ÍNDICE

Capítulo III
PROGRAMA DE DOCTORADO EN SEGURIDAD INTERNACIONAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

OPERACIONES CIBERNÉTICAS DURANTE EL PRIMER AÑO DEL CONFLICTO ARMADO ENTRE RUSIA Y UCRANIA

CYBER OPERATIONS DURING THE FIRST YEAR OF THE ARMED CONFLICT BETWEEN RUSSIA AND UKRAINE

Mariano César Bartolomé[1]
Abril de 2023

Resumen

En febrero del año 2022, Rusia inició una «operación militar especial» en Ucrania invadiendo su territorio. Así, estalló un conflicto armado que todavía se encuentra en desarrollo. Teniendo en cuenta que las operaciones cibernéticas son una parte importante de los conflictos armados modernos, encuadrables en un formato flexible de ciberguerra, nuestro trabajo explora las acciones de ese tipo ejecutadas durante el primer año de hostilidades, por parte de ambos contendientes. Las conclusiones obtenidas confirman que los dos protagonistas emplearon intensamente herramientas cibernéticas de diverso tipo. También se constata el limitado éxito obtenido en esta materia por Rusia, esbozándose explicaciones para esos magros resultados.

Palabras clave: ciberseguridad; ciberataque; ciberguerra; Rusia; Ucrania.

Abstract

In February 2022, Russia launched a «special military operation» in Ukraine, invading its territory. Thus, an armed conflict broke out that is still in progress. Bearing in mind that cyber operations are an important part of modern armed conflicts, which can be framed in a flexible format of cyber warfare, our presentation explores the actions of this type carried out during the first year of hostilities by both contenders. The conclusions obtained confirm that both protagonists made intensive use of cyber

[1] Doctor en Relaciones Internacionales. Profesor permanente (Colegio Interamericano de Defensa, Washington DC).

PhD in International Relations. Permanent Professor (Inter American Defense College, Washington DC).

tools of various types. We also note the limited success achieved in this area by Russia, and outline explanations for these meager results.

Keywords: cybersecurity; cyber-attack; cyberwar; Russia; Ukraine.

1. INTRODUCCIÓN

En febrero del año 2022, Rusia inició una «operación militar especial» en Ucrania, invadiendo su territorio. Así, estalló un conflicto armado convencional con enormes tasas de daño en términos de vidas y bienes materiales, que ya cumplió un año y continúa activo.

Las causas mediatas e inmediatas de la contienda no son objeto del presente trabajo, como tampoco lo es el análisis de las medidas adoptadas por sus máximos decisores en los niveles político y estratégico. Sí interesan, en cambio, las acciones asociadas directamente a este acontecimiento desplegadas en el ciberespacio, definido por los especialistas (Kissinger, 2016; Quintana, 2016) como un entorno virtual de información e interacciones entre personas, sustentado en infraestructuras y sistemas de información y telecomunicaciones. Ese entorno, o dominio, tiene una dimensión de seguridad, a la cual se refiere la ciberseguridad; dentro de este campo se encuadra la ciberguerra, cuyos límites y contenidos son motivo de controversia, en las esferas de la Seguridad Internacional y la Defensa.

De acuerdo con el postulado según el cual las operaciones cibernéticas forman parte indisociable de los conflictos armados modernos (Stevens, 2018; Theiler, 2011), surgen dos interrogantes centrales. El primero de ellos se refiere a la forma y el grado de cumplimiento de tal postulado en el caso ruso-ucraniano, en tanto el segundo gira en torno al encuadre de las operaciones cibernéticas de este caso contemporáneo dentro del concepto ciberguerra. De esta manera, el objetivo principal del presente trabajo consiste despejar esos interrogantes, como también la identificación y análisis de las operaciones cibernéticas ejecutadas por los dos contendientes durante su primer año de desarrollo del conflicto.

El tema elegido aporta a una mayor y mejor comprensión de los aspectos cibernéticos del principal conflicto armado activo, a nivel global. Hasta el momento, esta arista no ha sido abordada en detalle desde el ámbito académico,

por lo cual se lo considera original y un aporte concreto al Estado del Arte del caso. Además, la cuestión contribuye a la actualización del conocimiento disponible sobre los contenidos y límites del concepto ciberguerra, y su aplicabilidad.

El trabajo se estructura en tres partes principales, siendo la primera la presente introducción. En ella se encuentran el objetivo perseguido, la delimitación temporal empleada y ciertas precisiones conceptuales, necesarias para comprender e interpretar de manera adecuada al problema y sus diferentes aristas. La segunda parte se inicia con una discusión sobre el concepto «ciberguerra», su aplicación al caso de estudio en este trabajo, y las condiciones de ese eventual empleo. Con ese marco conceptual, luego se abordan las operaciones cibernéticas que cada contendiente llevó a cabo contra el otro, tanto antes del inicio del conflicto armado, como tras el estallido de las hostilidades. Finalmente, en el espacio de conclusiones generales se interpretan los resultados del trabajo desde el marco teórico y conceptual, con una respuesta a los interrogantes centrales, y se comunican algunos hallazgos.

2. DESARROLLO

2.1. Contenidos y límites del concepto «ciberguerra»

Se anticipó en el espacio introductorio que la ciberguerra se inserta en el marco de la ciberseguridad, que se enfoca en las amenazas y riesgos que surgen y se despliegan en el ciberespacio. Es un concepto que surgió hace ya tres décadas, pero todavía hoy existen controversias y disensos en torno a su significado y, lo que es igualmente importante, su aplicabilidad. En su primera versión, refería a contiendas donde las tecnologías de la información y las comunicaciones serían la principal arma y a la vez el campo de batalla predominante. Implicaba interceptar y destruir los sistemas de comunicaciones digitales del adversario, obteniendo la mayor parte de su información, al tiempo que se lo privaba de la información propia. Esa forma de combate, agregaron luego los responsables de este enfoque, involucra diferentes tecnologías vinculadas al comando y control, a la recolección y procesamiento de datos, y a las comunicaciones, entre otras funciones (Arquilla y Ronfeldt, 1993).

En aquella aproximación inicial, la ciberguerra se circunscribió a la esfera de las operaciones militares, sobre todo de alta y mediana intensidad, mientras

la «guerra de redes» enfocó en el plano civil, tanto entre Estados como al interior de las sociedades (Arquilla y Ronfeldt, 1993, 1995, 1997). Sin embargo, una visión retrospectiva no sólo no indica avances relevantes en el desarrollo de ese concepto, en esas etapas, sino incluso difusos límites con la idea de «guerra de la información» (Schwartau, 1994; Libicki, 1995), que fue la tempranamente adoptada por el Departamento de Defensa estadounidense.

Las acciones ofensivas atribuidas a Rusia en Estonia y Georgia, en 2007 y 2008 respectivamente, corroboraron la transformación del ciberespacio en un nuevo dominio de la guerra, confirmada desde prestigiosos medios periodísticos (*The Economist*, 2010) y académicos (*Lynn*, 2011). Por la desventaja que representa, se vuelve inviable la limitación de las capacidades militares a los dominios convencionales y cobran importancia las ciberarmas. De acuerdo con los criterios de Rid (2013) y Stevens (2018), las ciberarmas pueden ser entendidas como códigos informáticos empleados (o diseñados para ser empleados) con el objetivo de amenazar o causar daño físico, funcional o mental a estructuras, sistemas o seres vivos. Carecen de forma física definida y su carácter inmaterial complica la identificación, intercepción y destrucción.

Las formas de combate cibernéticas son el resultado directo de la existencia de ciberarmas. En el plano interestatal, son motivo de múltiples controversias, pues no son claros sus contenidos ni límites, como tampoco lo son las diferencias de su empleo en tiempos de paz o guerra. Tampoco queda claro cuándo un acto de combate cibernético es considerado un «uso de la fuerza» de acuerdo con el Derecho Internacional Humanitario, ni el tipo de blancos aceptables para ese marco normativo (Hathaway y Klimburg, 2012). Cuando estas formas de combate tienen un sentido ofensivo, dan lugar a un ciberataque: Burton (2015) lo entiende como un esfuerzo para interrumpir, retrasar o destruir redes de computadoras; otra lectura, algo más amplia, refiere a un acto que apunta a recolectar, interrumpir, denegar o destruir recursos de sistemas de información, o la información en sí misma (The Hague Centre for Strategic Studies, 2015).

En este proceso, no se ha logrado un consenso absoluto en torno al concepto de ciberguerra. Dos posiciones, en torno a esta cuestión, pueden identificarse[2]. La primera postula que la ciberguerra es el resultado de una percepción sobrestimada de la peligrosidad de las amenazas cibernéticas, negativamente

[2] Se excluyen deliberadamente de esta tipología aquellos empleos del vocablo «ciberguerra» al solo efecto de llamar la atención sobre la importancia o gravedad del tema, desde una perspectiva periodística

influenciada por una visión realista de las Relaciones Internacionales. Así, los choques interestatales en el plano cibernéticos son escasos y aislados, con tasas de daño limitadas que no se pueden comparar con los efectos de ataques cinéticos (Craig y Valeriano, 2018; Maness y Valeriano, 2018; Valeriano y Maness, 2017). Desde esta perspectiva, la cuestión de los ciberataques ha sido «militarizada», muchas veces por cuestiones domésticas (injerencia en, o control de, las políticas públicas vinculadas con el tema) y económicas (contratos, presupuestos), y dominada por una terminología bélica que distorsiona la realidad (Rid, 2013; Dunn Cavelty, 2012; O'Conell, 2012).

Otra lectura más reciente de la ciberguerra, que podríamos denominar «amplia», la encuadra en un conflicto bélico, trascendiendo la naturaleza militar —o no— de sus protagonistas, que pueden incluir actores no estatales. El dominio cibernético no debe ser, necesariamente, el campo de batalla predominante del evento bélico (Quintana, 2016). Esta perspectiva en mucho más flexible que la inicialmente propuesta por Ronfeldt y Arquilla. En aquella versión original, se otorgaba centralidad a las operaciones cibernéticas dentro de la contienda armada, subrayando el carácter militar de protagonistas y blancos.

En el presente trabajo adoptamos esta visión amplia de la ciberguerra, considerando de manera preliminar que es aplicable al conflicto armado que protagonizan Rusia y Ucrania. Es decir, de manera flexible, englobamos en ese concepto de ciberguerra a las operaciones cibernéticas (ofensivas y defensivas) que se desarrollan en el marco de un conflicto armado, independientemente de la naturaleza de su perpetrador directo o del tipo de blanco. Esas operaciones se combinan con otras acciones, ejecutadas en los restantes dominios y, en tanto formas de combate, encuadran dentro del Derecho Internacional Humanitario, o Derecho Internacional de los Conflictos Armados (Schmitt, 2017; 2013).

2.2. Acciones cibernéticas bilaterales, previas al estallido de hostilidades

Conviene tener presente que, en el momento del conflicto armado con Ucrania, Rusia era considerada una potencia de primer orden en el panorama de la ciberseguridad y la ciberguerra. La literatura especializada da cuenta de su responsabilidad en la ejecución de diversos ciberataques, a lo largo de los últi-

---

que no está acompañada por un desarrollo conceptual. El trabajo de Richard Clarke (2011), que rápidamente se constituyó en un éxito de ventas en los Estados Unidos, es un buen ejemplo.

mos tres lustros. Algunos de ellos tuvieron amplias repercusiones en el campo de la Seguridad Internacional (Bartolomé, 2022).

En ese contexto, las operaciones cibernéticas contra Ucrania, atribuidas directa o indirectamente a Rusia, no son novedosas. Sus antecedentes pueden rastrearse casi hasta inicios de siglo, aunque estas actividades se multiplicaron una década más tarde, cuando las relaciones bilaterales sufrieron un severo deterioro, tras los eventos conocidos en Ucrania como *Euromaidan* y el derrocamiento del presidente prorruso Viktor Yanukovich. Como correlato de estos hechos, Rusia ocupó y anexó la península de Crimea, justificando la acción *a posteriori* con un plebiscito local de controvertida legitimidad. Ese aumento llevó a apreciar retrospectivamente que Ucrania se había tornado en un verdadero campo de pruebas, «patio de juegos» (Martin, 2022) o «cocina experimental» (Barker, 2022) para las operaciones cibernéticas ofensivas de Rusia.

Durante ese lapso, en sentido inverso, numerosos grupos ucranianos de *hackers* se enfocaron en sitios web oficiales de Rusia, así como en correos electrónicos de altos funcionarios de ese país, para exfiltrar información útil a los intereses de su país. En 2016, uno de esos grupos logró vulnerar una cuenta de correo perteneciente a un influyente asesor de Vladimir Putin apellidado Surkov, sustrayendo información altamente sensible. Así, el llamado «Surkov Leaks» permitió conocer planes del gobierno ruso para desestabilizar a su homólogo ucraniano, con el objeto de influenciar los términos de un acuerdo entre ese régimen y las fuerzas prorrusas separatistas del Donbass, en favor de estas últimas (Shandra y Silly, 2019; Standish, 2016).

Buena parte de las operaciones cibernéticas rusas contra Ucrania han sido atribuidas a diversos «grupos APT»[3]. En ese contexto sobresalió *Armagedon*, o *Gamaredon*, una entidad supuestamente subordinada a los servicios de inteligencia de esa potencia. Se le atribuyeron a esta organización, desde su creación y hasta fines del año 2021, miles de ataques contra entidades públicas y privadas ucranianas, con fines de espionaje e interrupción o control de infraestructuras

[3] APT es el acrónimo en idioma inglés de «amenazas permanentes avanzadas» y se emplea para denominar a grupos clandestinos que cuentan con importantes y sofisticadas capacidades de ataque cibernético, normalmente con fines de destrucción o de espionaje, pero también criminales. Según un especialista español (Sánchez-Román Urrutia, 2020), a través de estos grupos los servicios de inteligencia de algunos países realizan acciones en el ciberespacio, financiándolos a esos efectos.

críticas[4] (Toulas, 2021). Para el espionaje, a través de técnicas de engaño instalaba en los sistemas atacados programas informáticos maliciosos (en adelante, *malware*) que exfiltraban datos sensitivos (Toulas, 2022a).

A mediados del mes de enero de 2022, Ucrania fue víctima de múltiples ciberataques. Los archivos de numerosas bases de datos fueron destruidos mediante un *malware* que fue denominado *Whispergate* por las empresas de ciberseguridad. Las pericias informáticas no lograron determinar el origen del ataque, aunque sí hallaron similitudes con ataques ejecutados años antes por *Sandworm*, otro grupo APT acusado de responder a los servicios de inteligencia rusos (Abrams, 2022a). Por la misma época, decenas de sitios *web* del gobierno ucraniano fueron objeto de ataques «de desfiguración», proyectándose en las pantallas un mensaje en idiomas ruso, polaco y ucraniano, advirtiendo a los usuarios que su información personal alojada en esos sitios había sido robada (Krebs y Kwon, 2022). Igual que en ocasiones anteriores, desde Kiev se aseguró que los ataques fueron llevados a cabo por un grupo afiliado a los servicios especiales de Rusia y Bielorrusia (Lyngaas et al., 2022), sin ahondar en mayores detalles.

Exactamente un mes después, al tiempo que Putin continuaba negando las posibilidades de invasión al país vecino, sufrieron ciberataques la cartera de Defensa ucraniana e importantes bancos privados, cuyos sitios web quedaron fuera de servicio por efecto de reiteradas denegaciones de servicio[5]. Desde el ministerio de Transformación Digital local se calificó al ataque como el más grande en su tipo, en la historia del país. El gobierno de Zelensky le otorgó la responsabilidad a su homólogo ruso, mientras la Casa Blanca acusó directamente a la Dirección de Inteligencia Militar de esa potencia (White House, 2022).

[4] La idea de infraestructuras críticas se refiere a sistemas, máquinas, edificios o instalaciones relacionados con la prestación de servicios esenciales a la población.

[5] La denegación de servicio (habitualmente referida como DDoS, debido a su sigla en idioma inglés) refiere a la saturación de un sitio *web* con una gran cantidad de estímulos falsos simultáneos, para paralizarlo intencionalmente. Esos estímulos se emiten desde máquinas infectadas previamente con programas maliciosos para cumplir esa tarea.

2.3. Iniciativas cibernéticas rusas tras el inicio de la «Operación militar especial»

En vísperas del inicio de la «operación militar especial» en Ucrania, recrudecieron los ataques cibernéticos contra este país. Por un lado, se reiteraron las denegaciones de servicio contra entidades bancarias y diversos ministerios (Lyngaas, 2022). Simultáneamente, *malwares* de destrucción de archivos afectaron a diversas agencias gubernamentales, además de una importante institución financiera y empresas privadas contratistas del gobierno (Abrams, 2022b). Con el tiempo, estos programas fueron denominados *IsaacWiper* y *HermeticWiper* por los especialistas (Gatlan, 2022a). Iniciada la invasión, Rusia atacó y dejó fuera de servicio el servicio de Internet satelital Ka-Sat, operado por la empresa alemana Viasat, mediante otro *malware* denominado *AcidRain*. La agresión afectó a decenas de miles de clientes, incluyendo organismos militares y de seguridad (Pearson et al., 2022).

A partir del ataque contra Ka-Sat y a lo largo de todo el primer mes de hostilidades armadas, los ciberataques rusos fueron numerosos y relativamente constantes, en su mayoría ejecutados a través de grupos APT, según indicó un informe de la firma Microsoft (2022). Empero, la cantidad de esos ataques fue notablemente menor a la que se hubiera esperado: el aumento fue inferior al 20 por ciento, respecto al mes previo al inicio de las acciones armadas (Check Point, 2022a). Y varios de esos episodios habrían correspondido, en realidad, a atacantes vinculados a gobiernos de terceros países (entre ellos China, Corea del Norte e Irán), o autónomos. Estos actores se valieron de diversos temas relacionados con la guerra en Ucrania para intentar penetrar servicios informáticos de los beligerantes, y también de países europeos (Palmer, 2022).

De acuerdo con el referido reporte, los ataques de Rusia incluyeron el empleo de *malware* destructivo y apuntaron a infraestructuras críticas, incluyendo generación de energía nuclear y transportes; además, hubo un vínculo directo entre varios ataques cibernéticos y las operaciones militares cinéticas (Microsoft, 2022). Sin embargo, el efecto de estos ataques fue llamativamente limitado y no se correspondió con las credenciales que ostenta esa potencia en estos menesteres.

Durante los siguientes meses de acciones bélicas y hasta el primer aniversario de la invasión, Rusia ejecutó numerosas operaciones cibernéticas ofensivas, de diferente tipo, en buena medida a través de grupos APT. Empero, tanto su

cantidad como su efectividad fueron limitados. En cuanto a lo primero, una empresa de ciberseguridad estadounidense estimó que en el primer semestre de guerra esos hechos aumentaron aproximadamente un 110 por ciento con relación a la etapa prebélica equivalente, incremento que no sería particularmente significativo. En cuanto a lo segundo, los ciberataques continuaron priorizando infraestructuras críticas, en muchos casos complementando operaciones cinéticas (Check Point, 2022b). Todavía a finales del año 2022, seguía latente el peligro de un ciberataque ruso de magnitud, contra la infraestructura eléctrica ucraniana, con sus sistemas de generación y redes de transmisión al borde del colapso, por efecto de los sostenidos ataques cinéticos recibidos. Empero, todo indica que ese ataque nunca se produjo (Majkut y Dawes, 2022).

Entre las acciones que sobresalieron en esa etapa cabe mencionar, apenas comenzado el segundo mes, un ataque de denegación de servicio contra la compañía Ukrtelecom, el mayor proveedor ucraniano de servicios de Internet a usuarios civiles y militares, que redujo su operatividad a cifras mínimas, durante un día (Brewster, 2022). Técnicamente, fue un ataque contra la infraestructura crítica, como también lo fue otro finalmente fallido, sucedido a comienzos del mes de abril y atribuido a *Sandworm*. Esa agresión apuntó a desconectar varias subestaciones eléctricas y así interrumpir la provisión de energía a la población local, empleando un *malware* llamado *Industroyer*; acto seguido, se intentaría borrar los rastros del ataque mediante otro programa malicioso conocido como *CaddyWiper*. También por esa época, *Armagedon* desarrolló extensas campañas de engaño informático enfocadas en blancos ucranianos y de la Unión Europea, destinadas a infectar los sistemas atacados con *malware* de espionaje. En el primer caso, los ardides apelaron a la identificación de criminales de guerra rusos; en el segundo, a las necesidades de armamento de las fuerzas armadas ucranianas y cómo colaborar en ese sentido (Toulas, 2022b).

Como dato interesante, de esas campañas también formó parte un APT conocido como *Ghostwriter*, que formaría parte del ministerio de Defensa de Bielorrusia (Gatlan, 2022b). Los primeros indicios de este grupo datan del año 2017, a partir de una investigación de la prestigiosa empresa de ciberseguridad del gigante Google enfocada en varias operaciones de desinformación en Internet dirigidas a audiencias de Europa Oriental. En general, sus narrativas se alineaban con los intereses de seguridad rusos y enfocaban en los negativos efectos de la presencia de la Organización del Tratado del Atlántico Norte (OTAN) en esa región (Mandiant, 2021).

2.4. Las respuestas cibernéticas de Ucrania

Al momento de iniciarse la operación militar rusa, la situación de Ucrania en materia de ciberseguridad, en términos comparativos con su oponente, era de nítida inferioridad. Una apreciación generada en el prestigioso Instituto Internacional de Estudios Estratégicos (IISS) en vísperas de la invasión (Austin, 2022), sugería que los grupos de hackers locales podían desplegar cierta «resistencia» a la agresión en el ciberespacio, aunque sin especificar los alcances de ese concepto. Todo esto, claro, sujeto a la evolución de las operaciones cinéticas: si Kiev caía bajo control ruso sin que previamente se hubieran preservado los datos y servidores allí ubicados, la pérdida para los defensores sería enorme. De allí que, en aquellos cruciales momentos, el gobierno ucraniano preparara planes de contingencia en ese sentido, contemplando inclusive el traslado de servidores fuera del país (Infobae, 2022, 9 de marzo).

El mencionado cálculo del IISS, ciertamente escéptico, también contemplaba la colaboración que prestarían Estados Unidos y otros países, especialmente Gran Bretaña, en actividades cibernéticas defensivas. Específicamente en el caso estadounidense, en el texto de una «asociación estratégica» anunciada en septiembre de 2021 consta una profundización de la cooperación bilateral en materia de ciberseguridad y ciberguerra (White House, 2021). En vísperas de la invasión rusa a Ucrania, la Casa Blanca confirmó que se había preparado para esa contingencia desde fines del año anterior (White House, 2022). En esos momentos previos no quedaba en claro, en cambio, el tipo de respuestas que Estados Unidos y otras naciones podían implementar, como respuesta a ciberataques rusos contra Ucrania. De acuerdo con diferentes fuentes, el rango de represalias podía fluctuar desde sanciones a funcionarios responsables de esas acciones, hasta operaciones ofensivas físicas o cibernéticas a los servidores involucrados. Menos certera aún, era la probabilidad de desatar ciberataques contra blancos de alto valor en Rusia (Shalal, 2022).

Iniciada la invasión a Ucrania, el poder ejecutivo estadounidense dispuso de un menú de respuestas cibernéticas ofensivas de diferente tenor, que incluía ataques a la infraestructura crítica, que fueron descartados para evitar un involucramiento directo (Dilanian y Cube, 2022). No obstante, la cooperación con el régimen de Kiev se intensificó, según testimonió inicialmente ante una comisión del Senado el titular del Comando Cibernético de las fuerzas armadas de ese país, aunque sus declaraciones no fueron específicas: «Brindamos soporte analítico remoto y llevamos a cabo actividades de defensa alineadas con