ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

32/2022 4 de abril de 2022

*Enrique Cubeiro Cabello**

El ciberespacio en la guerra de Ucrania

El ciberespacio en la guerra de Ucrania

Resumen:

Un mes después del inicio de la invasión de Ucrania por las tropas rusas, el autor analiza el empleo que del ciberespacio se ha hecho del conflicto, especialmente por parte de Rusia, a través de la crónica de las acciones más notables que han trascendido a los medios. Finalmente, expone las claves que a su juicio podrían explicar el por qué el ciberespacio está jugando un papel mucho menos relevante y decisivo que el que muchos expertos vaticinaban *a priori* y las razones por las que Rusia no estaría obteniendo excesivos éxitos en un ámbito de las operaciones en el que se le suponía la supremacía al inicio de la invasión.

Palabras clave:

Rusia, Ucrania, Putin, ciberataque, ciberguerra, ciberespionaje, propaganda, *malware*, infraestructura crítica, guerra híbrida, phishing, Anonymous.

Cyberspace in the Ukrainian war

Abstract:

One month after the start of the invasion of Ukraine by Russian troops, the author analyses, through the chronicle of the most notable actions revealed by the media, how both opposing parties (especially Russia) are using cyberspace to support their objectives. Finally, he exposes the key elements that, in his opinion, could explain why cyberspace is playing a much less relevant and decisive role than the one that many experts predicted a priori and the reasons why Russia would not be obtaining excessive success in a domain of operations in which its supremacy had been taken for granted at the beginning of the invasion.

Keywords:

Russia, Ukraine, Putin, cyberattack, cyberwarfare, cyberespionage, propaganda, malware, critical infrastructure, hybrid warfare, phishing, Anonymous.

Cómo citar este documento:

CUBEIRO CABELLO, Enrique. *El ciberespacio en la guerra de Ucrania*. Documento de Opinión IEEE 32/2022.
https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO32_2022_ENRCUB_Ucrania.pdf y/o enlace bie[3] (consultado día/mes/año)

El ciberespacio en la guerra de Ucrania

Transcurrido un mes desde el inicio de la invasión de Ucrania por las tropas rusas, parece un buen momento para analizar qué está pasando en la dimensión ciberespacial del conflicto; dimensión que es, sin duda, la más opaca por motivos obvios.

A priori, muchos analistas esperaban que Rusia explotara sus enormes capacidades para operar en y a través del ciberespacio para inclinar, todavía más, la contienda a su favor. Esta creencia nacía de varias circunstancias. En primer lugar, por el de sobra conocido empleo sistemático, desde hace más de una década, del ciberespionaje, el cibersabotaje, la desinformación y la propaganda por parte de los rusos en el marco de eso que se ha dado por llamar guerra híbrida y que podríamos definir como el empleo coordinado y sincronizado de todas las capacidades de un Estado —económicas, militares, de información, diplomáticas, etc.— para combatir y erosionar a un oponente sin rebasar jamás el umbral que pueda desencadenar el derecho de respuesta en legítima defensa e, incluso, imposibilitando cualquier tipo de respuesta. Dado que la utilización de esas capacidades en tiempo de paz podría estar sujeta a prevenciones que seguramente desaparecerían en caso de conflicto armado, se suponía que Rusia las utilizaría de forma masiva, intensa y decisiva. Al fin y al cabo, así lo había hecho en anteriores ocasiones: ataques masivos de denegación de servicio, simultaneados con campañas de desinformación habían sido empleados con anterioridad contra Estonia en el 2007 y contra Georgia y Kirguistán en los años siguientes, justo antes de iniciarse las campañas militares contra estos dos últimos Estados[1]. Y, en estos más de 10 años transcurridos, se suponía que Rusia habría multiplicado enormemente sus capacidades.

Además, Rusia lleva desde el 2014 utilizando a Ucrania como una especie de campo de pruebas para sus ciberarmas y las campañas de desinformación y propaganda. Por tal motivo, se sospechaba que las agencias rusas podrían haber posicionado malware en infinidad de sistemas ucranianos (de infraestructuras críticas, de servicios esenciales, de información gubernamentales, y hasta de mando y control, de combate y de armas de sus fuerzas armadas) y que, llegado el momento decisivo, se activarían al unísono

[1] KOZLOWSKI, Andrzej. *Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan.* Disponible en: https://eujournal.org/index.php/esj/article/view/2941

provocando algo así como un «apagón» del ciberespacio ucraniano, con el que vendría el caos, la confusión, la desmoralización y hasta la inacción defensiva de su oponente.

En resumen, lo que se vaticinaba era que Rusia emplearía de forma simultánea, y en una fase que se iniciaría con cierta antelación (días, semanas) a la invasión militar, un amplio abanico de acciones en y a través del ciberespacio. Entre ellas:

- Activación de *malware* previamente posicionado en objetivos de interés (fundamentalmente, con fines de sabotaje).
- Ciberataques masivos de denegación distribuida de servicios (DDoS) contra sitios web ucranianos.
- Ciberataques masivos contra infraestructuras críticas y servicios esenciales de Ucrania (*wipers*, *ransomware*, DDoS).
- *Defacements* masivos en sitios oficiales ucranianos.
- Campañas masivas de *phishing*.
- Campañas masivas de suplantación de identidad en redes sociales (RRSS).
- Distribución de *malware* altamente sofisticado (*wipers*, *ransomware*, troyanos, *exploit kits)*.
- Potentes campañas de desinformación y propaganda.
- Iniciativa, manejo y control de la narrativa.

Además, se esperaba que esas actividades no se circunscribieran al ciberespacio ucraniano y que estuvieran dirigidas, en mayor o menor medida, a terceros actores, especialmente a la OTAN, la UE y a sus Estados miembros.

Tampoco parecía muy probable la intervención ofensiva en el conflicto de otros actores. Se consideraba más que probable que Rusia avasallase desde el principio a Ucrania y mantuviera una supremacía en el ciberespacio que le otorgara su control total y que, debido a la transversalidad del ciberespacio, tuviera enorme impacto en los ámbitos operativos terrestre, naval y aéreo.

Pero, como ha ocurrido en cada guerra en las tres o cuatro últimas décadas, la corriente mayoritaria entre los analistas se ha visto contestada por una realidad inesperada.

Quizá lo más llamativo de esta guerra es que, cuando todo el mundo suponía un conflicto diferente a todo lo anterior debido al esperado empleo masivo de las «herramientas

híbridas», nos hemos encontrado con el conflicto más convencional de las últimas décadas.

Y frente a aquellos que vaticinaban que la próxima gran guerra comenzaría con un clic y se dirimiría en gran medida en y a través del ciberespacio, nos encontramos una guerra en la que carros y obuses tienen casi el total protagonismo, con una pequeña dimensión aérea y naval y un peso casi insignificante de «lo ciber», al menos en apariencia.

Recopilemos cronológicamente lo más reseñable acontecido en la dimensión ciberespacial del conflicto (al menos, de lo que ha podido conocerse a través de fuentes abiertas):

Entre el 13 y el 15 de enero —unos 40 días antes de la invasión y justo después del fracaso de las conversaciones entre EE. UU. y Rusia sobre la posible admisión de Ucrania en la OTAN— se produjo una oleada de ataques que dejaron sin servicio varias decenas de sitios web gubernamentales, entre los que estaban el del Ministerio de Relaciones Exteriores, el Gabinete de Ministros y el Consejo de Seguridad y Defensa, así como servicios bancarios[2]. Los atacantes reemplazaron los sitios web con texto en ucraniano y ruso en los que decían: «¡Ucranianos! ... Toda la información sobre ti se ha hecho pública. Ten miedo y espera algo peor. Es tu pasado, presente y futuro» (Figura 1).

[2] Disponible en: https://www.reuters.com/technology/massive-cyberattack-hits-ukrainian-government-websites-amid-russia-tensions-2022-01-14/

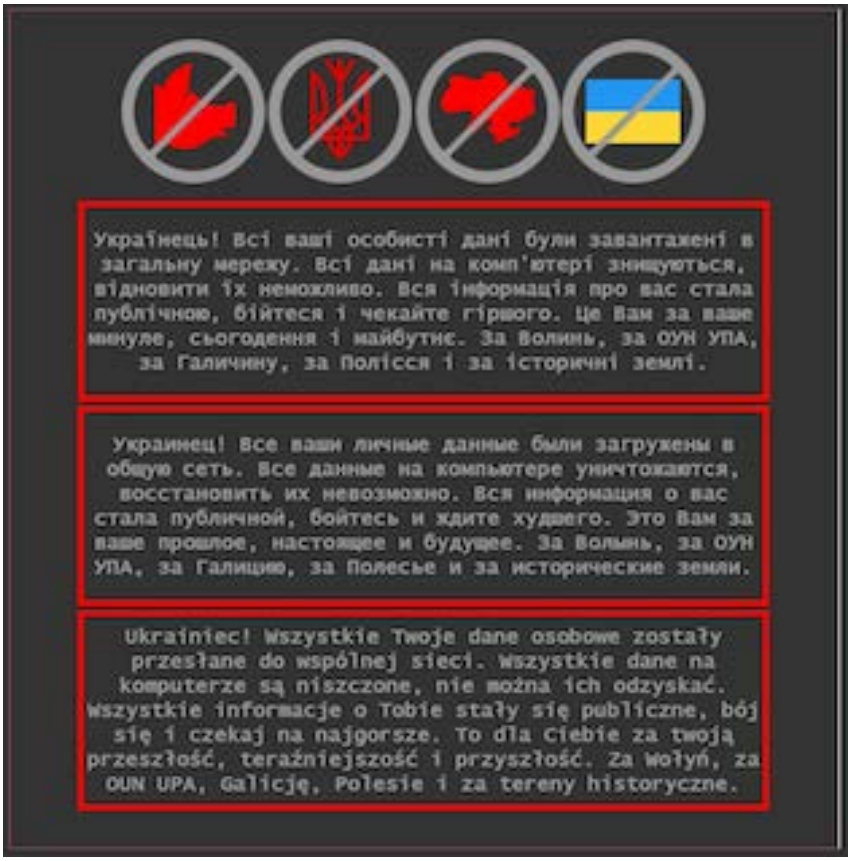

Figura 1. Texto aparecido en los dispositivos afectados por el ataque de mediados de enero.

Según fuentes oficiales ucranianas, no se filtró ningún dato y la mayoría de los sitios fueron restaurados en unas pocas horas.

En esas mismas fechas, se detectó por vez primera un *malware* cuya estructura era similar a la de un *ransomware*, pero que carecía de función de recuperación, por lo que su finalidad era únicamente la de borrado. El *wiper*, denominado DEV-0586 o WhisperGate, afectó a numerosos dispositivos de organizaciones gubernamentales y de entidades civiles ucranianas[3]. El Gobierno de Ucrania acusó de estos ataques a Rusia, lo que fue negado por el gobierno ruso.

Tras estos hechos, la OTAN anunció que daría a Ucrania acceso a su plataforma de intercambio de información sobre *malware*[4].

El 15 de febrero, una segunda gran oleada de ataques de denegación distribuida de servicios (DDoS) golpeó los sitios web del Ministerio de Defensa, el Ejército y los dos

[3] Disponible en: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[4] Disponible en: https://www.nato.int/cps/en/natohq/news_190850.htm

bancos más grandes de Ucrania, afectando a las aplicaciones móviles y los cajeros automáticos de los bancos[5]. Tanto el Gobierno del Reino Unido como el Consejo de Seguridad Nacional de los EE. UU. atribuyeron públicamente el ataque a la Dirección Principal de Inteligencia (GRU) de Rusia, declarando haber observado la transmisión de grandes volúmenes de información desde la infraestructura conocida del GRU hacia las IP y dominios afectados[6,7]. Nuevamente, desde el Kremlin se negó que el ataque se originara en Rusia.

El 23 de febrero, una tercera oleada de ataques DDoS eliminó varios sitios web gubernamentales, militares y bancarios de Ucrania[8]. El mismo día, *malware* de borrado de datos fue detectado en cientos de dispositivos pertenecientes a organizaciones ucranianas, que abarcaban los sectores financiero, de defensa, de aviación y de las tecnologías de la información[9]. El *malware*, bautizado como HermeticWiper, fue compilado a finales de diciembre de 2021[10].

El ataque coincidió con el reconocimiento ruso de las regiones separatistas en el este de Ucrania y la autorización del despliegue en ellas de tropas rusas, que se iniciaría al día siguiente. De nuevo hubo lanzamiento de acusaciones desde EE. UU. y Reino Unido[11], negadas por Rusia.

El 27 de febrero, la organización hacktivista Anonymous anunciaba en Twitter estar «oficialmente en guerra contra el Gobierno ruso» y prometía apoyar a Ucrania contra «la brutal invasión del Kremlin»[12]. El mismo día declaraban haber echado abajo el sitio web del Ministerio de Defensa ruso[13], sin que esto haya sido confirmado.

---

[5] MCLAUGHLIN, Jenna. *Ukraine says government websites and banks were hit with denial of service attack.* Disponible en: https://www.npr.org/2022/02/15/1080876311/ukraine-hack-denial-of-service-attack-defense?t=1648144256783

[6] Disponible en: https://www.ncsc.gov.uk/news/russia-ddos-involvement-in-ukraine

[7] RFE/RL. U.S., U.K. Say Russian Government Responsible For Cyberattack On Ukraine. Disponible en: https://www.rferl.org/a/us-blames-russia-cyberattack-ukraine/31710689.html

[8] CERULUS, Laurens. *Minister: Ukraine websites down in another 'massive' online attack.* Disponible en: https://www.politico.eu/article/minister-ukraine-websites-down-in-another-massive-online-attack/

[9] GUERRERO-SAADE, Juan Andrés. *HermeticWiper: New Destructive Malware Used In Cyber Attacks on Ukraine.* Disponible en: https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

[10] EDITOR. *HermeticWiper: nuevo malware que borra datos ataca a Ucrania.* Disponible en: https://www.welivesecurity.com/la-es/2022/02/24/hermeticwiper-nuevo-malware-tipo-wiper-ataca-ucrania/

[11] TIDY, Joe. *Ukraine crisis: 'Wiper' discovered in latest cyber-attacks.* Disponible en: https://www.bbc.com/news/technology-60500618

[12] MILMO, Dan. *Anonymous: the hacker collective that has declared cyberwar on Russia.* Disponible en: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

[13] BUZZ Staff. *'Anonymous' Hackers' Cyber War Against Russia For Ukraine Has Twitter Rooting.* Disponible en: https://www.news18.com/news/buzz/anonymous-hackers-cyber-war-against-russia-for-ukraine-has-twitter-rooting-4812329.html

El 28 de febrero, la compañía estadounidense de comunicaciones por satélite Viasat emitió un comunicado en el que informaba de que procedía a investigar un ciberataque que había provocado una interrupción parcial de sus servicios de banda ancha en Ucrania y en toda Europa[14]. Al parecer, los primeros indicios atribuían la interrupción al mismo ataque DDos que había afectado a bancos y sitios gubernamentales de Ucrania el día 23 de febrero.

A primeros de marzo, la compañía Avast anunciaba la distribución gratuita de un descifrador para la cepa de *ransomware* Hermetic Wiper[15], periodo inusualmente breve para lo que suele ser habitual en el lanzamiento de una solución frente a un *ransomware*.

El 3 de marzo, un grupo afín a Anonymous declaraba haber atacado la Agencia Espacial de Rusia, lo que fue desmentido por el director de la Agencia, que calificó a los supuestos atacantes de «estafadores de poca monta»[16]. Del mismo modo, algunos grupos de hackers (por ejemplo, Conti) declararon su apoyo a Putin y amenazaron a aquellos que actuaran en su contra[17].

Ese mismo día, el Servicio de Seguridad de Ucrania (SSU) anunciaba que piratas informáticos «enemigos» habían comprometido diversos sitios web pertenecientes a organismos oficiales ucranianos a través de los cuales estaban distribuyendo falsos comunicados de capitulación de Ucrania[18].

Según diversos informes, a partir del día 6 de marzo, Rusia incrementa significativamente la intensidad de las campañas de *phishing* contra la población ucraniana, con la intención de insertar *malware* en sus dispositivos[19]. Debido al éxodo masivo hacia occidente, estas campañas llegan con bastante intensidad a Polonia y Hungría.

En torno al 15 de marzo, Anonymous cambia su estrategia de atacar sitios web e infraestructuras rusas para centrarse en los ataques a las multinacionales (por ejemplo,

---

[14] Disponible en: https://www.reuters.com/business/aerospace-defense/satellite-firm-viasat-probes-suspected-cyberattack-ukraine-elsewhere-2022-02-28/

[15] Disponible en: https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-hermeticransom-victims-in-ukraine/

[16] SENDINO, Sara. *Anonymous ataca la agencia espacial rusa y su director les llama "estafadores de poca monta".* Disponible en: https://www.lasexta.com/tecnologia-tecnoxplora/ciencia/anonymous-ataca-agencia-espacial-rusa-director-llama-estafadores_202203036220f9915bbac900016d2fb9.html

[17] BING, Christopher. *Russia-based ransomware group Conti issues warning to Kremlin foes.* Disponible en: https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/

[18] GATLAN, Sergiu. *Ukraine says local govt sites hacked to push fake capitulation news.* Disponible en: https://www.bleepingcomputer.com/news/security/ukraine-says-local-govt-sites-hacked-to-push-fake-capitulation-news/

[19] KREBS, Brian. *Report: Recent 10x Increase in Cyberattacks on Ukraine.* Disponible en: https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/

Nestlé) que siguen operando en Rusia[20] (Figura 2), así como a intentar romper el bloqueo informativo al que Putin ha sometido a su propia población, mediante el empleo de campañas masivas de SMS y WhatsApp[21], cuyos efectos reales se desconocen por el momento. Por esas mismas fechas, algunas fuentes informan de la práctica desarticulación del grupo Conti, al haber sido expuesta información crítica sobre el grupo por *insiders* ucranianos[22].

El 21 de marzo, el presidente Biden alertaba de que Rusia podría lanzar posibles ciberataques contra su país en los próximos días: «Tenemos información de inteligencia que indica que Rusia está explorando opciones para potenciales ciberataques»[23]. Biden urgía al sector privado estadounidense, propietario y gestor de la mayoría de las infraestructuras críticas y servicios esenciales de la nación, a «acelerar los esfuerzos para cerrar sus puertas digitales» y a reforzar sus sistemas de seguridad.

Y, para finalizar, el 24 de marzo, fecha de cierre de este artículo, cuentas simpatizantes del grupo Anonymous se hacían eco del ataque del grupo hacktivista al Banco Central de Rusia[24] y avisaban de la publicación inminente de miles de archivos confidenciales obtenidos en el ataque.

[20] Disponible en: https://www.dailymail.co.uk/news/article-10639253/Anonymous-hackers-tell-companies-operating-Russia-pull-youre-next.html

[21] DEL CASTILLO, Carlos. *Anonymous centra su "ciberguerra" contra Rusia en torpedear la censura del Kremlin.* Disponible en: https://www.eldiario.es/tecnologia/anonymous-centra-ciberguerra-rusia-torpedear-censura-kremlin_1_8831374.html

[22] LAPIENYTĖ, Jurgita. *Conti leaks: pro-Ukrainian member exposed more gang's chats and Trickbot's source code.* Disponible en: https://cybernews.com/news/conti-leaks-pro-ukrainian-member-exposed-more-gangs-chats-and-trickbots-source-code/

[23] SGANGA, Nicole. *"It's coming": President Biden warns of "evolving" Russian cyber threat to U.S.* Disponible en: https://www.cbsnews.com/news/russia-cyber-attack-threat-biden-warning/

[24] FERNÁNDEZ, Manuel. *Anonymous habría hackeado el Banco de Rusia: amenaza con publicar miles de documentos.* Disponible en: https://www.elespanol.com/omicrono/software/20220324/anonymous-hackeado-banco-rusia-amenaza-publicar-documentos/659684106_0.html

Figura 2. Comunicado en Twitter de la cuenta Anonymous TV publicado el 20 de marzo de 2022.

Por lo tanto, de manera resumida, el panorama en el ciberespacio ha venido hasta ahora dibujado por lo siguiente:

- Ataques rusos muy puntuales a infraestructuras críticas y servicios esenciales de Ucrania.
- Ataques masivos rusos a sitios web de Ucrania (fundamentalmente, DDoS).
- Numerosos *defacements* en sitios oficiales de Ucrania.
- Campañas de *phishing* y suplantaciones de identidad a media escala en RRSS.
- Distribución limitada de *malware* ruso de sofisticación media-baja.
- Ámbito de actividad bastante circunscrito a Ucrania.
- Anonymous y otros grupos hacktivistas han tomado partido contra Rusia (con escaso impacto hasta ahora).

- Campañas rusas de desinformación y propaganda, con gran efectividad en territorio ruso y Estados afines y escasa en el resto del Mundo.
- Narrativa ampliamente a favor de Ucrania, con Rusia a la defensiva y muy escasa capacidad de contranarrativa.

Es decir, se ha cumplido lo esperado en lo referente a ataques contra sitios web, cuentas oficiales y redes sociales, e incluso podemos identificar dos fases diferenciadas:

- Una primera, previa la invasión, iniciada en torno al 13 de enero, enfocada a la preparación del entorno operacional (esencialmente, a provocar temor, caos, confusión en la población ucraniana, debilitando su voluntad de vencer y la confianza en sus dirigentes e instituciones).
- Una segunda, iniciada en el momento de la invasión, en la que se continuó con la metodología de la primera, intensificándose progresivamente y ampliando sus objetivos, probablemente existiendo cierta sincronización de las acciones con las del resto de ámbitos operacionales en el plano militar.

Pero, por lo general, todos los ataques han sido de escasa complejidad técnica y de efectos bastante efímeros. Para nada ha existido, de momento, algo parecido a ese «ciberapagón» pronosticado.

Y en cuanto a la desinformación y propaganda, ocurre algo similar. Las armas rusas puede que estén perdiendo efectividad por ser ya demasiado conocidas. Los ejércitos de troles y sus medios oficiales de desinformación parecen no ser tan efectivos como en épocas pasadas. El hecho de que la opinión pública esté de forma abrumadora a favor de Ucrania impide practicar esas tácticas rusas, exitosas en campañas anteriores en las que la igualdad entre las partes era mucho más acusada. También el que las redes sociales hayan aplicado medidas activas contra la desinformación y se haya amordazado a Sputnik y RT en la mayor parte del mundo han debilitado enormemente la capacidad del Kremlin para influir sobre la narrativa.

El que Rusia no haya impuesto su enorme superioridad para operar en el ciberespacio es algo que está suscitando gran interés. ¿No ha querido o no ha podido?

Al igual que ya hay numerosas voces que sostienen que la capacidad del ejército ruso para la guerra convencional ha sido ampliamente sobreestimada, hay quien extiende esa misma impresión al ciberespacio. La opacidad del ciberespacio y la sofisticación y

efectividad de algunas campañas rusas de ciberespionaje y sabotaje pueden haber llevado a calibrar esas capacidades muy por encima de la realidad. Desde luego, parece extraño que, de haber podido, Rusia no haya hecho un uso más amplio del ciberespacio contra su, *a priori*, débil oponente. Esa superioridad, y sus efectos sobre el resto de capacidades, habrían reducido notablemente la capacidad de respuesta ucraniana, disminuyendo su moral y voluntad de vencer, y permitiendo a Putin algo bastante más parecido a un paseo militar que lo que se está encontrando.

De ahí que haya quién considere que Rusia ya ha gastado su arsenal para el ciberespacio[25]. Porque resultaría extraño que, de tener esa capacidad en sus manos, Putin no la hubiera empleado ya de forma amplia y decisiva para evitar la prolongación de un conflicto cada vez más contestado en todo el mundo (Rusia incluida) y que siega la vida de decenas, si no centenares, de soldados rusos cada día. Según esta corriente de opinión, Rusia sería también un gigante con pies de barro en el ciberespacio.

Pero hay otras posibles explicaciones.

Por ejemplo, que ese supuestamente temible «ciberarsenal» ruso haya perdido bastante de su efectividad en los últimos meses. Para que un *malware* funcione, ha de explotar alguna vulnerabilidad en el sistema objetivo. Ucrania lleva años siendo apoyada por diversos Estados y organizaciones en la mejora de su nivel de ciberseguridad. Por lo que se sabe, esos apoyos experimentaron un gran salto cualitativo y cuantitativo desde octubre del año pasado, al involucrar EE. UU. en ello importantes recursos a través de su Mando de Ciberdefensa, el US CYBERCOM, y de algunas de sus principales compañías tecnológicas (por ejemplo, Microsoft)[26]. Ese apoyo habría permitido reducir de forma rápida y notable muchas de las vulnerabilidades existentes en sus infraestructuras críticas y servicios esenciales, lo que explicaría el tan elevado como inesperado nivel de conectividad y operatividad que todavía presentan a estas alturas del conflicto.

También hay quien sostiene que la intención de invadir Ucrania fue algo solamente conocido por el círculo más cercano al presidente Putin. El mantenimiento del secreto habría impedido planear debidamente la campaña a los diferentes organismos estatales con capacidad para ello. A mi juicio, esto no parece muy probable, salvo que en esas

[25] WOLF, Josephine. *Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine.* Disponible en: https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/

[26] Disponible en: https://www.windowscentral.com/microsoft-has-committed-over-35-million-help-ukraine

altas esferas se valorara la invasión como un paseo militar, que cualquiera sabe. Pero sigamos con el razonamiento. Es posible que en el resto de ámbitos operativos se haya hecho uso de planes de contingencia que no existían para el ciberespacio. Aunque *best sellers*, películas y series de televisión hayan creado la idea de que los ciberataques se planean y ejecutan en segundos, la realidad es muy otra. Un ciberataque dirigido puede requerir semanas o meses de concienzudo análisis. Por lo tanto, de estar en lo cierto, aquellos que opinan que la invasión pilló desprevenidas a las agencias de inteligencia y a las fuerzas armadas, sería probable que en cuestión de semanas o meses se intensificaran los ciberataques, una vez completadas las fases de análisis, *weaponization*, entrega, explotación, instalación, establecimiento del mando y control y acciones sobre el objetivo, propias de la *killchain* de un ciberataque complejo. En cualquier caso, esta situación demostraría que *una* de las creencias más extendidas entre los expertos (el preposicionamiento de malware en sistemas ucranianos para ser activado llegado el momento) no se habría producido. O, quizá, invitaría a sospechar que buena parte de él pudiera haber sido localizado y desactivado en esos últimos meses de intenso apoyo estadounidense.

El temor de Rusia a los efectos colaterales impredecibles que resultan inherentes a los ciberataques podría ser otro argumento. En un contexto en que los daños infligidos a Estados neutrales podrían tener unas consecuencias importantes, nos encontramos con unas «armas» cuyos efectos destructores, en algunas ocasiones propagados en cascada, pueden extenderse mucho más allá del objetivo pretendido. Stuxnet (2010) fue un ataque quirúrgico cuyo único objetivo era la central iraní de Natanz y, más concretamente, su planta de enriquecimiento de uranio. A pesar del aislamiento de la red objetivo, unos años más tarde los sistemas infectados en todo el mundo se contaban por millares[27]. NotPetya (2017) fue un ataque que se cree de origen ruso y dirigido muy específicamente contra Ucrania. En este caso, los sistemas infectados fueron mucho más numerosos y provocaron pérdidas que se estiman en torno a los 10 000 millones de dólares en todo el mundo[28] (la compañía Maersk valoró sus pérdidas en unos 200 millones[29]). El ciberespacio se percibe con frecuencia como un universo paralelo, en el

[27] VELUZ, Danielle. *STUXNET Malware Targets SCADA Systems.* Disponible en: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems
[28] GREENBERG, Andy. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* Disponible en: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[29] MATHEWS, Lee. *NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million.* Disponible en: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/

que existe una gran dificultad para la atribución de las acciones. Por ello, tendemos a pensar que Rusia no solo carece absolutamente de escrúpulos, sino también de temores al emplear sus cibercapacidades ofensivas. Pero puede que hayamos vuelto a errar en la evaluación. Es posible que Putin prefiera no correr el riesgo de extender el conflicto y haya renunciado, al menos por el momento, a utilizar algunas de las más potentes ciberarmas de su arsenal para evitar que esos daños colaterales, descontrolados e impredecibles, que podrían ser calificados de ataque armado, afecten a algún tercer Estado y puedan alterar una situación que tiene razonablemente controlada (por ejemplo, mediante la invocación por parte del Estado víctima del artículo 5 de la OTAN).

Por otra parte, el abrir una contienda ilimitada en el ciberespacio es algo que tampoco le conviene a Putin. Rusia es una potencia en lo que se refiere a capacidades ofensivas en el ciberespacio; aunque no la única ni la más capaz. Pero tiene un enorme «cibertalón» de Aquiles: la ciberseguridad de sus infraestructuras, redes y sistemas. Rusia no está precisamente considerado como uno de los países más ciberseguros del mundo[30]. Y, en el caso de un conflicto desatado en el ciberespacio, podría sufrir intensamente en sus carnes todo aquello de lo que lleva años aprovechándose.

En cualquier caso, lo que resulta evidente es que el ciberespacio no está jugando ese papel decisivo que muchos le auguraban y, también, que parece poco probable que esta situación varíe de forma sustancial a corto plazo.

Esto puede llevarnos a extraer conclusiones equivocadas (por ejemplo, a suponer que la dimensión ciberespacial va a jugar un papel residual en los conflictos modernos) que nos lleven a adoptar decisiones que nos pesen en un futuro (por ejemplo, a no dedicar suficientes recursos a esta capacidad militar). Seamos prudentes. Este es un conflicto muy peculiar y todavía desconocemos de él muchas cosas.

A pesar de lo visto, yo sigo opinando lo mismo que hace un mes: la importancia del ciberespacio en el devenir de los conflictos será cada vez mayor y, dada su transversalidad, la superioridad propia en los ámbitos terrestre, naval o aéreo nunca estará asegurada si el adversario cuenta con la superioridad ciberespacial.

Enrique Cubeiro Cabello
Capitán de navío

[30] FRISBY, Joshua. *Cybersecurity Exposure Index (CEI) 2020*. Disponible en: https://passwordmanagers.co/cybersecurity-exposure-index/