>> Jorge Dávila

La Ciberguerra entre los escombros

El drama de la invasión de Ucrania por el ejército imperial ruso a finales del mes de febrero de 2022, ha golpeado irreversiblemente a la sociedad europea y marcará el futuro de Europa en las próximas generaciones. En esta ocasión, el escenario bélico convencional se da sobre un escenario de Tecnologías de la Información nunca antes vista en una guerra. Se pueden percibir los efectos reales del denominado Quinto Escenario y quizás podamos aprender algo de ello. El tiempo permitirá un análisis más detallado y sopesado de lo que aquí está ocurriendo, pero a estas alturas –finales de marzo– podemos echarle un vistazo preliminar a ver si sacamos alguna conclusión.

Es curioso ver cómo la paz suele ser inconsciente hasta que llega la guerra, en ese momento, más o menos todos los ciudadanos empiezan a sospechar que las cosas no estaban tan bien como parecían. Sin embargo, esa conciencia inmanente queda superada rápidamente por alguna idea simple, supuestamente diáfana, que termina explicando todo en pocas palabras y ubicando la culpa de todo siempre lejos de uno mismo, de nuestra sociedad o incluso de nuestro país.

Los que saben de Geopolítica siempre han dicho que el régimen de Putin, como muchos otros regímenes totalitarios a lo largo de la Historia, no duda en recurrir a la guerra y a las economías de guerra para 1) sanear y revitalizar su propia economía, 2) instaurar una unidad (aparente y efímera) entre sus ciudadanos alrededor del concepto de Nación o de Pueblo, 3) expandir su territorio económico y/o militar, y 4) establecer y/o mantener una oligarquía autoritaria de ricos frente a una multitud de siervos pobres.

No nos habíamos quitado las mascarillas y Putin coloca cientos de miles de soldados en las fronteras propias y de estados títere como Bielorrusia con Ucrania, y un 24F empieza una Guerra y una invasión que muchos no esperaban. Sin embargo, los que saben de esto, ven (ahora y entonces) movimientos económicos (controlar la producción de gas, la acumulación de reservas, la gestión internacional de la deuda nacional, el posicionamiento energético en Europa, la censura y reconfiguración de Internet para su mejor control, etc.) que auguraban algo "grande" dentro de los planes del Kremlin. A toro pasado y revisando ahora aquellos datos, está más claro que esta guerra se lleva fraguando años, que era la idea central de la autocracia putiniana y su oligocrática corte de multimillonarios y que, en todo ello, los propios ucranianos nada tenían que hacer.

Esta guerra pone de manifiesto lo que nos gusta a los países en paz: ningunear la geopolítica y desterrar cualquier *situational awareness* que pueda romper la placidez de nuestras cañas en una terraza privada invasora del espacio público. Cuando la realidad se nos impone y ya no podemos seguir negándola, empiezan los lamentos, los golpes de pecho y los espasmos de todo tipo para digerir rápidamente esta nueva realidad no deseada. Algunos se convierten espontáneamente en ONGs y llevan indiscriminadamente materiales para los refugiados; otros se transforman en Agencias de Viajes, que pretenden reubicar a los huidos del horror en vete tú a saber qué ubicaciones y en qué condiciones; otros saltan del sofá en su casa para coger el teclado de su ordenador y alistarse en supuestos ciber-movimientos *hacktivistas* para contratacar desde los suburbios burgueses de las ciudades europeas y de otras demarcaciones.

Cualquiera de esas tres situaciones son ejemplo de la falta de profesionalidad de nuestras sociedades en lo que

Cabría preguntarse si las iniciativas particulares no pueden terminar siendo la excusa para que imperialistas rusos decidan escalar la contienda en Ucrania y considerarlos actos de guerra por parte de las potencias de la OTAN. Tanto para atacar o defender infraestructuras TI, como para prestar ayuda y hospitalidad a los refugiados, la respuesta debería ser más profesional y controlable por parte de los que decimos ser sociedades democráticas, justas y transparentes.

La vieja Europa, atemorizada

Atemorizada, la vieja Europa toma como suya esa guerra y reconoce el flanco ucraniano como un flanco europeo y la UE y toda su población decide condenar la guerra de Putin, la invasión de Ucrania y, sobre todo, la aniquilación de cualquier infraestructura y la masacre de civiles (al estilo de la batalla de Alepo[1]), que claramente representa la esencia de esta estrategia bélica.

Está claro que a los cuerpos de defensa ucranianos no les ha cogido de sorpresa esta invasión y hasta la fecha han demostrado al mundo su capacidad de combatir y de frenar al cacareado segundo (o tercero) más potente ejército de la tierra. Este valor y previsión, aderezado con las armas que pronto se han animado a mandar los demás países europeos –y Estados Unidos–, ha convertido una supuesta invasión relámpago en una guerra convencional mucho más lenta y de la que todavía no hemos visto la fase de guerra urbana y la posible fase insurgente de postguerra.

[1] https://en.wikipedia.org/wiki/Battle_of_Aleppo_(2012-2016)

a la organización social y ciudadana se refiere. Hacer llegar materiales a un país es un problema logístico serio que hay que desarrollar profesionalmente y con mucho control; de lo contrario, pronto florecerá la corrupción y la estafa entre tantas buenas intenciones.

Mover millones de refugiados es algo que hay que tomarse mucho más en serio que dejarse llevar por el llanto de niños, mujeres u hombres que están siendo atacados y despojados de todo. Estamos hablando de seres humanos y no de mascotas por lo que las reacciones viscerales no deberían estar permitidas. No es organizar unas vacaciones de unos días, sino una emigración en la que los desplazados tienen que rehacer completamente y partiendo de nada, sus vidas en otros territorios, en otros idiomas, en otras culturas. Estamos hablando posiblemente de años y no de días, y si no me creen, piensen en cuánto tiempo se tardará en reconstruir las infraestructuras que ahora están triturando las bombas, cohetes y misiles de crucero de la maquinaria de guerra rusa, y de la europea algo también.

Declarada la "ciberguerra" contra Rusia

Algunas cuentas de Twitter que utilizan la identidad colectiva **Anonymous**, el mismo 25F ya habían declarado la "ciberguerra" contra Rusia y reivindicado la autoría de varios ataques informáticos contra instituciones públicas rusas y medios de comunicación al servicio del Kremlin. El primer ataque fue al "canal de propaganda" **RT** (**Russia Today**), cuyo impacto fue sólo el de paralizar la actividad de su web durante algunas horas para que luego se recuperase sin efecto permanente alguno.

Simultáneamente se han dado otras operaciones en el ciberespacio que han sido más interesantes. Por una parte está la banda privada de ciberdelincuentes conocida como **Conti Team**, los cuales no se arrugaron al ponerse al lado de Putin en la Deep Web y beber de los cálices más puros de la servidumbre a la autocracia rusa que les ha permitido realizar libremente y sin consecuencias sus negocios planetarios de extorsión.

Conti Team es uno de los grupos más activos de la industria del cibercrimen. Es un operador de *ransomware* modular (EMOTET, TrickBot botnet, Cobalt Strike, Ryuk) y una de sus armas (Ryuk) es el virus que tumbó múltiples empresas e instituciones públicas españolas en 2020 y 2021, como el SEPE o el **Ministerio de Trabajo**.

Lo único novedoso en esta guerra inesperada (pero previsible) es que las bombas no han conseguido quebrar las redes de comunicación multimedia que adornan nuestro día a día, y hoy cualquiera puede mandar su opinión, sus videos, sus vivencias, sus noticias, al resto del mundo a la vez que suenan las sirenas de ataque aéreo o estallan los cohetes a decenas de metros de distancia.

Antes de la invasión de Ucrania, en el trimestre final de 2021, se realizaron 722 campañas de ataque con *ransomware*, siendo LockBit 2.0 (30 %), Conti (19 %), PYSA (11 %), Hive (10 %), y Grief los virus más utilizados, lo que pone de manifiesto lo boyante que iba el cibercrimen en tiempos de paz.

Las bandas de extorsión, retratadas

La reacción al posicionamiento de Conti Team no se hizo esperar y se la conoce como **Contileaks**, que es una cuenta en Twitter[2] a través de la cual se ha liberado el contenido de los *chats* internos de esa organización (160.000 mensajes de enero 2021 a febrero 2022) y que son un magnífico ejemplo (digno de un estudio calmado y detallista) de lo bien que están organizadas estas bandas de extorsión a muy gran escala. Del análisis de esos datos se obtiene información de gran valor, como son direcciones de Bitcoin empleadas por la banda, el código fuente para las funciones de cifrado y descifrado, así como un constructor de su *ransomware*, el modelo organizativo de la banda (jerarquía, salarios, departamentos, etc.) e incluso guías sobre cómo realizar ataques. Brian Krebs[3] ha publicado en su sitio un análisis de la información más jugosa que se extrae de ellos.

Por otra parte, y relacionados específicamente con la invasión de Ucrania, hay varios ejemplos de *malware* diseñado para funcionar como ciberarmas y ese es el caso de los *wipers* disfrazados de *ransomware* (los *wipers* borran irreversiblemente el almacenamiento de los sistemas atacados). En concreto nos referimos a WhisperGate[4], HermeticWiper[5] e IssacWiper[6]. Con lo que está claro que las facciones pro-rusas estaban dispuestas a iniciar una versión Ciber de lo que las bombas con explosivos químicos ya estaban haciendo sobre la población ucraniana.

Tanto el alineamiento de las bandas privadas a favor de Putin y el Kremlin, como la respuesta etérea del colectivo conocido como Anonymous son iniciativas particulares y no parecen ser iniciativas promovidas por ningún estado. Eso no quiere decir que "a río revuelto" no haya beneficio de pescadores en el este y en el oeste y que, incluso, algunos comandos de ciberguerra rusos, ucranianos u occidentales puedan haberse camuflado detrás de esas iniciativas antes del inicio de las hostilidades.

Tirándose los trastos

Este escenario de organizaciones civiles, de particulares tirándose los trastos en el medio universal que es Internet, no es propiamente una ciberguerra sino más bien una lucha de bandas al estilo de las de Nueva York[7] en 1920 antes de llegar la Mafia italiana. Eso no quita para que sea un enfrentamiento polarizado por una invasión que sí se puede llamar guerra y que sí está promovida por un estado invasor, el ruso, contra un estado víctima, que es el ucraniano.

Aunque se han dado ataques con éxito por parte de Anonymous en los que ha puesto de manifiesto su presencia, sólo unos pocos han aportado

[2] https://twitter.com/ContiLeaks
[3] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/
[4] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
[5] https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/
[6] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
[7] https://en.wikipedia.org/wiki/The_Gangs_of_New_York_(book)

información que puede ser interesante. Lo más avanzado en este frente Ciber quizás sea el "hackeo" por parte de Anonymous a la agencia federal rusa **Roskomnadzor**[8], que es el regulador de la censura de medios en Rusia, y que se ha saldado con la filtración de 800 GB de sus archivos y bases de datos[9] de dicho organismo de control de Putin. Pero, ¿qué le importa a Putin que se sepa en el mundo cómo controla con mano dura y viril lo que sus nacionales reciben como información? Me temo que el valor de esta información es meramente historiográfico.

Por otro lado está el ataque con éxito por parte de Anonymous de la filial alemana **Rosneft Deutschland GmbH**[10] de la gran petrolera rusa con el mismo nombre, y que está presidida por el ex canciller alemán Schröder (está claro, también hay puertas giratorias en Alemania). En esta acción, alguien bajo la careta de Anonymous se hace con información confidencial (20 Tera bytes) de una empresa que forma parte de las **Infraestructuras Críticas de Alemania**. Aunque aseguran que la información conseguida no afecta a las infraestructuras energéticas de Alemania, y declaran que no quieren afectar al sector petrolero, lo cierto es que no han liberado esa información (justificándose en que quieren no favorecer a sus empresas competidoras) y que no está claro quién realmente la está escudriñando.

Las iniciativas particulares, cuestionadas

Habría que preguntarse si estas iniciativas particulares no pueden terminar siendo la excusa para que imperialistas rusos decidan escalar la contienda en Ucrania y considerarlos actos de guerra por parte de las potencias de la OTAN. Mi opinión es que los invasores no necesitan de excusas para escalar hacia arriba o hacia abajo su invasión de territorio ajeno.

En cualquier caso, tanto para atacar o defender infraestructuras TI, como para prestar ayuda y hospitalidad a los refugiados, la respuesta debería ser más profesional y controlable por parte de los que decimos ser sociedades democráticas, justas y transparentes.

Lo único que es novedoso en esta guerra inesperada (pero previsible) es que las bombas no han conseguido quebrar las redes de comunicación multimedia que adornan nuestra día a día, y hoy cualquiera puede mandar su opinión, sus videos, sus vivencias, sus noticias, al resto del mundo a la vez que suenan las sirenas de ataque aéreo o estallan los cohetes a decenas de metros de distancia. La campaña ucraniana sólo representa claramente el triunfo indiscutible de ARPANET[11] después de 56 años.

Más allá de los* defacements *de páginas web, del compromiso de algunas bases de datos en la nube, y la exfiltración de alguna información jugosa de alguna compañía rusa, los ataques Ciber no se pueden comparar al efecto real e histórico de las toneladas de explosivos y proyectiles que están regando con sangre y cascotes los campos de Ucrania, los campos de Europa.

Tal es así que el Ministerio de Estadística ruso ha dado instrucciones a todos los sitios web y servicios estatales para que cambien al sistema de nombres de dominio ruso (DNS .ru), que abandonen los alojamientos en servidores extranjeros, que desactiven cualquier código JavaScript que proceda del exterior y que fortalezcan la política de contraseñas, todo ello antes del pasado 11 de marzo. Con esto, la Rusia de Putin pretende desengancharse de Internet y confinar a todos sus nacionales/residentes a una autarquía permanentemente controlada y monitorizada del Kremlin, al más puro estilo de la Internet disponible en China desde hace ya bastante tiempo.

Tecnológicamente hablando es muy fácil desconectar a un país de la Internet global; de hecho, China lo ha hecho desde hace tiempo y algunos países también lo han conseguido, aunque sólo durante periodos transitorios. En las tecnologías de la información apagar es mucho más fácil que encender, lo que no es tan fácil es mantener una Internet local y soberana y que sus fronteras no sean penetradas por numerosos túneles que, como una hidra, se multipliquen más deprisa de lo que se van cerrando. Todo va a depender de las ganas que tenga el pueblo ruso de quedarse para siempre informativa y culturalmente confinado en su egocentrismo, o lo que es peor, en la eterna contemplación de su Zar. Lo que representa la Internet original (previa a 1995) es un genio al cual no se le puede fácilmente volver a meter en la botella.

Llegado a este punto hay que preguntarse si esto de las ciberguerras, los ciberejércitos, los ciberpatriotas o las ciberguerrillas realmente sirven para algo. El drama ucraniano nos pone delante de la cruda realidad y nos muestra que lo Ciber sólo es importante cuando NO estallan bombas de racimo[12] en el patio de tu casa, y la "madre de todas las bombas" (MOAB[13]) es decir, las bombas termobáricas[14], no te convierten en testigo de las explosiones químicas más potentes posibles.

Más allá de los *defacements* de páginas web, del compromiso de algunas bases de datos en la nube, y de la exfiltración de alguna información jugosa de alguna compañía rusa, los ataques Ciber no se pueden comparar al efecto real e histórico de las toneladas de explosivos y proyectiles que están regando con sangre y cascotes los campos de Ucrania, los campos de Europa. La ciberguerra sólo puede ser efectiva cuando no hay una guerra convencional que la haga palidecer. ■

[8] Servicio Federal de Supervisión de las Telecomunicaciones, Tecnologías de la Información y Medios de Comunicación en Rusia.

[9] Se advierte que directorios como ПОЧТА Приемная, contienen numerosos correos con adjuntos y que esos adjuntos pueden ser un vector típico de malware y enlaces de phishing, por lo que estos datos deben manipularse con herramientas de seguridad como Dangerzone y equivalentes. https://ddosecrets.com/wiki/Roskomnadzor

[10] https://anonleaks.net/en/2022/anonymous-germany/20-terabytes-anonymous-germany-hijacks-data-from-rosneft-germany/

[11] https://en.wikipedia.org/wiki/ARPANET

[12] https://en.wikipedia.org/wiki/Cluster_munition

[13] https://en.wikipedia.org/wiki/GBU-43/B_MOAB

[14] https://en.wikipedia.org/wiki/Thermobaric_weapon y https://en.wikipedia.org/wiki/Dust_explosion

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