ARTÍCULO DOI 10.52781/cmm.a125

La ciberguerra ruso-ucraniana: los ataques rusos contra las infraestructuras críticas ucranianas y las posibles lecciones para el Ejército Brasileño

The Russian-Ukrainian Cyber War: Russian attacks on Ukrainian Critical Infrastructure and possible lessons for the Brazilian Army

Resumen: ¿Qué lecciones puede extraer el Ejército Brasileño del conflicto entre Rusia y Ucrania en materia de ciberdefensa ante ataques contra infraestructuras críticas? Con la evolución del uso del ciberespacio, se ha producido un aumento significativo de los ataques para afectar las infraestructuras críticas de un Estado. El objetivo de este trabajo es analizar qué lecciones puede extraer el Ejército Brasileño de los ataques rusos a infraestructuras críticas ucranianas. Así, por medio de una metodología exploratoria, el texto se centra en comprender cuáles fueron los antecedentes del conflicto, qué acciones está tomando Rusia para afectar a Ucrania y la manera en que las acciones en el teatro de operaciones pueden relacionarse con la estrategia nacional de ciberseguridad de Brasil. Por lo tanto, este texto señala los cambios en la estrategia rusa relacionados con el uso y la adaptación de los ciberataques a las infraestructuras críticas, abordando las posibles lecciones que el Ejército Brasileño puede extraer.

Palabras Clave: guerra ruso-ucraniana; infraestructuras críticas; ejército brasileño; ciberdefensa; exploratoria.

Abstract: What lessons can the Brazilian Army learn about cyber defense in terms of attacks on critical infrastructures in the conflict between Russia and Ukraine? With the evolution of the use of cyberspace, there has been a significant increase in attacks aimed at affecting a State' critical infrastructures. The aim of this work is to analyze what lessons the Brazilian Army can learn from the Russian attacks on Ukrainian critical infrastructures. Thus,with exploratory methodology, the text focuses on understanding the background to the conflict, what actions are being used by Russia to affect Ukraine and how actions within the theater of operations can be related to Brazil's National Cybersecurity Strategy. Therefore, this text points out the changes in Russian strategy linked to the use and adaptation of cyber attacks critical infrastructures, addressing possible lessons that the Brazilian Army can absorb.

Keywords: russo-ukrainian war; critical infrastructures; brazilian army; cyber defense; exploratory.

Rachel Camilly Soares de Souza
Universidade Estadual da Paraíba
João Pessoa, PB, Brasil
rachelcamillyss@gmail.com

Thays Felipe David de Oliveira
Centro Universitário Estácio
Recife, PE, Brasil
thaysfelipe@gmail.com

Murilo Gustavo de Paula
Centro Universitário Estácio
Goiânia, GO, Brasil
murilogdpaula@gmail.com

Recebido: 10 sep. 2023
Aprobado: 12 dic. 2023

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 INTRODUCCIÓN

¿Qué lecciones puede extraer el Ejército brasileño del conflicto entre Rusia y Ucrania en materia de Ciberdefensa ante los ataques contra las infraestructuras críticas? Con los avances tecnológicos y la demostración de la fragilidad del ciberespacio, se están produciendo cada vez más ataques en ese ámbito, lo que puede afectar las infraestructuras críticas de un Estado, como las telecomunicaciones, la energía, las finanzas, etc. Los servicios que prestan estas infraestructuras tienen una dimensión estratégica, ya que son esenciales para los ciudadanos, las organizaciones y el Estado, puesto que desempeñan un papel imprescindible tanto para la seguridad y soberanía nacional como para la integración y el desarrollo económico sostenible del Estado (Segundo, 2019).

La invasión de Rusia a Ucrania el 24 de febrero del 2022 desencadenó la crisis de seguridad más importante en Europa desde la Segunda Guerra Mundial (Fonseca, 2023). Más allá de la tradicional Guerra Cinética, Rusia realizó operaciones cibernéticas a gran escala en Ucrania antes y después del inicio del conflicto (Schulze; Kerttunen, 2023). Desde el comienzo de este conflicto, al menos seis grupos diferentes de *crackers* vinculados al Estado llevaron a cabo alrededor de 240 operaciones cibernéticas contra objetivos civiles y militares ucranianos (Cerulus, 2019).

Se empleó un *malware* —término amplio utilizado para clasificar todo tipo de *software* malicioso utilizado para causar daños— junto con herramientas maliciosas y tácticas de seguridad sofisticadas de *hacking* en detrimento de las infraestructuras públicas. Los grupos de *Advanced Persistent Threat* (APT) vinculados a las agencias de información rusas son los actores presentes en esta campaña en curso. Un ciberatacante se conoce como APT, cuando una red o sistema es atacado de forma selectiva durante un largo período, con el objetivo de extraer información sensible, obtener acceso privilegiado o causar daños importantes. Los ataques APT se caracterizan por su naturaleza furtiva, la persistencia en el uso de técnicas avanzadas de invasión y explotación de vulnerabilidades, así como por la capacidad de evadir la detección de las medidas de seguridad tradicionales. Por lo general, este actor está bien entrenado y a menudo está vinculado a un Estado o incluso controlado por él (NCSC, 2018).

A pesar de su reputación en materia de ciberguerra, Rusia no ha logrado lanzar ciberataques decisivos contra la infraestructura de Tecnología de la Información (TI) de Ucrania. Los métodos y las herramientas del atacante fueron efectivos anteriormente, pero esta vez el resultado fue diferente al que muchos esperaban. Además de la efectividad reducida, el volumen de ciberataques rusos fue inferior al que esperaban los analistas de Ciberdefensa (NCSC, 2018).

El éxito de Ucrania hasta ahora en la defensa contra la ofensiva cibernética rusa se puede atribuir a tres elementos: los preparativos del gobierno en los años previos a la guerra, la asistencia a la ciberdefensa de la Organización del Tratado del Atlántico Norte (OTAN) y de los países de la Unión Europea. Además, cabe resaltar la participación de empresas privadas, como, por ejemplo, Microsoft, Amazon y SpaceX, que ofrecieron soluciones comerciales como servicios digitales en la nube y Starlink, un proyecto de constelación de satélites desarrollado por la empresa privada SpaceX, que consiste en miles de pequeños satélites en órbita terrestre baja, formando una red interconectada, que proporcionó infraestructura de comunicaciones crítica (CISA, 2022).

En resumen, para operativizar este trabajo, se realizó una investigación cualitativa. Además, de forma complementaria, este artículo representa un estudio de caso único. Así, el

objetivo de este trabajo es analizar qué lecciones puede extraer el Ejército Brasileño de los ataques rusos a las infraestructuras críticas ucranianas en el 2015.

2 ANTECEDENTES HISTÓRICOS SOBRE LOS CIBERATAQUES RUSOS

Rusia ha recurrido sistemáticamente a ciberataques contra Ucrania. Los *crackers*, individuos que invaden computadoras o sistemas informáticos con propósitos ilegales, vinculados a los servicios secretos rusos, han estado llevando a cabo operaciones ciberofensivas en Ucrania al menos desde la anexión de Crimea por parte de Rusia en el 2014. Sus objetivos incluían universidades, compañías eléctricas, el sector bancario y otras infraestructuras críticas. Inicialmente, Rusia pretendía causar frustración pública y debilitar a sus adversarios políticos en el sistema político ucraniano. En algunos casos, los atacantes utilizaron el malware KillDisk, convirtiendo a Ucrania en un banco de pruebas para el desarrollo de nuevas armas cibernéticas (Fonseca, 2023).

A partir del 2014, el grupo hacktivista prorruso (Greenberg, 2017) ***CiberBerkut***, vinculado a la agencia de información militar extranjera del Estado Mayor de las Fuerzas Armadas rusas, conocida como GRU, comprometió el sistema electoral central ucraniano al instalar un *malware BlackEnergy* en el sistema para socavar la confianza en el proceso electoral y causar inestabilidad política (Greenberg, 2017). Además, el día de las elecciones, el *CiberBerkut* lanzó una campaña masiva de ataques de denegación de servicio (DDoS) —un ciberataque diseñado para sobrecargar un sistema, servicio o red, haciéndolo inaccesible a los usuarios legítimos— para retrasar el recuento final de las elecciones y desacreditar el proceso electoral ante la población. El ataque no tuvo éxito, ya que no deslegitimó al ganador de las elecciones en el 2014. Sin embargo, el recuento final de votos se retrasó dos horas (CISA, 2022).

En el 2015, el *Sandworm*, un grupo APT vinculado al GRU, logró llevar a cabo el primer ciberataque reconocido públicamente a una red eléctrica (NCSC, 2018). Los atacantes lograron obtener remotamente el control de los sistemas de control de supervisión y adquisición de datos (SCADA) de tres empresas de distribución de energía ucranianas e interrumpir el suministro de energía. Alrededor de 225.000 personas estuvieron sin electricidad durante seis horas (Cisa, 2022). Así, casi un año después del mencionado ataque, la red energética ucraniana volvió a ser blanco de ataques. Esta vez, se utilizó el *malware Industroyer*, también conocido como *CrashOverride*, que tiene como objetivo los ciberataques contra sistemas de control industrial (ICS). El *Industroyer* fue diseñado para explotar vulnerabilidades específicas detectadas en protocolos de comunicación utilizados en sistemas de control industrial, tal como el protocolo *Modbus* y el protocolo IEC 61850, se ha convertido en la mayor amenaza para los sistemas de control industrial desde el *Stuxnet* (Whitehead, 2017). Este *malware* se utilizó para obtener remotamente el control de interruptores y disyuntores de subestaciones eléctricas mediante la instalación de una puerta trasera en el sistema de destino que explotaba los protocolos utilizados por los sistemas de control industrial (ICS) en toda la infraestructura crítica. Este ciberataque afectó a gran parte de la capital de Ucrania y fue atribuido al grupo *Electrum APT*, que está directamente asociado al *Sandworm* (Whitehead, 2017).

El peor incidente cibernético en Ucrania tuvo lugar en el 2017, cuando el grupo ruso APT *Telebots*, también vinculado al *Sandworm*, implantó el *malware* destructivo *NotPetya* contra los sectores financiero y energético de Ucrania (Cherepanov; Lipovsky, 2017). El *NotPetya* debe

su nombre a su parecido con el *ransomware Petya*, que atacó a principios del 2016 y extorsionó a las víctimas para obtener la clave para desbloquear sus datos. Esta vez, el *NotPetya*, independientemente de si la víctima pagó o no, saboteó el 10% de las computadoras en Ucrania (Cherepanov; Lipovsky, 2017). Se extendió por todo el sector financiero de Ucrania por medio de un popular programa de preparación de impuestos. Aunque el ataque tuviera como objetivo empresas dentro de Ucrania, el *malware* se salió de control y afectó a empresas multinacionales de toda Europa y Estados Unidos (EE.UU.). El impacto exacto en la economía ucraniana no está claro, pero las pérdidas económicas mundiales estimadas superaron los diez millones de dólares (Greenberg, 2018).

En el 2018, el Comando Cibernético de EE. UU. utilizó el comportamiento anterior de Rusia, así como otros indicadores y advertencias de que el Estado ruso estaba a punto de repetir sus esfuerzos, como justificación para lanzar una operación preventiva contra *Internet Research Agency*, una empresa rusa de propaganda y de operaciones de influencia diseñada para prevenir ataques durante las elecciones (Nakashima, 2019). Más recientemente, las operaciones rusas combinaron sofisticadas técnicas de espionaje con campañas criminales de *malware*. Durante la mayor parte del 2020, el grupo de *crackers* rusos, *Cozy Bear*, explotó una vulnerabilidad de la cadena de suministro en el programa *SolarWinds Orion* para retirar datos y herramientas digitales de una extensa lista de blancos (Sanger; Perlroth; Schmitt, 2020). La operación hizo sonar las alarmas, ya que ni la NSA ni grandes empresas como Microsoft detectaron la intrusión, porque probablemente implicó una combinación de inteligencia humana y operaciones cibernéticas para insertar código malicioso profundamente en los servidores.

El 23 de febrero del 2023, el día antes de la invasión rusa, se lanzó un ciberataque masivo utilizando el *malware HermeticWiper* en los equipos del gobierno ucraniano y en los sectores financieros, de aviación, de TI y de energía (Greenberg, 2018). Aunque no hay pruebas concretas que vinculen a los autores de este ataque con Rusia, el momento y la metodología utilizados sugieren fuertemente tal vínculo. Al día siguiente, pocas horas después de la invasión, se produjo otro importante ciberataque contra la red *KA-SAT* de *Viasat*, ampliamente utilizada por las fuerzas armadas y por la policía de Ucrania (Saade, 2022). El ataque combinó DDoS con el *malware AcidRain*, especialmente diseñado contra equipos de telecomunicaciones. Como resultado, la mayoría de los *módems Viasat* quedó inoperable y el servicio de Internet de banda ancha para cientos de miles de ucranianos y militares quedó interrumpido. Un efecto secundario de este ataque fue el hecho de que el *AcidRain* cruzó fronteras y afectó a otros países europeos, al igual que el *NotPetya* (Saade, 2022).

El siguiente gran incidente se registró en abril del 2022, cuando la infraestructura energética de Ucrania fue atacada por el *malware Industroyer II*, el sucesor del *Industroyer*, dirigido específicamente a subestaciones eléctricas de alta tensión (Viasat, 2022). El *malware CaddyWiper* también se implantó junto con el ***Industroyer II*** para borrar las huellas del ataque. Cabe señalar que, a diferencia de su predecesor, el *Industroyer II* se utilizó como arma autónoma al no requerir la intervención de un operador remoto (CERT-UA, 2022). Se trata de una actualización importante, ya que un arma de este tipo podría implantarse en una red corporativa y permanecer inactiva, esperando el momento adecuado para atacar. Este comportamiento genera complejidad para los profesionales de la ciberseguridad en el desempeño de sus funciones para prevenir un ataque. Exhibiendo, así, características consistentes con las actividades del grupo *Sandworm*, lo que

también se hizo con el *Industroyer* en el 2016, pero esta vez no se observaron impactos directos en la disponibilidad de energía. El éxito en frenar el ataque se debió a la respuesta inmediata de las autoridades de ciberdefensa ucranianas, que obtuvieron una importante experiencia en los últimos años, y a la asistencia de Microsoft y ESET (Zhora, 2022).

3 COOPERACIÓN CON EL SECTOR PRIVADO

El gobierno y las fuerzas armadas ucranianas superaron el impacto inicial de la invasión y enfrentaron con éxito estos ataques no cibernéticos. El Equipo de Respuesta a Emergencias Informáticas de Ucrania (CERT-UA) trabajó con empresas privadas para minimizar los efectos de la ofensiva cibernética de Rusia y mantener todos los sistemas críticos en operación con una interrupción mínima. Una semana antes de la invasión, cuando la guerra parecía inminente, el gobierno ucraniano empezó a preocuparse por la seguridad de sus datos y buscó formas de protegerlos. Hasta entonces, la ley ucraniana exigía que datos específicos del gobierno y del sector público se almacenaran en servidores ubicados físicamente en el país. El gobierno cambió la legislación, permitiendo que los datos sensibles del gobierno y del sector privado se transfieran a servidores en la nube fuera del país (Amazon, 2022).

En los días y semanas siguientes, estas empresas proporcionaron ayuda, soporte y los medios (equipos informáticos y centros de datos fuera de Ucrania) para la migración de datos de todos los sectores de Ucrania. La mayoría de los ministerios, universidades y empresas privadas ucranianas se beneficiaron de esta colaboración (Poireault, 2022). En efecto, Ucrania cambió la soberanía de los datos por una mejor Ciberdefensa contra los ataques rusos. Gracias a esta estrategia, no solo el gobierno ucraniano logró funcionar correctamente hasta el día de hoy, sino que la población también pudo seguir viviendo una vida en línea relativamente normal durante la guerra: la mayoría de los servicios públicos estaban disponibles. Todos estos factores tuvieron un impacto significativo en la moral de la nación y ciertamente ayudaron a mantener la resistencia de Ucrania a la invasión (Poireault, 2022).

Otro aspecto interesante fue la cooperación del CERT-UA con empresas privadas de ciberseguridad para monitorear e identificar posibles ciberataques. Incluso antes del ataque *Industroyer II* del 2022, investigadores de Microsoft (Poireault, 2022) y ESET (Smith, 2022) monitoreaban de forma remota redes en Ucrania y realizaban análisis de datos en tiempo real para identificar posibles actividades maliciosas. Además, durante las operaciones cibernéticas de Ucrania, se registró el primer uso confirmado de Inteligencia Artificial (IA), un avance tecnológico que permite a los sistemas simular inteligencia similar a la humana. Según el presidente de Microsoft, Brad Smith, Ucrania utilizó con éxito la IA para detectar, identificar y derrotar un ciberataque ruso sin intervención humana (Papachelas, 2022).

Por ejemplo, la empresa ucraniana de IA Primer modificó su servicio comercial de transcripción y traducción de voz basado en IA para que pudiera procesar las comunicaciones rusas interceptadas y resaltar automáticamente la información relacionada con las fuerzas ucranianas. Ucrania también utilizó un *software* avanzado de reconocimiento facial y de imágenes basado en IA de Clearview AI para identificar a los rusos fallecidos por medio de sus perfiles de redes sociales para notificar a sus familias sobre sus muertes y transferir sus cuerpos a las familias (Mcgee-Abe, 2023).

Las comunicaciones resilientes y seguras son esenciales para cualquier operación militar. Tras el ciberataque contra la infraestructura de comunicaciones por satélite de Viasat, el Ejército ucraniano se quedó sin comunicaciones por satélite. Esta situación comprometió toda la Defensa del país, y fue solucionada por otra empresa privada estadounidense, SpaceX, que ofreció a Ucrania acceso gratuito a sus servicios de Internet por satélite Starlink. Ucrania adoptó rápidamente el servicio como sustituto del sistema de comunicaciones militares del gobierno, que se encontraba conprometido, lo que resultó ser extremadamente útil y exitoso. El sistema también demostró su resistencia a la interferencia de señales, como afirmó recientemente el director ejecutivo de SpaceX, Elon Musk (Papachelas, 2022).

4 CONSIDERACIONES Y RESULTADOS ACERCA DE LA CIBERGUERRA ENTRE RUSIA Y UCRANIA

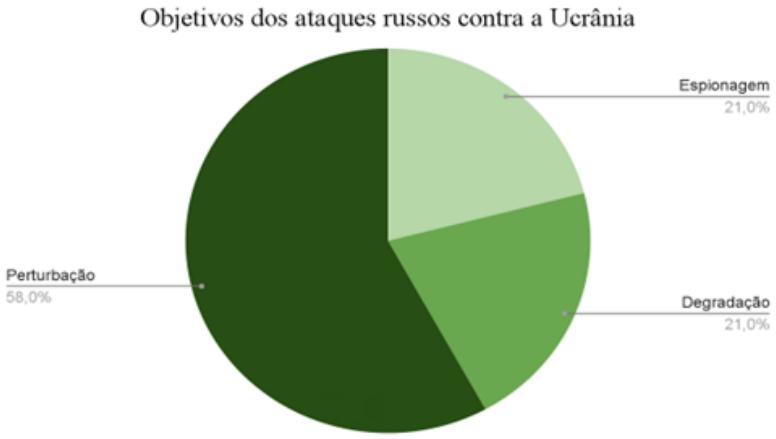
La falta de información verificable sobre los ciberataques rusos exitosos durante la guerra complica el panorama. Es probable que Ucrania no revele públicamente el alcance total de los impactos de las ofensivas cibernéticas rusas en sus infraestructuras para que Rusia no tenga una idea clara de la eficacia de sus operaciones cibernéticas (Werner, 2023). Por otra parte, Rusia podrá mantener algunas de sus capacidades cibernéticas en reserva para operaciones futuras o quizá ya esté trabajando en una nueva ofensiva cibernética aún no revelada. En cualquier caso, los años de preparación de Ucrania parecen haber dado sus frutos (Werner, 2023).

Los datos están en el centro de la era de la información, y eventos como el ciberataque *NotPetya* del 2017 han demostrado que el ciberespacio no respeta las fronteras tradicionales. Los daños colaterales de los ciberataques pueden ocurrir mucho más allá del blanco original. El *software* malicioso puede propagarse rápidamente por los países y afectar datos gubernamentales y corporativos en todo el mundo. Los sectores público y privado no pueden ignorar los daños potenciales de una crisis de este tipo. Se deben implementar nuevas estrategias susceptibles para aumentar la resistencia a este tipo de ataque. Como muestra el ejemplo ucraniano, los beneficios de la migración de datos a nubes fuera del país pueden superar desventajas como la pérdida de soberanía de los datos y pueden ser una solución. Otro aspecto que tener en cuenta es el hecho de que los grandes centros de datos empresariales que brindan servicios de computación en la nube son más difíciles de comprometer por parte de los grupos *APT* que los locales (Lewis, 2022).

Analizando el estilo de los ataques rusos, se observa que la actividad cibernética de Rusia durante la guerra ha sido más perturbadora que degradante, lo que es coherente con su comportamiento anterior. Como se puede observar en el Gráfico 1, al analizar estas operaciones cibernéticas por tipo, los objetivos cibernéticos preferidos de Rusia siguen siendo las actividades de modelos disruptivos y las campañas de ciberespionaje. Durante los primeros meses de su invasión de Ucrania en el 2022, los incidentes de perturbación representaron el 57,4% del total de incidentes, seguidos por el espionaje con el 21,3% (Muelle *et al*., 2023).

La confianza en operaciones disruptivas contrasta con el comportamiento de Rusia antes de la guerra, que acentuaba el espionaje. Dicho esto, tanto para la muestra de antes de la guerra como para la muestra de la guerra del 2022, las operaciones cibernéticas degradantes nunca fueron mayoría (Mueller *et al*., 2023) como se puede observar en el Gráfico 1.

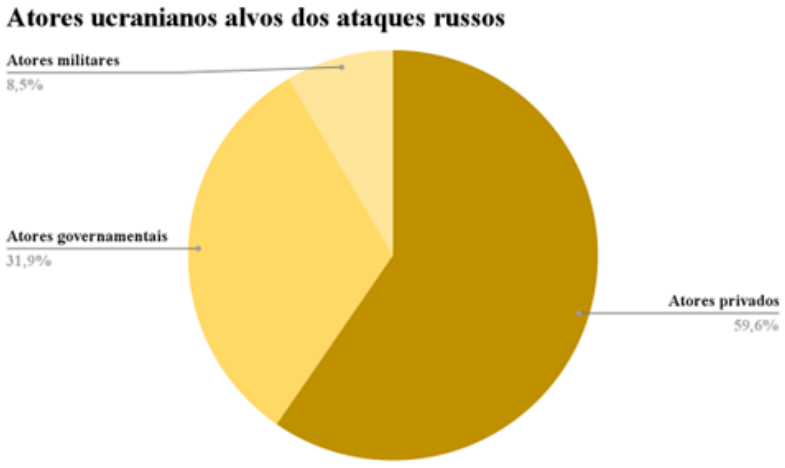
Gráfico 1 – Objetivos de los ataques rusos contra Ucrania



Fuente: Lewis, 2022.

Si se analizan los blancos de los ciberataques rusos en el total de 47 incidentes en el 2022, la mayoría (59,6%) se dirigieron a actores privados no estatales, seguidos de los ataques dirigidos a actores gubernamentales estatales y locales (31,9%). Solo cuatro (o el 8,5%) se dirigieron a actores militares gubernamentales, como se puede observar en el Gráfico 2 (Mueller *et al*., 2023).

Gráfico 2 – Actores ucranianos blancos de los ataques rusos



Fuente: Lewis, 2022.

Estos resultados arrojan dudas sobre hasta qué punto Rusia ha logrado integrar con éxito sus operaciones militares convencionales en los efectos cibernéticos. La coordinación con las fuerzas convencionales se ha convertido en un importante punto de discusión, con un gran segmento de los medios de comunicación social siguiendo a algunos analistas en la afirmación de que

ha habido una coordinación significativa entre las ciberoperaciones y las fuerzas militares convencionales (Lewis, 2022). Las operaciones militares rusas parecen tener dificultades para integrar efectos combinados, especialmente entre dominios.

5 LECCIONES PARA EL EJÉRCITO BRASILEÑO

La publicación de una nueva Estrategia Nacional de Ciberseguridad, E-Ciber, en febrero del 2020, es un logro importante para Brasil. La Estrategia de Defensa Nacional (END) define, desde el 2008, tres sectores de importancia estratégica para la defensa nacional: nuclear, espacial y cibernético, y a la Armada de Brasil corresponde la gestión del programa nuclear; a la Fuerza Aérea Brasileña, el programa geoespacial; y, al Ejército Brasileño, el liderazgo de la ciberdefensa en territorio nacional. Se constata que el Sector Cibernético, en la visión de END, no se limita a las actividades de Seguridad y Defensa Cibernética, ya que también incluye las Tecnologías de la Información y Comunicación (TIC) y los componentes básicos del Sector Cibernético en la actuación en red: (i) estructura de mando, control, comunicaciones, informática e inteligencia (C4I) para la actuación operativa y el funcionamiento administrativo de las Fuerzas Armadas; (ii) recursos de TIC; y (iii) arquitectura matricial, que hace viable el tránsito de información para apoyar el proceso de toma de decisiones, casi en tiempo real (Brasil, 2020a).

Dadas las lecciones de la guerra ruso-ucraniana, la seguridad y la defensa cibernéticas emergen naturalmente como imperativos de protección de las infraestructuras críticas de la información, asociadas con las infraestructuras críticas nacionales. En diciembre del 2020, Brasil dio un gran paso al crear el Sistema Militar de Defensa Cibernética (SMDC), cuyo órgano central es el Comando de Defensa Cibernética (ComDCiber), un comando operativo permanentemente activado e integrado por oficiales y *praças* de las Tres Fuerzas Armadas, como se muestra en la Figura 1 (Brasil, 2022c).

Figura 1 – Sistema militar de Defensa Cibernética

Fuente: Instituto Militar de Engenharia, sin año.

El SMDC realiza acciones de protección, exploración y ataques cibernéticos a favor de la Defensa Nacional, con diversos beneficios para la sociedad, en apoyo a la ciberseguridad en actividades

interagencias que se forma en la actuación de las Fuerzas Armadas de forma cooperativa con otros organismos, conciliando así intereses y coordinando esfuerzos, con el objetivo de evitar la duplicidad de actividades, la dispersión de recursos y la divergencia de soluciones, incluida la protección de las infraestructuras críticas del País. Si bien el Ejército Brasileño hace un trabajo excepcional al liderar la estructuración de la Seguridad y Defensa Cibernéticas brasileñas, es evidente que las tácticas que dominan las Fuerzas Armadas se basan en el dominio terrestre, y no en el ciberespacio (Brasil, 2020b).

La ciberguerra entre Rusia y Ucrania, específicamente los ataques rusos a la infraestructura crítica ucraniana, ofreció una serie de lecciones valiosas para Brasil; estos eventos resaltan la importancia de la preparación y capacitación para enfrentar las amenazas cibernéticas dirigidas a los sectores estratégicos del país.

Una de las lecciones clave es la necesidad de invertir en capacidades de ciberdefensa. Por lo tanto, existe la necesidad de desarrollar y mejorar sus habilidades en la protección de los sistemas energéticos, de comunicación, de transporte y otras áreas estratégicas del país. Esto requiere un enfoque integral que involucre tecnología, especialización en ciberseguridad y capacitación adecuada para sus equipos (Harknett, 2009).

El Ejército Brasileño se ha empeñado en la Defensa Cibernética de Infraestructuras Críticas, reconociendo la importancia de enfrentar incidentes relacionados con ataques cibernéticos. Sin embargo, es esencial destacar la necesidad continua de perfeccionamiento e implementación regular de ejercicios y simulaciones, el Exercício Guardião Cibernético 5.0 (EGC), con sede en la Escola Superior de Defesa, en Brasília (DF), representa um marco significativo en la preparación y defensa cibernética de Brasil. Realizado anualmente y considerado el mayor evento del Hemisferio Sur dedicado a la defensa digital, a lo largo de los días del evento, el EGC presenta dinámicas y simulaciones diseñadas para capacitar a sectores críticos del país contra ciberataques. Estas actividades no solo ponen a prueba la capacidad de respuesta contra estos ataques, sino que también promueven la colaboración entre agencias gubernamentales, empresas privadas vinculadas a la infraestructura crítica del país y a la comunidad académica (Padilha, 2023).

Además, desempeñan un papel crucial a la hora de probar y fortalecer la preparación cibernética del Ejército, permitiendo identificar brechas, mejorar los procedimientos de respuesta a incidentes cibernéticos y mejorar la colaboración entre los equipos involucrados (Padilha, 2023). La fuerza armada terrestre puede desempeñar un papel activo brindando orientación sobre medidas cibernéticas, como la implementación de sistemas de detección e intrusión, políticas de autenticación, protección de datos y capacitación de empleados de empresas privadas que brindan servicios esenciales al país, tales como bancos, empresas de energía y telecomunicaciones.

Además, es fundamental invertir en recursos ofensivos de Seguridad Cibernética. Los ciberataques rusos a Ucrania exigieron una capacidad de respuesta rápida y eficaz ante este tipo de agresiones. Demostrando para Brasil la relevancia de tener la capacidad de identificar, rastrear y neutralizar actores hostiles que buscan dañar la infraestructura crítica del país (Buchan, 2009).

Otro punto que destacar es la cooperación y el intercambio con aliados internacionales, ya que la Guerra Cibernética es una amenaza transnacional que requiere esfuerzos definidos para combatirla. Por lo tanto, debemos buscar alianzas estratégicas con otras naciones, compartiendo conocimientos, tecnologías y experiencias para fortalecer los recursos de respuesta a ciberataques de Brasil. Además, la colaboración con organizaciones internacionales, como la OTAN, puede proporcionar un marco estratégico para hacer frente a esta amenaza a nivel mundial (Samuel; Sharma, 2012).

Además, es necesario discutir la importancia del decreto n.º 11.200, de 15 de septiembre del 2022, que trata del Plan Nacional de Seguridad de Infraestructuras Críticas (Plansic), que es una iniciativa de suma relevancia para el país. Este plan consiste en una serie de medidas y directrices que tienen como objetivo garantizar la seguridad y resiliencia de las infraestructuras críticas, asegurando la continuidad de los servicios esenciales ofrecidos a la población en caso de ataques a dichas infraestructuras. Además, el mencionado decreto prevé la creación de un Sistema Integrado de Datos de Seguridad de Infraestructuras Críticas, el cual será administrado por el Gabinete de Seguridad Institucional de la Presidencia de la República (GSI/SP), con el objetivo de monitorear e identificar amenazas y vulnerabilidades en estas infraestructuras (Brasil, 2022a). El plan también prevé una distribución de las responsabilidades entre ministerios para la elaboración de planes sectoriales de seguridad para estas infraestructuras:

Tabla 1 – Distribución de responsabilidades entre los Ministerios para la elaboración de planes sectoriales de seguridad de las infraestructuras críticas

ÁREA PRIORITARIA	SECTOR	MINISTERIO RESPONSABLE
Aguas	Presas	Ministerio de Desarrollo Regional
	Abastecimiento Urbano de Aguas	
Energía	Energía Eléctrica	Ministerio de Minas y Energía
	Peganbio -	
Transporte	Terrestre	Ministerio de Infraestructura
	Aéreo	
	Acuavial	
Comunicaciones	Telecomunicaciones	Ministerio de Comunicaciones
	Radiodifusión	
	Servicios Postales	
Finanzas	Finanzas	Ministerio de Economía
Bioseguridad y Bioprotección	Bioseguridad y Bioprotección	Ministerio de Salud
Defensa	Defensa	Ministerio de Defensa

Fuente: Brasil, 2022a.

La distribución sectorial de la responsabilidad desempeña un papel crucial en la agilidad y eficiencia de la respuesta en emergencias. Con ministerios designados para áreas prioritarias específicas, como energía, transportes, comunicaciones, entre otros sectores estratégicos, la clara estructuración de las responsabilidades facilita la toma de decisiones rápidas y coordinadas en caso de amenazas o ataques a alguna infraestructura crítica del país. Esta división de responsabilidades proporciona una respuesta ágil y efectiva, asegurando que se adopten las medidas adecuadas para preservar la continuidad de los servicios esenciales ofrecidos a la población.

Otro punto que merece énfasis es que la inteligencia, la vigilancia y el reconocimiento desempeñan un papel crucial en la detección y prevención de ciberataques. El Ejército Brasileño debe invertir en recursos de inteligencia cibernética, utilizando tecnologías avanzadas, por ejemplo, la IA y el aprendizaje automático para monitorear y evaluar posibles amenazas. Esta capacidad de anticipar ataques permitirá una respuesta rápida y eficaz para proteger la infraestructura crítica del país (Lee, 2012).

Finalmente, cabe resaltar la cooperación entre el sector de comunicaciones del Ejército, las instituciones gubernamentales y los sectores de la sociedad civil, como empresas privadas de tecnología e instituciones académicas, para desarrollar estrategias integrales de ciberdefensa. Esta colaboración permitirá una respuesta coordinada y eficiente ante potenciales ciberataques (Carretero; Cruz; Sempere, 2010).

La Guerra Cibernética entre Rusia y Ucrania ofrece lecciones valiosas a Brasil y al mundo. Al aprender de estos eventos e implementar medidas de respuesta rápida, el Ejército puede fortalecer sus capacidades y estar preparado para enfrentar desafíos similares en el futuro. Esto garantizará la seguridad y la soberanía de Brasil, protegiendo sus Infraestructuras Críticas y manteniendo la estabilidad en un mundo cada vez más digital e interconectado (Alberts; Garstka, 2000).

6 CONSIDERACIONES FINALES

Un país de grandes proporciones territoriales, poblacionales y económicas, como Brasil, que busca una creciente inserción internacional, debe buscar constantemente lecciones de los conflictos internacionales en curso que se puedan aplicar para mejorar los sectores de sus Fuerzas Armadas, teniendo en vista que el caso de la guerra de Rusia en Ucrania, por ejemplo, demuestra la importancia del ciberespacio como uno de los medios más importantes para conducir un conflicto en la actualidad.

A pesar de la existencia de ramas cibernéticas en las fuerzas singulares (en Brasil, la END, predomina la rama cibernética del Ejército), como fue el caso de las antiguas ramas aéreas de los Ejércitos y Armadas, que se unieron para crear las Fuerzas Aéreas, existe la posibilidad de construir una nueva Fuerza Armada, u organización de doble empleo, formada por cibercombatientes especializados, provenientes de la combinación de las ramas cibernéticas de las Fuerzas Singulares actualmente existentes.

Después de todo, la organización, los tiempos, los medios y las tácticas de combate exploradas en el quinto ámbito de la guerra son muy distintos de los anteriores. Observamos lo que sucede en la guerra ruso-ucraniana, donde una batalla cibernética dura unas pocas horas, mientras que las batallas terrestres, marítimas y aéreas duran días o semanas.

Por lo tanto, la búsqueda de lecciones aplicables al Ejército Brasileño es imprescindible para el desarrollo de nuevas políticas de Ciberdefensa, además de una actualización más frecuente de la Estrategia Nacional de Seguridad Cibernética, ya que Brasil, tomando en consideración sus potencialidades internacionales y la cantidad de recursos naturales integrados al territorio, no puede descuidar su segmento de defensa y la importancia del desarrollo del quinto dominio en la actualidad.

REFERENCIAS

ALBERTS, D. S.; GARSTKA J. J. **Network-centric warfare**: Developing and leveraging information superiority. Washington, DC: CCRP Publications, 2000.

AMAZON. Amazon Staff. Safeguarding Ukraine's data to preserve its present and build its future. **Amazon News**, [*s. l.*], 9 jun. 2022. Disponível em: https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-itspresent-and-build-its-future. Acesso em: 15 maio 2023.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Versão sob apreciação do Congresso Nacional (Lei Complementar 97/1999, art. 9o, § 3o). Brasília, DF: Ministério da Defesa. 2020a.

BRASIL. **Decreto nº 11.200, de 15 de setembro de 2022**. Aprova o Plano Nacional de Segurança das Infraestruturas Críticas. Brasília, DF: Congresso Nacional, 2022a.

BRASIL. Presidência da República. **Estratégia Nacional de Segurança Cibernética – E-Ciber**. Decreto nº 10.222. Brasília, DF: Presidência da República, 2022b.

BRASIL. Ministério da Defesa. **Sistema Militar de Defesa Cibernética entra em vigor nesta terça-feira**. Brasília, DF: Presidência da República, 2022c.

BRASIL. Ministério da Defesa. **Defesa e Segurança cibernéticas**. Rio de Janeiro, RJ; Instituto Militar de Engenharia. Disponível em: http://www.defesacibernetica.ime.eb.br/. Acesso em: 20 maio 2023.

BUCHAN, J. P. Protecting national critical infrastructure against cyber threats. **Computers & Security**, [*s. l.*], v. 28, n. 3, p. 191-198, 2009.

CARRETERO, M. M.; CRUZ, A. D.; CRUZ, J. R. Strengthening International cooperation for combating cybercrime. **Computer Law & Security Review**, Amsterdam, v. 26, n. 5, p. 501-507, 2010.

CERT-UA – COMPUTER EMERGENCY RESPONSE TEAM OF UKRAINE. Cyber attack of the Sandworm group (UAC-0082) on energy facilities of Ukraine using malware INDUSTROYER2 and CADDYWIPER. **CERT-UA**, Kyiv, 12 dez. 2022. Disponível em: https://cert.gov.ua/article/39518. Acesso em: 17 jul. 2023.

CERULUS, L. How Ukraine became a test bed for cyberweaponry. **Politico**, Bruxelles, 14 fev. 2019. Disponível em: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/. Acesso em: 15 jul. 2023.

CHEREPANOV, A.; LIPOVSKY, R. Industroyer: Biggest threat to industrial control systems since Stuxnet. **We Live Security**, Bratislava, 12 jun. 2017. Disponível em: https://www.

welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/. Acesso em: 18 jul. 2023.

CISA – CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. Russian State-Sponsored and criminal cyber threats to critical infrastructure. **CISA**, Washington, DC, 20 abr. 2022. Disponível em: https://www.cisa.gov/uscert/ncas/alerts/aa22-110aI. Acesso em: 3 jul. 2023.

FONSECA, L. A guerra cibernética e o conflito Rússia versus Ucrânia. **Revista de Relações Exteriores**, [*s. l.*], 24 fev. 2023. Disponível em: https://relacoesexteriores.com.br/a-guerra-cibernetica-e-o-conflito-russia-versus-ucrania/. Acesso em: 1 abr. 2023.

GREENBERG, A. Everything We Know About Russia's Election-Hacking Playbook. **Wired**, [*s. l.*], 6 set. 2017. Disponível em: https://www.wired.com/story/russia-election-hacking-playbook/. Acesso em: 16 set. 2023.

GREENBERG, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History, **Wired**, [*s. l.*], 22 ago. 2018.

HARKNETT, M. Defending cyberspace and other metaphors. **Journal of Strategic Studies**, Oxfordshire, v. 32, n. 1, p. 5-31, 2009.

LEE, R. M. Active cyber defense: Applying Air Force doctrine for cyber operations. **Air & Space Power Journal**, [*s. l.*], v. 26, n. 6, p. 50-61, 2012.

LEWIS, J. Cyber War And Ukraine. **CSIS**, [*s. l.*], 16 jun. 2022. Disponível em: https://www.csis.org/analysis/cyber-war-and-ukraine. Acesso em: 9 maio 2023.

MCGEE-ABE, J. One year on: 10 technologies used in the war in Ukraine. **Tech Informed**, [*s. l.*], 24 fev. 2023. Disponível em: https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/. Acesso em: 9 maio 2023.

MUELLER, G. *et al*. Cyber Operations during the Russo-Ukrainian War. **CSIS**, [*s. l.*], 13 jul. 2023. Disponível em: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war. Acesso em: 24 ago 2023.

NAKASHIMA, E. U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. **The Washington Post**, Washington, DC, 27 fev. 2019. Disponível em: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html. Acesso em: 10 ago. 2023.

NCSC – NATIONAL CYBER SECURITY CENTER. Reckless campaign of cyber attacks by Russian military intelligence service exposed. NCSC, [*s. l.*], 3 out. 2018. Disponível em: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed. Acesso em: 22 jul. 2023.

PADILHA, L. Exercício do Guardião Cibernético 5.0 – Forças Armadas, órgãos públicos e empresas realizam grande treinamento. **Defesa Aérea e Naval**, Brasília, DF, 6 out. 2023. Disponível em: https://www.defesaaereanaval.com.br/ciberseguranca/exercicio-guardiao-cibernetico-5-0-forcas-armadas-orgaos-publicos-e-empresas-realizam-grande-treinamento. Acesso em: 1 dez. 2023.

PAPACHELAS, A. Building defenses for cyberwarfare. **Kathimerini**, London, 14 nov. 2022. Disponível em: https://www.ekathimerini.com/opinion/interviews/1197775/building-defenses-for-cyberwarfare/. Acesso em: 30 jul. 2023.

POIREAULT, K. Interview: Microsoft Shares Its Experience of Migrating Data in Times of Cyber Warfare. **Infosecurity**, [*s. l.*], 30 set. 2022. Disponível em: https://www.infosecurity-magazine.com/interviews/interview-microsoft-migrating-data/. Acesso em: 10 jun. 2023

SAADE, J. A. G. HermeticWiper. New Destructive Malware Used In Cyber Attacks on Ukraine. **Sentinel One**, [*s. l.*], 23 fev. 2022.

SAMUEL, C.; SHARMA, M. **Securing cyberspace**: International and Asian perspectives. Washington, DC: World Scientific Publishing, 2012.

SANGER, D.; PERLTOTH, N.; SCHMITT, E. Scope of Russian Hacking Becomes Clear: Multiple U.S. agencies were hit. **New York Times**, New York, 14 dez. 2020. Disponível em: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html. Acesso em: 2 ago. 2023.

SCHULZE, M.; KERTTUNEN, M. Cyber Operations in Russia's War against Ukraine. **SWP Comment**, [*s. l.*], abr. 2023. Disponível em: https://www.swp-berlin.org/publications/products/comments/2023C23_CyberOperations_UkraineWar.pdf. Acesso em: 7 de jun. 2023.

SEGUNDO, C. B. T. **A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos**. Brasília, DF: Escola Superior de Guerra, 2019. Disponível em: https://repositorio.esg.br/handle/123456789/1205. Acesso em: 7 maio 2023.

SMITH, B. **Defending Ukraine**: Early Lessons from the Cyber War. Blog Microsoft, [*s. l.*], 22 jun. 2022. Disponível em: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/. Acesso em: 21 dez. 2023.

VIASAT. KA-SAT Network cyber attack overview. **Viasat**, [*s. l.*], 30 mar. 2022. Disponível em: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview. Acesso em: 15 jul. 2023.

WERNER, D. Russian invasion of Ukraine exposes cybersecurity threat to commercial satellites. **Spacenews**, [*s. l.*], 14 abr. 2023. Disponível em: https://spacenews.com/russian-invasion-of-ukraine-exposes-cybersecurity-threat-to-commercial-satellites/. Acesso em: 1 jul. 2023.

WHITEHEAD, D. E. *et al*. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *In*: ANNUAL CONFERENCE FOR PROTECTIVE RELAY ENGINEERS (CPRE), 70., 2017, Texas. **Anais** [...]. Texas, 2017.

YIN, R. **Estudo de Caso**: Planejamento e métodos. Porto Alegre: Bookman, 2015.

ZHORA, V. The potential of Russian hackers is probably overestimated. **State Service of Special Communications and Information Protection of Ukraine**, Kiev, 16 mar. 2022. Disponível em: https://cip.gov.ua/en/news/viktor-zhora-potencial-rosiiskikh-khakeriv-imovirno-pereocinenii. Acesso em: 13 jul. 2023.


ECEME