cyber-war-games-russia#:~:text=Press-,Estonia%20hosts%20NATO%2Dled%20cyber%20war%20games%2C%20with%20one%20eye,only%20added%20to%20the%20stakes.

4 NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, *Sitio web oficial*, (11 de mayo de 2022), https://ccdcoe.org/.

5 ALONSO, Rodrigo, *El Kremlin reconoce que Rusia sufre la peor ola de ciberataques de su historia*, ABC, 18 de marzo de 2022, https://www.abc.es/tecnologia/redes/abci-kremlin-reconoce-rusia-sufre-peor-ciberataques-historia-202203180042_noticia.html.

de tipo DDoS,[6] *phishing*[7] y *malware*[8] que si bien no han podido ser comprobados como acciones no-kinéticas por parte del Kremlin, se tiene registro de que fueron iniciados en territorio ruso o ejecutados por empresas u organizaciones aliadas en contra de Ucrania, y que han estado coordinados con las acciones kinéticas en el teatro de guerra.[9]

Lo importante a resaltar del evento realizado en la nación báltica es que los simulacros interactivos de ciberseguridad en los que participaron más de 2,000 expertos provenientes de 32 países, así como gobiernos y compañías privadas, es que dichos ejercicios en los que la finalidad era ayudar a defender las regiones de Berylia (una nación insular imaginaria en conflicto con su también inexistente vecino del sur, Crimsonia), tuvieron como horizonte el hecho altamente probable y cercano de ataques digitales destructivos por parte de Rusia en contra de Ucrania y sus aliados occidentales, principalmente los que conforman la Alianza militar del Atlántico a la que siguen intentando sumarse más países como Suecia y Finlandia, por no decir Ucrania misma, y ante lo cual Rusia ha prometido represalias técnicas y militares en caso de concretarse, sobre todo por parte de Finlandia, ya que sería una amenaza para su seguridad por la proximidad que las fuerzas armadas de la OTAN podrían alcanzar en sus fronteras.[10]

Para comprender la enorme relevancia de este particular evento de ciberseguridad y ciberdefensa internacionales, allende el *factum* de que la esfera ciberdigital es una dimensión de gran importancia táctica y estratégica en la operatividad militar actual, en los protocolos de seguridad nacionales de muchos Estados y que es el elemento principal de diferenciación específica en la forma de guerra híbrida, tal como se mencionó en el análisis anterior, que es determinante en toda organización sociopolítica, hay que recordar dos hechos que brindan el sustento histórico justificativo de la urgencia para la generación del marco regulativo y el fundamento jurídico y estratégico que posibiliten la creación de protocolos en caso de ciberataques de cualquier tipo, magnitud y en cualesquiera que sean las infraestructuras y sistemas informáticos.

Así pues, en primera instancia hay que recordar que tras la desintegración del bloque soviético en 1991 y las subsecuentes independizaciones de varias regiones que antes formaban parte de la

6 DDoS (*Distributed Denial of Service*) es el ataque de denegación de servicio distribuida en sitios web basado en la saturación de sus capacidades para funcionar mediante sobrecargas de solicitudes de acceso.

7 Usualmente realizados por medio de correos electrónicos con el objetivo de robar información confidencial.

8 También ejecutados a través de correos electrónicos, son programas maliciosos que pueden, entre otras cosas, robar, borrar o bloquear los datos de equipos computacionales y servidores, así como controlarlos remotamente.

9 SÁNCHEZ, Valentina T., *Ciberataques, el cuarto campo de batalla en la invasión rusa a Ucrania*, France 24, 5 de marzo de 2022, https://www.france24.com/es/programas/ciencia-y-tecnolog%C3%ADa/20220305-ciberataques-el-cuarto-campo-de-batalla-en-la-invasi%C3%B3n-rusa-a-ucrania. Destaca en este aspecto el reporte realizado por Microsoft intitulado *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine*. Digital Security Unit, 27 April 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd; *véase* también DEUTSCHE WELLE, *Rusia coordina ataques cibernéticos y militares en Ucrania, según Microsoft*, 28 de abril de 2022, https://www.dw.com/es/rusia-coordina-ataques-cibern%C3%A9ticos-y-militares-en-ucrania-seg%C3%BAn-microsoft/a-61615216. Asimismo, el pasado lunes 21 de marzo, el presidente de EE.UU., Joe Biden, advirtió sobre la alta probabilidad de ciberataques a su nación e instó a las empresas estadounidenses a que mejoraran sus ciberdefensas, sobre todo las de infraestructuras críticas. SINK, Justin y MANSON, Katrina, *Rusia tiene preparado ciberataque contra EU, advierte Biden*, El Financiero, 21 de marzo de 2022, https://www.elfinanciero.com.mx/mundo/2022/03/21/rusia-tiene-preparado-ciberataque-contra-eu-advierte-biden/.

10 GARDNER, Frank, *El ingreso de Suecia y Finlandia a la OTAN ¿es una amenaza o un estímulo para Europa?*, BBC News, 11 de mayo de 2022, https://www.bbc.com/mundo/noticias-internacional-61373742; POZA MAUPAIN, Pedro, *Finlandia apoya una adhesión "sin demora" a la OTAN*, El Mundo, 12 de mayo de 2022, https://www.elmundo.es/internacional/2022/05/12/627cb58b21efa0b55d8b45e7.html; EUROPA PRESS, *Rusia promete a Finlandia "represalias de carácter militar" si se une a la OTAN*, 12 de mayo de 2022, https://www.europapress.es/internacional/noticia-rusia-promete-finlandia-represalias-caracter-militar-si-une-otan-20220512132014.html.

Unión de Repúblicas Soviéticas Socialistas (URSS), entre las que se encuentra precisamente Estonia, esta novel nación atravesó por un proceso revolucionario de digitalización que le ha posicionado como uno de los poquísimos países cuyos servicios gubernamentales y privados son digitales casi en su totalidad.

El segundo evento paradigmático acaeció en el año 2007 cuando Estonia demostró los catastróficos peligros de ser un país hiperconectado y altamente dependiente de las estructuras digitales. La decisión gubernamental de trasladar la estatua del Soldado de Bronce (originalmente llamado *Monumento a los Libertadores de Tallin*, que para los rusos es una representación de su victoria sobre el nazismo, mientras que para los estonios, por el contrario, es un símbolo rememorativo de la opresión que sufrieron por medio siglo a manos del ejército rojo), derivó en dos días de revueltas masivas y saqueos que fueron atizados con noticias falsas, tácticas de guerra de información y uno de los casos de ciberataques más grandes jamás perpetrados que inhabilitaron los servicios en línea de bancos, agencias mediáticas y órganos gubernamentales estonios durante varias semanas.[11] A raíz de estos catastróficos eventos que tuvieron como saldo la muerte de una persona, miles de detenidos y el colapso económico, político y social de Estonia, la ciberseguridad se convirtió en una de las cuestiones más importantes de desarrollo, fomento e inversión por parte del gobierno.

Con los antecedentes mencionados y los recientes eventos en materia de ciberseguridad que tienen como horizonte probable que los frentes de batalla se amplíen al ciberespacio, resuenan las campanadas premonitorias de una cuestión extremadamente delicada que el Estado mexicano ha de priorizar y elaborar las normatividades referentes a la dimensión ciberdigital que son fundamentales para la seguridad y el aseguramiento de la soberanía nacional.

Considerando las experiencias de otras naciones en relación a la tecnológica, marco jurídico y estructura en materia de ciberespacio, México podría tener como camino el analizar escenarios en materias protocolos y mecanismos técnicos, jurídicos y criminalísticos que en todo caso permitiesen conjuntar políticas y acciones concretas para proteger tanto a la población mexicana de los cibercrímenes como a las vitales estructuras computacionales y ciberdigitales del país ante posibles ataques de individuos, grupos o Estados que podrían colapsar profundamente el orden interno y la soberanía de nuestra nación.

REFERENCIAS

1.*Bibliohemerograficas*

ALONSO, Rodrigo, *El Kremlin reconoce que Rusia sufre la peor ola de ciberataques de su historia*, ABC, 18 de marzo de 2022.

DEUTSCHE WELLE, *Rusia coordina ataques cibernéticos y militares en Ucrania, según Microsoft*, 28 de abril de 2022.

EUROPA PRESS, *Rusia promete a Finlandia "represalias de carácter militar" si se une a la OTAN*, 12 de mayo de 2022.

GARDNER, Frank, *El ingreso de Suecia y Finlandia a la OTAN ¿es una amenaza o un estímulo para Europa?,* BBC News, 11 de mayo de 2022.

11 MCGUINNESS, Damien, *How a cyber attack transformed Estonia*, BBC, 27 April 2017, https://www.bbc.com/news/39655415.

MCGUINNESS, Damien, *How a cyber attack transformed Estonia*, BBC, 27 April 2017.

MCLAUGHLIN, Jenna, *Estonia hosts NATO-led cyber war games, with one eye on Russia*, NPR, 2 de mayo de 2022.

MICROSOFT, *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine*, Digital Security Unit, 27 April 2022.

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDCOE), *Sitio web oficial*, (11 de mayo de 2022).

POZA MAUPAIN, Pedro, *Finlandia apoya una adhesión "sin demora" a la OTAN*, El Mundo, 12 de mayo de 2022.

SÁNCHEZ, Valentina T., *Ciberataques, el cuarto campo de batalla en la invasión rusa a Ucrania*, France 24, 5 de marzo de 2022.

SINK, Justin y MANSON, Katrina, *Rusia tiene preparado ciberataque contra EU, advierte Biden*, El Financiero, 21 de marzo de 2022.