Documento
Opinión

99/2022 10 de noviembre de 2022

*Ada Gavrila* *

**La gran ciberguerra de Ucrania que no ocurrió**


# La gran ciberguerra de Ucrania que no ocurrió

## Resumen:

Actualmente la sociedad internacional lidia con un conflicto híbrido en Ucrania, donde las armas tradicionales y las cibernéticas se utilizan a la vez. La gran sorpresa de la invasión rusa ha sido la aparente ausencia de una gran guerra cibernética. Se suponía que, para preparar el terreno para el asalto físico, Moscú primero lanzaría un ciberataque total que paralizaría Ucrania. Pero esto no sucedió.

Este artículo explica las razones por las cuales, en la búsqueda de ventajas estratégicas o tácticas en Ucrania, Rusia no ha utilizado las potentes herramientas cibernéticas que en apariencia posee. Además, muestra cómo la guerra de Ucrania puede modificar los parámetros tradicionales de los conflictos internacionales a través de una nueva configuración de los piratas informáticos.

## Palabras clave:

Ciberseguridad, Rusia, guerra cibernética, Ucrania, piratas informáticos.

# *Ukraine's great cyberwar that didn't happen*

*Abstract:*

*International society is currently grappling with a hybrid conflict in Ukraine, where traditional and cyber weapons are being used in tandem. The big surprise of the Russian invasion has been the apparent absence of a major cyber war. Russia was supposed to first launch an all-out cyber-attack that would cripple Ukraine and set the stage for the physical assault that followed. But this did not happen.*

*This article explains why Russia has not used the powerful cyber tools it apparently possesses in pursuit of strategic or tactical advantages in Ukraine. Furthermore, it shows how the Ukrainian war may change the traditional parameters of international conflicts through the new configuration of hackers.*

*Keywords: cyber security, Russia, cyber warfare, Ukraine, hackers.*

**Cómo citar este documento**:

GAVRILA, A. *La gran ciberguerra de Ucrania que no ocurrió*. Documento de Opinión IEEE 99/2022.
https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO99_2022_ADAGAV_Ucrania.pdf y/o enlace bie[3] (consultado día/mes/año)

## Introducción

La invasión de Ucrania por parte de Rusia ha alterado tanto el mundo real como el mundo virtual. Sin embargo, esto no es nada nuevo, ya que —tal y como se conoce— la actual guerra deriva del prolongado conflicto ruso-ucraniano que comenzó en 2014, caracterizado por los ataques cibernéticos rusos a infraestructuras críticas ucranianas. Entre ellos cabe destacar el ataque a la red eléctrica de Ucrania en diciembre de 2015 que provocó un apagón de hasta seis horas en más de 230.000 hogares[1], la parálisis de la Tesorería de Ucrania en diciembre de 2016[2] y el ataque con el *malware* NotPetya en 2017[3].

En la última década, Rusia ha asumido una postura cibernética cada vez más asertiva, basada en su disposición a llevar a cabo ciberoperaciones en sistemas de infraestructura crítica a fin de influir en el discurso público y crear confusión. Además, Moscú ha demostrado en varias ocasiones su disposición a emplear ciberataques ofensivos incluso en situaciones distintas a la guerra con el objetivo de afectar los resultados políticos y económicos en otros Estados[4] y garantizar su victoria[5].

Este artículo se propone analizar, en primer lugar, el desarrollo de la guerra cibernética. En segundo lugar, se argumentará por qué Rusia ha cambiado su estrategia cibernética. Por último, se presentará el impacto de la nueva configuración de los piratas informáticos sobre futuros conflictos.

---

[1] Cfr. COUNCIL ON FOREIGN RELATIONS. «Compromise of a power grid in eastern Ukraine». Diciembre de 2015. Disponible en: https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine

[2] El ciberataque detuvo los sistemas de la Tesorería durante varios días, por lo que los trabajadores estatales y los jubilados no pudieron recibir sus pagos (ZINETS, Natalia. «Ukraine hit by 6,500 hack attacks, sees Russian "cyberwar"». Reuters, 29 de diciembre de 2016. Disponible en: https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC).

[3] Este ciberataque infectó una decena de sitios web de organizaciones ucranianas —incluidos bancos, ministerios, periódicos y empresas de electricidad— y se extendió a posteriori a varios Estados occidentales, como Alemania, Francia, Estados Unidos o el Reino Unido (HERN, Alex. «WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017», *The Guardian*. 30 de diciembre de 2017. Disponible en: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware).

[4] El ejemplo más relevante es la intromisión en las elecciones presidenciales de EE. UU. en 2016, cuando los ataques cibernéticos rusos contribuyeron a generar una atmósfera de desconfianza, polarización y fragmentación social. Este ataque cibernético no solo perjudicó las posibilidades de las víctimas de ganar las elecciones, sino que contribuyó a la ya declinante fe de los estadounidenses en las instituciones democráticas.

[5] ORENSTEIN, Mitchell. «Russia's use of cyberattacks: Lessons from the Second Ukraine War». Foreign Policy Research Institute, 7 de junio de 2022. Disponible en: https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/

## Desarrollo de la guerra cibernética[6] en Ucrania

Antes de que Rusia invadiera Ucrania el 24 de febrero, analistas, expertos y funcionarios de diversos Estados pensaban que los ciberataques iban a desempeñar un papel esencial en la guerra[7]. En concreto, el 22 de febrero de 2022, minutos después de que el presidente Joe Biden anunciara nuevas sanciones contra los bancos y las élites rusas, David Ring, un alto funcionario del FBI, pidió a las empresas estadounidenses y a los gobiernos locales que tuvieran muy presente el potencial de los ataques de *ransomware* a medida que la crisis entre el Kremlin y Ucrania se agudizara[8].

Desde hace casi una década, Ucrania se ha convertido en el conejillo de indias de Rusia: ha resultado víctima de numerosos ciberataques rusos lanzados contra los sistemas de información de sus instituciones estatales y empresas privadas[9]. Consiguientemente, era lógico pensar que la situación se repetiría en 2022. En cierta manera sucedió. Durante el preludio de la invasión rusa, se registraron varios ciberataques contra Ucrania.

[6] La expresión *guerra cibernética* se refiere al uso de las tecnologías de la información y la comunicación (TIC) para interrumpir las actividades de un Estado u organización con fines estratégicos o militares y causar daños comparables a los de la guerra real (SINGER, Peter W. y FRIEDMAN, Allan. *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press, 2014, pp. 20-22. Disponible en: http://book.itep.ru/depository/cyberwar/P.W.Singer_Allan_Friedman_Cybersecurity_and_Cyberwar_What_Everyone_Needs_to_Know_2014_Oxford_University_Press.pdf).

[7] MILLER, Christina. «Throwback attack: Russia breaches Wolf Creek Nuclear Power facility», *Industrial Cybersecurity Pulse*. 24 de febrero de 2022. Disponible en: https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-russian-breaches-wolf-creek-nuclear-power-facility/

[8] LYNGAAS, Sean. «US officials tell businesses to watch for potential ransomware attacks after Biden announces Russia sanctions». CNN, 22 de febrero de 2022. Disponible en: https://edition.cnn.com/2022/02/22/politics/russia-sanctions-fbi-cyber-threats-ransomware/index.html

[9] En 2016 Ucrania sufrió el primer ataque de *malware* diseñado específicamente para atacar una infraestructura eléctrica (PAKHARENKO, Glib. «*Cyber Operations at Maidan: A First-Hand Account», en* GEERS, Keneth [ed.], *Cyber war in perspective: Russian aggression against Ukraine*. CCDCOE, 2015, pp. 60-65. Disponible en: https://web.archive.org/web/20161202005747/https:/ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf).

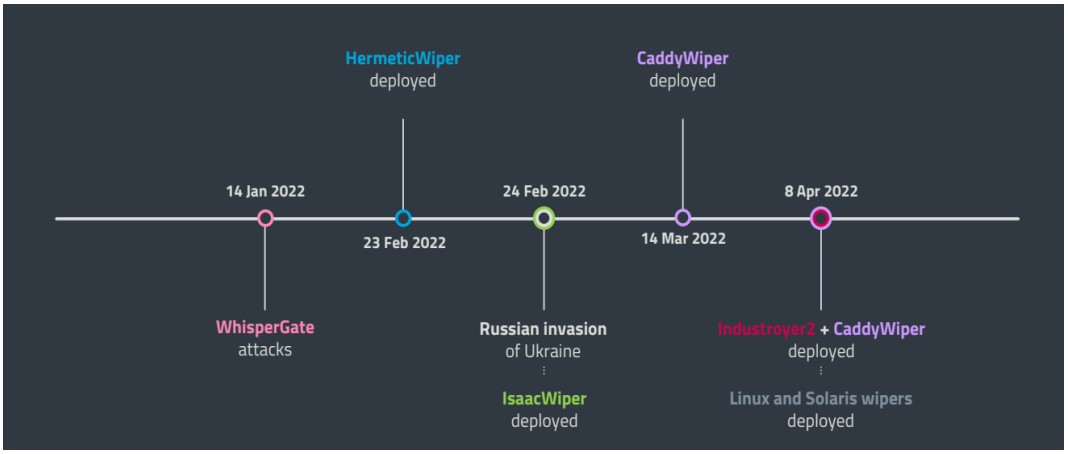


Figura 1. Ciberataques detectados por ESET antes y durante la invasión rusa
Fuente: ESET. *Threat Report T1, 2022.* Disponible en: https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

El primer ciberataque tuvo lugar el 14 de enero y afectó a alrededor de setenta sitios web gubernamentales, incluidos el del Ministerio de Relaciones Exteriores, el Gabinete de Ministros y el Consejo de Seguridad y Defensa de Ucrania. Los piratas informáticos reemplazaron los sitios web con un texto en ucraniano, polaco y ruso que decía: «Ten miedo y espera lo peor». La mayoría de los sitios fueron restaurados a las pocas horas del ataque[10].

El 15 de febrero un gran ataque de denegación de servicio —DDoS, por sus siglas en inglés—[11] derribó las páginas web del Ministerio de Defensa, el Ejército y los dos bancos más grandes de Ucrania, PrivatBank y Oschadbank. *The New York Times* lo describió como «el mayor asalto de este tipo en la historia del país»[12].

El 24 de febrero, una hora antes de la invasión militar, una nueva actividad maliciosa, cuyo objetivo era la red satelital KA-SAT, propiedad de Viasat, interrumpió el acceso a internet en Ucrania y desactivó miles de turbinas eólicas alemanas que usaban Viasat para comunicarse. A pesar de su significativo impacto, las expectativas de los analistas acerca de «un gran ataque cibernético» contra la infraestructura ucraniana no se

[10] POLITYUK, Pavel y HOLLAND, Steve. «Cyberattack hits Ukraine as U.S. warns Russia could be prepping for war». Reuters, 2020. Disponible en: https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/

[11] Se define como el ataque a un sistema de computadoras o a una red con el objetivo de que un servicio o recurso sea inaccesible para sus usuarios legítimos.

[12] KRAMER, Andrew E. «Hackers Bring Down Government Sites in Ukraine», *The New York Times*. 28 de abril de 2022. Disponible en: https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html

cumplieron. Una de las posibles explicaciones es que dos días antes del ataque la Unión Europea había desplegado un equipo de respuesta rápida cibernética, denominado CERT-UE y compuesto por varios expertos en seguridad cibernética[13].

Según el informe de ESET, los diversos *malware* utilizados hasta el momento —HermeticWiper, IsaacWiper y CaddyWiper— fueron destinados a organizaciones específicas (no) gubernamentales con el objetivo de afectar su capacidad para responder adecuadamente a la invasión. ESET registró víctimas en los sectores financiero, gubernamental y en los medios de comunicación y atribuyó tanto HermeticWiper como CaddyWiper a Sandworm[14], un grupo identificado por EE. UU. como parte de la agencia de inteligencia militar rusa GRU.

Además, el 25 de febrero, desde organizaciones y empresas como ESET o Vectra AI se barajó la posibilidad de una «guerra cibernética total» entre Rusia y Occidente a causa de la avalancha de ciberataques en Ucrania previa a la invasión[15]. En aquel momento, los ataques cibernéticos se habían convertido en el arma del primer ataque.

Un informe[16] publicado por Microsoft en abril de 2022 muestra que la mayoría de los ciberataques fueron programados para coincidir con misiles entrantes o ataques terrestres. El informe destaca una sutileza considerable en las primeras semanas de la guerra, cuando los bombardeos y los movimientos de tropas eran obvios pero las operaciones cibernéticas eran menos visibles y más difíciles de atribuir a las agencias de inteligencia rusas, al menos de inmediato. Además, la compañía concluyó que Rusia había comenzado a prepararse para los ataques cibernéticos en marzo de 2021, al mismo tiempo que había empezado a desplegar tropas a lo largo de su frontera con Ucrania. Los ataques cibernéticos preparatorios parecen haber tenido como objetivo

[13] TIDY, Joe. «Ukraine: EU deploys cyber rapid-response team». BBC News, 22 de febrero de 2022. Disponible en: https://www.bbc.com/news/technology-60484979

[14] Si bien algunos especularon que Sandworm podía ser un grupo que trabajaba desde Rusia, hasta 2020 el Departamento de Justicia de los EE. UU no lo identificó efectivamente como la Unidad Militar 74455 de la Dirección Principal de Inteligencia de Rusia. Se cree que fue responsable de los ataques DDoS de 2008 en Georgia y de la interrupción de la red eléctrica de Ucrania en 2015 (cfr. COUNCIL ON FOREIGN RELATIONS. «Sandworm». Disponible en: https://www.cfr.org/cyber-operations/sandworm).

[15] VECTRA AI. «As the War in Ukraine Spirals, Vectra AI Announces Free Cybersecurity Services». 28 de febrero de 2022. Disponible en: https://www.vectra.ai/news/as-the-war-in-ukraine-spirals-vectra-ai-announces-free-cybersecurity-services

[16] BURT, Tom. «The hybrid war in Ukraine». Microsoft, 27 de abril de 2022. Disponible en: https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/

recopilar inteligencia militar y de política exterior[17] y obtener acceso a infraestructuras críticas —sobre todo a proveedores de servicios de energía— con el fin de apoyar la toma de decisiones del Gobierno ruso y mantener una preparación continua del entorno cibernético para futuras contingencias.

En el último informe de junio de 2022[18], los analistas llegaron a dos conclusiones. Por un lado, dos tercios de los ciberataques rusos lanzados en contra de Ucrania habrían fracasado en los primeros meses de la guerra. Parece ser que Ucrania está bien preparada para defenderse de los ciberataques, gracias en parte al trabajo de empresas como Microsoft y Google, que trasladan gran parte de los sistemas y bases de datos ucranianos a la nube, a servidores fuera de Ucrania. Por otro lado, la campaña de desinformación de Moscú para establecer una narrativa de la guerra favorable a Rusia que está funcionando mejor de lo esperado. Rusia está utilizando la desinformación con el objetivo de manipular psicológicamente a la sociedad ucraniana y reforzar la legitimación de su invasión. Esta estrategia es muy bien conocida: la misma doctrina militar rusa[19] establece que la información y la guerra psicológica sientan en gran medida las bases para la victoria en la guerra.

## El cambio de la estrategia cibernética rusa

Según lo anterior, está claro que Rusia no ha utilizado la estrategia cibernética como se pensaba, así como tampoco se ha producido el Cyber Pearl Harbor[20] advertido durante años. Desde el 24 de febrero los ciberataques contra los sistemas ucranianos han sido mucho menos dañinos de lo que podrían haber resultado. Según el informe de ESET, los dos ataques más relevantes han sido los de los *malware* CaddyWiper, el 14 de marzo,

[17] Tal y como ha sucedido en otros conflictos en los cuales Rusia ha estado involucrada, como Georgia (2008) y Siria (desde 2011 hasta la actualidad).
[18] MICROSOFT. *Defending Ukraine: Early Lessons from the Cyber War.* 22 de junio de 2022. Disponible en https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
[19] MINISTRY OF FOREIGN AFFAIRS. *Doctrine of Information Security of the Russian Federation.* Diciembre de 2016. Disponible en: https://publicintelligence.net/ru-information-security-2016/
[20] Durante años los expertos han advertido que la próxima guerra se librará en el ciberespacio. Un Pearl Harbor cibernético derretiría los sistemas gubernamentales, paralizaría la infraestructura crítica y hundiría a las fuerzas armadas y las sociedades modernas en la oscuridad (ROHOZINSKI, Rafal. «The missing "cybergeddon": What Ukraine can tell us about the future of cyber war». International Institute for Strategic Studies, 9 de marzo de 2022. Disponible en: https://www.iiss.org/blogs/survival-blog/2022/03/the-missing-cybergeddon-what-ukraine-can-tell-us-about-the-future-of-cyber-war).

e Industroyer2, el 8 de abril. Y en ambos casos fueron mitigados rápidamente por la colaboración ESET-CERT-UE.

Por lo tanto, las infraestructuras críticas de Ucrania —como el sistema de comunicaciones, los sistemas de energía y los de atención médica— han sufrido en mayor medida ataques militares directos que cibernéticos. Esto resulta muy curioso, pues cuando las fuerzas rusas invadieron la península de Crimea en 2014 ya habían cerrado la infraestructura de telecomunicaciones de la península, inhabilitado la gran mayoría de los sitios web ucranianos y bloqueado los teléfonos móviles de varios funcionarios ucranianos[21].

Existen principalmente tres argumentos que explican el cambio estratégico de Rusia en el ciberespacio.

En primer lugar, el principal motivo, según Lauren Zabierek[22], es que Rusia ha querido evitar una escalada de tensiones con terceros Estados o efectos indirectos más allá de Ucrania[23]. Concretamente, el Kremlin habría intentado prevenir un efecto *spillover* de ciberataques que pudieran desencadenar una guerra cibernética con Occidente. Ninguna potencia internacional tiene interés en provocar una guerra mundial cibernética, ni siquiera Rusia —sobre todo en un contexto en el cual su economía está muy debilitada—. Es muy probable también que la guerra haya creado una especie de distensión en la que ambas partes entienden que los ciberataques catastróficos darían como resultado la destrucción mutua y asegurada de sus infraestructuras críticas.

Además, la intención de Putin ha sido evitar la invocación del artículo 5 del Tratado del Atlántico Norte[24], sobre todo después de que la organización haya actualizado su Concepto Estratégico en la Cumbre de Madrid de junio de 2022. Si la versión anterior[25],

---

[21] EUROPEAN UNION EXTERNAL ACTION. «Eight Years On, War in Ukraine Brings Back Painful Memories of Crimea's Invasion». 18 de marzo de 2022. Disponible en: https://www.eeas.europa.eu/eeas/eight-years-war-ukraine-brings-back-painful-memories-crimea%E2%80%99s-invasion_en

[22] Experta en ciberseguridad y directora ejecutiva del Cyber Project de la Escuela Harvard Kennedy.

[23] Cfr. GIBNEY, Elizabeth. «Where is Russia's cyberwar? Researchers decipher its strategy», *Nature.* 17 de marzo de 2022. Disponible en: https://www.nature.com/articles/d41586-022-00753-9

[24] Cfr. CUBEIRO CABELLO, Enrique. «El ciberespacio en la guerra de Ucrania» (Documento de Opinión, n.º 32). IEEE, 2022. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO32_2022_ENRCUB_Ucrania.pdf

[25] OTAN. *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* Lisboa, 19-20 de noviembre de 2010. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

de 2010, afirmaba brevemente el aumento de los ciberataques contra Occidente, el nuevo documento[26] acusa directamente a Rusia de utilizar operaciones cibernéticas maliciosas y una estrategia de desinformación contra los aliados para «establecer esferas de influencia» y «perseguir sus objetivos políticos de socavar el orden internacional». Rusia se convierte además en la «amenaza más significativa y directa» para la seguridad de la Alianza.

El segundo argumento sostiene que, dado que las operaciones cibernéticas no le proporcionaron una ventaja operativa en 2014, ahora Rusia ha priorizado sus acciones militares sobre ellas[27]. Los ataques cibernéticos no son todavía efectivos como herramientas de coerción en la guerra, ya que hasta el momento no han conseguido un efecto perceptible sobre la violencia en el mundo físico[28]. A pesar de ser cada vez más comunes, las operaciones cibernéticas en tiempos de guerra no son tan útiles como las bombas y los misiles cuando de lo que se trata es de infligir daño físico y psicológico al enemigo. En pocas palabras, una carga explosiva causa más daño a largo plazo que un *software* malicioso.

Asimismo, la guerra cibernética no puede reemplazar las formas tradicionales de combate. Los Estados no usarán la guerra cibernética en lugar de la tradicional, pero sí que dependerán cada vez más del ciberespacio como dominio para perseguir nuevos objetivos informativos[29].

Por último, según el tercer argumento —el más plausible—, el deseo de los Estados de aumentar sus capacidades en materia de ciberdefensa habría cobrado gran relevancia en los últimos años. Ucrania es el mejor ejemplo. En los últimos ocho años ha sobrevivido

[26] OTAN. *NATO 2022 Strategic Concept.* Madrid, 29 de junio de 2022. Disponible en https://www.nato.int/strategic-concept/

[27] ISHAK, Natasha. «Is Russia holding back from cyberwar?», *Vox*. 19 de marzo de 2022. Disponible en: https://www.vox.com/2022/3/19/22986316/russia-ukraine-cyber-attacks-holding-back

[28] KOSTIUK, Nadiya y ZHÚKOV, Yuri M. «Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?», *Journal of Conflict Resolution,* vol. 62, n.º 2. Febrero de 2019 (primera publicación en 2017). Disponible en: https://web.archive.org/web/20220316084344/https://journals.sagepub.com/doi/10.1177/0022002717737138

[29] La guerra cibernética tiene que ver ante todo con la información, con su control y utilización como medio para lograr objetivos políticos. Al ser principalmente un dominio informativo, el ciberespacio es más útil para perseguir objetivos informativos y manipular psicológicamente a la sociedad que se desea atacar que para ganar una guerra (KOSTYUK, Nadiya y GARTZKE, Erik. «Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine», *Texas National Security Review,* vol. 5, n.º 3. Verano de 2022. Disponible en: https://tnsr.org/2022/06/why-cyber-dogs-have-yet-to-bark-loudly-in-russias-invasion-of-ukraine/

a ataques rusos masivos contra su infraestructura crítica, así como a una ola de *malware* destructivo —NotPetya—. Estas lecciones vitales para el Gobierno ucraniano han reforzado su resiliencia y capacidad de respuesta. En el contexto actual, las defensas cibernéticas de Ucrania se han visto aumentadas gracias a la asistencia extranjera[30]. Además, Ucrania sigue manteniendo un alto nivel de operatividad y conectividad, gracias sobre todo a la inversión masiva[31] para establecer un servicio de internet satelital en el país, operado por SpaceX.

Sin embargo, algunos expertos apuntan que Rusia podría estar manteniendo en reserva sus armas cibernéticas más agresivas. Si la guerra terrestre se estanca y las sanciones financieras le afectan demasiado, Moscú aumentará los ataques cibernéticos contra Ucrania o apuntará, por ejemplo, a empresas y mercados financieros internacionales[32]. En este sentido, cabe destacar que, a pesar de que la mayor parte de la ciberactividad rusa se ha centrado en Ucrania, Microsoft ha detectado ciento veintiocho intrusiones en la red en cuarenta y dos países[33]. Por lo tanto, Ucrania no es el único Estado víctima de ciberataques desde el inicio de la guerra. Se han detectado intrusiones en España[34], Alemania[35] o el Reino Unido[36], entre otros lugares.

---

[30] Para Cubeiro Cabello la actuación de los Estados, en concreto de EE. UU, ha sido clave (cfr. CUBEIRO CABELLO, Enrique. *Op. cit*.). El Mando de Ciberdefensa (US CYBERCOM) y la Agencia de los Estados Unidos para el Desarrollo Internacional han reducido considerablemente las vulnerabilidades de los servicios esenciales e infraestructuras críticas ucranianas, fortaleciendo su capacidad para prevenir y mitigar los ataques cibernéticos.

[31] Según varias fuentes, el Gobierno estadounidense ha gastado alrededor de 800.000 dólares en el establecimiento del servicio y ha entregado más de cinco mil terminales al Gobierno ucraniano (COLLIER, Kevin. «Starlink internet becomes a lifeline for Ukrainians». NBC News, 2022. Disponible en: https://www.nbcnews.com/tech/security/elon-musks-starlink-internet-becomes-lifeline-ukrainians-rcna25360).

[32] GIBNEY, Elizabeth. *Op. cit.*

[33] Cfr. MICROSOFT. *Op. cit.*

[34] A partir de la invasión, el envío de correos electrónicos peligrosos por parte de grupos rusos a los principales medios de comunicación españoles de prensa, radio y televisión ha aumentado un 3000 por ciento y ha alcanzado picos de más del 4000 por ciento desde el pasado 1 de marzo (AGUIRREGOMEZCORTA, Marta. «El otro campo de batalla: se intensifican los ciberataques rusos a las empresas españolas», *Nius.* 4 de marzo de 2022. Disponible en: https://www.niusdiario.es/ciencia-y-tecnologia/tecnologia/otra-guerra-ciberataques-rusos-alcanzan-empresas-espanolas_18_3292022292.html).

[35] En mayo de 2022, Killnet, un grupo de piratas informáticos prorrusos, dejó fuera de servicio las páginas web del Ministerio de Defensa alemán, el Parlamento, la Policía Federal y varias autoridades policiales locales (GEBAUER, Matthias *et al*. «Putin-Fans attackieren deutsche Behördenseiten», *Der Spiegel*. 6 de mayo de 2022. Disponible en: https://www.spiegel.de/politik/deutschland/killnet-cyberangriffe-wladimir-putin-fans-attackieren-deutsche-behoerdenseiten-a-2be17f20-3688-4674-b82d-d7889a532c80).

[36] Una de cada tres empresas británicas avisaba a finales de marzo de que estaba experimentando ciberinfracciones o ciberataques al menos una vez a la semana (DEPARTMENT FOR DIGITAL, CULTURE, MEDIA AND SPORT y LOPEZ MP, Julia. «Businesses urged to boost cyber standards as new data reveals nearly a third of firms suffering cyber attacks hit every week». UK Government, 30 de marzo

## Los piratas informáticos en la guerra

Uno de los componentes más interesantes de la guerra cibernética ruso-ucraniana es que los Estados no son los únicos actores, sino que cada una de las partes ha recibido el apoyo de diversos grupos cibernéticos. Ucrania ha recibido el apoyo de grupos de piratas informáticos como Anonymous, GhostSec o de los Ciberpartisanos bielorrusos, mientras que a favor de Rusia están, entre otros grupos, Conti, Free Civilian o Killnet.

Además, Ucrania ha seguido una estrategia cibernética única en el conflicto: el 26 de febrero el Gobierno anunció la creación de un «ciberejército de voluntarios» para proteger la infraestructura crítica ucraniana, realizar misiones de espionaje cibernético contra las tropas rusas y atacar objetivos militares rusos. Hasta ahora, los hacktivistas han conseguido borrar muchos archivos CIS, cambiar el nombre de cientos de carpetas a «putin_stop_this_war» y exponer las direcciones de correo electrónico y las credenciales administrativas de miembros del Gobierno ruso. Asimismo, de cien bases de datos rusas analizadas, noventa y dos se habían visto comprometidas por los piratas informáticos.[37] Yurii Shchyhol, jefe del Servicio Estatal de Comunicaciones Especiales y Protección de la Información de Ucrania, ha reconocido la importancia de la labor de los hacktivistas: al proporcionar información a las instituciones gubernamentales sobre cómo defender adecuadamente la infraestructura crítica, ninguno de los ataques cibernéticos ha permitido al enemigo destruir base de datos alguna o causar una fuga de datos privados[38]. No obstante, estos grupos deben tener cautela, ya que apuntar a un objetivo equivocado o ejecutar una operación desproporcionada puede crear tensión adicional.

El establecimiento de grupos de piratas informáticos en ambos frentes ha llevado a Clarke[39] a determinar que la guerra en Ucrania está cambiando la toma de decisiones de los grupos cibernéticos en lo que respecta al reclutamiento. Antes de la guerra, los mercenarios cibernéticos se configuraban como grupos apolíticos, cuyas motivaciones

---

de 2022. Disponible en: https://www.gov.uk/government/news/businesses-urged-to-boost-cyber-standards-asnew-data-reveals-nearly-a-third-of-firms-suffering-cyber-attacks-hit-every-we

[37] DELCKER, Janosch. «Ukraine's IT army: Who are the cyber guerrillas hacking Russia?», *Deutsche Welle*. 24 de marzo 2022. Disponible en: https://www.dw.com/en/ukraines-it-army-who-are-the-cyber-guerrillas-hacking-russia/a-61247527

[38] ROSEN, Kenneth R. «The Man at the Center of the New Cyber World War», *Politico*. 14 de julio de 2022. Disponible en: https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486

[39] CLARKE, Aaron. «Hacking the Invasion: The Cyber Implications of Russia's Invasion of Ukraine», *Third Way*. 7 de junio de 2022. Disponible en: http://thirdway.imgix.net/pdfs/hacking-the-invasion-the-cyber-implications-of-russias-invasion-of-ukraine.pdf

eran el dinero —a menudo—, la alteración de infraestructuras críticas o una afiliación vaga con alguna causa. Sin embargo, el contexto actual es distinto. Si estos grupos estaban impulsados anteriormente por las ganancias de los pagos de rescate, ahora se despliegan en un conflicto armado por el bien de su país o de un país con el que se sienten solidarios. Las reglas anteriores de los grupos de piratas informáticos en la región se están erosionando y estos se están dividiendo a lo largo de las líneas de conflicto[40]. En pocas palabras, los piratas informáticos se están enfrentando entre sí, en favor o en contra de Rusia. A medida que continúan los ataques cibernéticos y la contienda, las divisiones cada vez más profundas entre los dos frentes suponen un cambio determinante de cara a futuros conflictos.

En el frente ruso, la fragmentación de los grupos[41] y la falta de normas acordadas podrían suponer una futura modificación de las modalidades de reclutamiento. En lugar de aceptar a alguien con experiencia cibernética para llevar a cabo los ataques, estos grupos podrían comenzar a exigir que se mantenga una cierta «lealtad política» para la admisión.

Asimismo, la motivación de los ciberataques está cambiando: ya no es solamente intelectual o económica, sino también política, por lo que sus consecuencias han dejado de centrarse solamente en causar una pérdida económica para extenderse a los conflictos entre Estados, que también demuestran y miden sus fuerzas en el ciberespacio.

En el frente ucraniano, el Gobierno ha expresado su apoyo al ciberejército de voluntarios, pero también ha dejado claro que no trabajan al unísono[42]. Es la primera vez en la historia de Ucrania —y probablemente en la historia mundial— en la que casi 300.000 ciberprofesionales voluntarios coordinan sus esfuerzos para planificar y ejecutar cualquier ataque a la infraestructura cibernética rusa sin necesidad de respaldo

[40] ACCENTURE. *Global Incident Report: Threat Actors Divide along Ideological Lines over the Russia-Ukraine Conflict on Underground Forums*. 2022. Disponible en: https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf

[41] El ejemplo más relevante se produjo el 19 de mayo de 2022, cuando el grupo cibernético prorruso Conti anunció el fin de sus operaciones tras eliminar oficialmente su infraestructura de ataques y dividir sus actividades cibernéticas maliciosas entre grupos más pequeños.

[42] GILL, Jaspreet. «Why Ukraine recruiting amateur “IT army” could backfire», *Breaking Defense*. 2 de marzo de 2022. Disponible en: https://breakingdefense.com/2022/03/why-ukraine-recruiting-amateur-it-army-could-backfire/

estatal. Lo hacen por su cuenta. Aunque el Gobierno ucraniano pueda expresar su preocupación u objeciones a ciertas «tareas», nada impide que el grupo lleve a cabo un ataque sin su aprobación o que determinadas ramificaciones actúen fuera de los objetivos establecidos.

## Conclusiones

Tradicionalmente, Rusia ha sido muy activa en el ciberespacio, razón por la cual una de las creencias más extendidas entre los expertos es que sus capacidades cibernéticas son muy amplias. Sin embargo, en la práctica, se ha creado una brecha entre la actuación de Rusia en la guerra cibernética contra Ucrania y lo que los Estados y la doctrina suponían.

La combinación de ataques cinéticos con ataques cibernéticos en la guerra híbrida busca generalmente abrumar al enemigo en la toma de decisiones, crear disturbios sociales y polarización o paralizar infraestructuras críticas, como los servicios gubernamentales, la energía, las finanzas y el transporte. Rusia no ha conseguido ninguno de estos objetivos hasta ahora.

Asimismo, la estrategia cibernética rusa actual no ha sido nada eficaz en comparación con la utilizada en la anexión de Crimea en 2014, lo que principalmente se debe a que las capacidades cibernéticas defensivas de Ucrania no son las mismas que hace ocho años. Y además Ucrania cuenta con el apoyo de varios Estados, empresas —como Microsoft y Google— y sobre todo de piratas informáticos, como Anonymous o el ciberejército de voluntarios.

La gran novedad de la contienda atañe al protagonismo de los actores no estatales: por primera vez en la historia, cualquiera puede unirse a la guerra. Si de cara al futuro los grupos de piratas informáticos demuestran que no necesitan el apoyo gubernamental para actuar, la capacidad real de que un Estado controle la actividad maliciosa en su territorio cada vez será más limitada. Incluso en ausencia de un conflicto, los grupos de piratas informáticos externos podrían comenzar a formarse por razones puramente políticas. Esto supone que en los conflictos futuros los propios Estados podrían necesitar a actores externos que apoyen las actividades cibernéticas lanzadas contra el adversario.

Aunque el Cyber Pearl Harbor que se esperaba del primer gran choque entre Estados industriales avanzados en el siglo XXI no ha sucedido, la situación puede ir cambiando. La incertidumbre sobre la duración y la capacidad de destrucción de Rusia continuará modificando la dinámica del conflicto y podría alterar el desarrollo actual de su componente cibernético. Si bien la guerra cibernética total no ha surgido, el impacto en diferentes áreas de la ciberseguridad se sentirá en futuras contiendas. Desde el inicio de la guerra, numerosos Estados han denunciado el aumento de los ciberataques rusos contra sus infraestructuras.

Por consiguiente, resulta absolutamente necesario para la paz y la seguridad internacionales que Occidente priorice una estrategia de ciberdefensa coherente y aumente la inversión en capacidades cibernéticas defensivas —y quizás ofensivas también— para responder de manera adecuada a las amenazas del ciberespacio.

A pesar de que la guerra cibernética en Ucrania no ha transcurrido tal y como se esperaba, ha jugado un papel importante desde el inicio, poniendo de manifiesto la existencia de dos desafíos en la sociedad internacional: por un lado, comprender bajo qué circunstancias podría o no ocurrir una ciberguerra en futuros conflictos y, por otro lado, determinar hasta qué punto los Estados siguen siendo los únicos actores que controlan el ciberespacio ante el desafío de los nuevos hacktivistas.

*Ada Gavrila**
Politóloga por la Universidad de Granada
Delegación de la Junta de Andalucía en Bruselas
@ada_gavrila