CEERI
Centro de Estudios Estratégicos de Relaciones Internacionales

Ciberguerra y Guerra Híbrida:

el conflicto Rusia-Ucrania como laboratorio bélico

Por **Miguel Mouso Genco**

Informe del Grupo de Investigación de Ciberespacio y Tecnología

Contenidos

Resumen _____ 4

Introducción _____ 5

La ciberguerra y su contexto: un acercamiento conceptual _____ 7

Tensión y guerra cibernética: el caso de Rusia y Ucrania _____ 10

Conclusiones: un laboratorio bélico digital y no tan digital _____ 15

Referencias _____ 17

Sobre el grupo

Las expresiones del ciberespacio afectan y alteran las relaciones entre naciones y de éstas con la sociedad civil. Este nuevo fenómeno tensiona las relaciones de poder tradicional entre los Estados, conjuntamente con las presiones y nuevas demandas de actores gubernamentales y no estatales digitalmente empoderados.

En ese sentido desde el CEERI nos hemos puesto el desafío de pensar e incorporar a la literatura internacional nuevas propuestas conceptuales para intentar explicar nuevas acciones de política ciber en la arena de la política internacional.

Líneas de investigación: El ciberespacio y su inclusión en las teorías de RI - Fake News y Deepfake - Ciberseguridad y Ciberguerras - Economía Digital y nuevas formas de integración.

Sobre el autor

Miguel Mouso Genco es estudiante de la Licenciatura en Relaciones Internacionales, Universidad Nacional del Centro de la Provincia de Buenos Aires (UNICEN), Argentina.

Sobre nosotros

El Centro de Estudios Estratégicos de Relaciones Internacionales (CEERI), es una organización no gubernamental, sin fines de lucro, independiente y plural.

Nuestra misión es generar herramientas que contribuyan al desarrollo de las sociedades, procurando la comunión e integración regional tanto a nivel público como privado.

Resumen

En los últimos años, la guerra ha experimentado transformaciones profundas, marcadas por fenómenos como la Guerra Híbrida y la incorporación del ciberespacio al ámbito bélico. En este contexto, los ciberataques a Infraestructura Crítica se han vuelto un componente central, particularmente en el marco de las tensiones entre Rusia y Ucrania antes y después de 2022. Este informe se propone analizar esas dinámicas propias de la ciberguerra, evaluar sus repercusiones en dicho conflicto y comprender cómo estas transformaciones están modificando las formas contemporáneas de la guerra. Para ello, se examinaron noticias, documentos técnicos e informes gubernamentales sobre ciberataques, sus impactos y la evolución de la ciberguerra. Los hallazgos muestran un incremento tanto cuantitativo como cualitativo en estos ataques, lo que indica que la ciberguerra no solo se ha integrado como nunca antes a las tácticas militares, sino que también ha complejizado y desdibujado los frentes tradicionales del conflicto. Asimismo, se observa una diversificación en la cantidad y tipo de actores involucrados, y un fortalecimiento de los vínculos entre Estados-nación y actores no estatales, lo cual amplía y redefine los límites de la arena de combate actual.

Palabras Clave

Ciberguerra, conflicto Rusia-Ucrania, Infraestructura Crítica, Guerra Híbrida, Ciberataques.

Cita sugerida

Mouso Genco, M. (19 de agosto, 2025). *Ciberguerra y Guerra Híbrida: el conflicto Rusia-Ucrania como laboratorio bélico*. Centro de Estudios Estratégicos de Relaciones Internacionales.

Introducción

Los últimos años han sido turbulentos en términos de conflictos bélicos, siendo un caso clave el desencadenamiento de la guerra Rusia-Ucrania a principios de 2022. A su vez, durante este tiempo, los avances tecnológicos y la digitalización han jugado un rol en la transformación de la arena bélica: drones, guerra de información, redes sociales, ofensivas cibernéticas, etc. Así, la fisonomía de la guerra está experimentando transformaciones significativas.

Este informe se centrará en una de sus dimensiones clave: la ciberguerra y los ataques a la Infraestructura Crítica (IICC), con foco en el conflicto ruso-ucraniano. Se considera que este conflicto ha representado para varios actores un *terreno de pruebas* para planificar y ejecutar diversas tácticas de guerra cibernética, incluso previo a la invasión del 2022. En este sentido, se abordarán algunas dinámicas particulares de la ciberguerra con el fin de comprender las repercusiones han tenido estos tipos de ataques en el caso ucraniano y cómo la integración de esta tácticas en el conflicto, en paralelo a otros cambios enmarcados dentro del concepto de *Guerra Híbrida* (GH), han ido modificando las formas del *campo de batalla*.

En primer lugar, se definirán conceptos que resultan esenciales para el marco del informe, brindando el contexto necesario para interpretar el sentido y las principales dinámicas de los ciberataques en la guerra. A su vez, se explicará brevemente la importancia de la IICC y la relevancia e impactos de los ciberataques en su contra. En segundo lugar, se analizará el caso del conflicto ruso-ucraniano y los los ciberataques contra la IICC. Esta sección se dividirá en tres: primero, se examinará la escalada ciberofensiva previa al inicio de la guerra formal, partiendo del 2013; luego, se destacarán las repercusiones originadas con el estallido del conflicto en el 2022; y en tercer lugar, se profundizará en la evolución de la ciberguerra hasta la actualidad. Por último, se brindarán algunas conclusiones extraídas del análisis del periodo previo y posterior al 2022.

Nota Metodológica

Para la realización de esta investigación se utilizó una variedad de fuentes, tanto primarias –noticias, bases de datos e informes y estadísticas gubernamentales– como secundarias –resaltando blogs corporativos, documentos técnicos especializados y artículos periodísticos de análisis.

En torno a los documentos técnicos se destacan bases de datos e informes especializados en la materia, principalmente de empresas privadas del ámbito de la ciberseguridad (como CheckPoint y Fortinet) e investigadores independientes (como Bellingcat), que profundizan en los pormenores de los ciberataques y posibilitan una mejor comprensión técnica de los mismos. También se utilizaron informes y estadísticas gubernamentales, principalmente provenientes de organismos del gobierno ucraniano y de la Unión Europea[1] (como el SSSCIP o el CERT-EU), con datos específicos sobre la ciberguerra –especialmente en cuanto a cantidad, tendencias y tipos de ciberataques a partir del inicio del conflicto bélico.

Se recabaron noticias y artículos de distintos medios y fuentes periodísticas (como Reuters y Wired) y especializadas en la materia (como The Cyber Express y otros), que aportan información sobre ciberataques puntuales, así como análisis más complejos sobre sus implicancias en ciberseguridad, aspectos técnicos e impactos materiales. A partir de estas fuentes, así como de un examen integral de los actores involucrados, sus acciones, los hechos y sus repercusiones durante el periodo analizado, se establecieron las conclusiones explayadas en el presente informe.

[1]Aunque se trata en general de informes que aportan datos específicos sobre los ciberataques, debe tenerse en cuenta que sus interpretaciones y conclusiones pueden estar sesgadas, especialmente debido al involucramiento de las partes en el conflicto. En este sentido, se ha intentado matizar las mismas con el uso de otras fuentes, con el fin de mantener la rigurosidad del informe.

La ciberguerra y su contexto: un acercamiento conceptual

Antes de analizar la ciberguerra en el conflicto ruso-ucraniano, es necesario realizar una aproximación a distintos conceptos y marcos que serán centrales para comprender en detalle la complejidad de este fenómeno. Para ello se delimitará, por un lado, el concepto mismo de ciberguerra, así como el marco en el que esta se desenvuelve. Por otro lado, se explicará la importancia de la IICC y la relevancia que conllevan los ciberataques en su contra.

El Contexto: Guerra Híbrida, Ciberespacio y Ciberguerra

Para comprender la importancia de los ciberataques en el contexto del conflicto europeo, es necesario primero situarlos dentro del marco más amplio de transformación de la guerra y de los nuevos escenarios en los que esta se desarrolla. Un concepto que ha intentado captar estos cambios experimentados en los últimos años ha sido el de *Guerra Híbrida* (GH). Según Joseph S. Nye (2015), la GH implica un tipo de conflicto aún más descentralizado, en términos de los distintos frentes donde se focalizan las tensiones –cada vez más alejado de los tradicionales enfrentamientos entre ejércitos convencionales de los Estados-Nación–. En este tipo de guerra, se difuminan las fronteras entre el ámbito militar y el civil, donde el rival central pasa a ser la *sociedad enemiga* –utilizando todos los medios posibles para destruir su voluntad política–, y adquieren un mayor protagonismo los actores no-estatales en el conflicto (Merino Gabriel, 2024).

Además, Frank Hoffman (2007) complementa esta descripción enfatizando dos rasgos de la GH. Por un lado, su *multi-nodalidad*, o sea, la conducción de la guerra tanto por Estados como por otros actores, actuando directa y coordinadamente en términos operacionales y tácticos dentro del mismo marco bélico, apuntando en este sentido a provocar efectos físicos y psicológicos. Por otro lado, su *multi-modalidad*, siendo que los actores involucrados utilizan una amplia gama de tácticas de guerra, incluyendo acciones militares convencionales, tácticas irregulares, formas terroristas o criminales.

Otro término central para comprender el escenario en que se producen los ciberataques es el de *ciberespacio*, entendido como: el *ecosistema virtual*, derivado de la interacción entre usuarios, software y servicios de internet a través de dispositivos y redes en conexión, sostenido a su vez sobre una *red material e interdependiente*, compuesta de infraestructuras de las TICs, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados en industrias críticas (Sein, 2022).

Para comprender el ciberespacio es esencial, en este sentido, entender la dualidad interconectada entre el ecosistema virtual, habitado por diversos actores, y las indispensables bases e infraestructuras materiales que posibilitan la existencia de este ambiente digital. Así mismo, es esta la arena donde cobran relevancia fenómenos como la ciberseguridad, los ciberataques, la ciberdefensa y, especialmente, la ciberguerra.

Con los conceptos previos como marco, se procederá a analizar el fenómeno de la *ciberguerra*, cuya originalidad recae esencialmente en los medios utilizados para hacer la guerra y el ambiente donde se desenvuelve. Una definición preliminar podría establecer que se trata de "la utilización de todas las herramientas electrónicas e informáticas para derrumbar los sistemas electrónicos y de comunicación del enemigo y mantener operativos los propios" (Sánchez Medero, 2012, p.125). Es decir, la intrusión de la guerra en el ciberespacio. Sin embargo, como modalidad bélica que refleja las transformaciones propias de la GH, la ciberguerra presenta dinámicas aún más complejas y difusas, que no siempre resultan evidentes a simple vista. En primer lugar, la ciberguerra configura un esfuerzo bélico donde, a la par del rol protagónico de actores militares y del Estado, también participan actores no militares y no estatales: grupos de *hackers*, *hacktivistas* civiles, empresas de seguridad, grupos terroristas, organizaciones criminales, etc. Todos pueden participar activa o pasivamente del conflicto, y sus vínculos con los Estados en combate no siempre son claros.

En segundo lugar, el fenómeno de la *ciberguerra*, a pesar de incluir la palabra guerra en el término, difumina parcialmente las fronteras que dividen países beligerantes de no beligerantes y permite ataques a Estados en contextos pacíficos. Esto significa que, debido a la complejidad y la relativa anonimidad del ciberespacioque ofrece para facilidades para negar responsabilidades, los ataques encarados en este ecosistema pueden producirse sin necesariamente existir un contexto de guerra en el sentido tradicional de la palabra. Los ciberataques realizados contra Estonia en el 2007[2] –probablemente el primer ataque cibernético a gran escala contra un Estado, presumiblemente

[2]Se trató de un ataque DDoS que inhabilitó a escala nacional sitios web del gobierno, bancos, medios de comunicaciones y otras organizaciones estonias, en el marco de disturbios tras el retiro de un monumento de la era soviética. Aunque Estonia y países de la OTAN atribuyen responsabilidad del ataque a Rusia, el país ha negado su involucramiento en el hecho (Traynor, 2007).

Por último, se trata de una forma de guerra que puede adoptar modalidades y objetivos diversos, aunque no excluyentes entre sí. Un tipo de modalidad puede involucrar el aspecto comunicativo y propagandístico, por ejemplo, con el uso de bots, noticias falsas y otras tácticas para consolidar el apoyo bélico doméstico y contrarrestar el de la *sociedad enemiga*. Otra modalidad puede combinar aspectos de ciberinteligencia, con la meta de recabar información sensible y llevar adelante acciones de espionaje, por ejemplo, a través del uso de *spyware*. Por último, existe una modalidad aún más destructiva que será de especial interés para los fines del presente informe, y que implica el uso de tácticas de ciberataque para sabotear e impedir el funcionamiento de las IICC de un país.

Los Ciberataques a Infraestructura Crítica

Para la Cybersecurity and Infrastructure Security Agency (CISA) de EE.UU., el término de IICC hace referencia a todos aquellas redes o sistemas, físicos o digitales, cuya centralidad implique que su incapacitación o destrucción podría tener efectos serios en la seguridad nacional, la economía, la salud pública o en varias a la vez (CISA, s.f.). Diversos sectores entran en esta categoría[4]: servicios básicos –tendido eléctrico, agua, gas–, telecomunicaciones, burocracia, sistemas industriales, sistemas sanitarios, transporte, defensa, energía, entre otros.

Como destaca Sol González (2022), diversas cuestiones resaltan la importancia de la IICC para un país. Por un lado, el ataque a uno de estos sectores suele tener impactos que afectan a otros ámbitos de la sociedad; por ejemplo, la interrupción del servicio eléctrico y bancario por un ciberataque puede tener repercusiones, no solo en la población civil, sino también en otros sectores críticos, como sistemas industriales y empresas, multiplicando consecuencias.

Por otro lado, la progresiva digitalización e interconexión de estos sectores en el ciberespacio no solo los vuelve más vulnerables a ciberataques, sino que también torna más imprevisible su alcance potencial considerando el aspecto global y transnacional del ámbito digital. En este sentido, Ucrania probablemente sea uno de los países que más experiencia ha tenido como blanco de sucesivos ciberataques, especialmente desde la década pasada, enmarcados en el aumento de las tensiones con Rusia desde el 2014 y la anexión de Crimea.

Resulta complejo identificar un evento que pueda representar el punto de inicio del enfrentamiento cibernético; en realidad, puede hablarse de un

[4]La CISA destaca 16 sectores críticos para la seguridad nacional, aunque la infraestructura y los sectores relevantes pueden variar según el país.

proceso complejo y difuso de escalada de las tensiones. Aunque no todos los ciberataques previos tuvieron el mismo impacto, si existen antecedentes relevantes que pueden ser contrastados con el inicio de la guerra en 2022. Sin embargo, es necesario aclarar que, dada la naturaleza de los ciberataques, no siempre puede trazarse claramente el involucramiento de ambos Estados en estos actos.

Tensión y guerra cibernética: el caso de Rusia y Ucrania

Tensiones Rusia-Ucrania hacia el 2022 y ciberataques sobre IICC

Como punto de inicio se tomarán los hechos desencadenados por el Euromaidán en el 2013 y la anexión de Crimea, destacando inicialmente la Operación Armagedón: una campaña de ciberespionaje dirigida contra el gobierno ucraniano, fuerzas de seguridad y fuerzas armadas. Aunque no se trató de un ataque a IICC, las reflexiones de Jason Lewis (jefe de inteligencia de Lookingglass, firma que analizó esta campaña) planteaban que: "el componente cibernético de la guerra cinética[5] parece ser un método exitoso para labores de reconocimiento" (Prince, 2015). Sin embargo, los posteriores ciberataques irían mutando en su diversidad y potencial destructivo.

Un hecho central a resaltar en la escalada de tensiones cibernética sería ciertamente el ciberataque BlackEnergy que, a fines del 2015, tuvo por blanco subestaciones y centros de distribución de energía, interrumpiendo el suministro energético por varias horas en parte de la región ucraniana de Ivano-Frankivsk y dejando secuelas en la infraestructura. A su vez este ataque, a diferencia de la Operación Armagedón, sería mucho más sofisticado en su aspecto técnico, logístico y de planificación, calificado por Kim Zetter (2016) como el primer ciberataque confirmado capaz de inutilizar una red de distribución energética. A partir de entonces, la sofisticación de los ciberataques iría en aumento.

En 2016 un nuevo ciberataque[6] al suministro eléctrico –esta vez en parte de la

[5] Aunque el eufemismo de "guerra cinética" no está librado de polémica en su uso e implicancias, se lo retoma en este informe solo para contrastar entre las tácticas bélicas "cinéticas" – vinculadas a la guerra convencional y uso de potencia de fuego en el campo de batalla – y las tácticas "cibernéticas" – ligadas a los rasgos mencionados en nuestra definición de "ciberguerra" realizada al inicio del trabajo.

zona de Kiev– de características similares y repercusiones menores, pero de mayor complejidad en su técnica y ejecución, comenzó a plantear diversas cuestiones. Por un lado, el aumento de los ataques informáticos a instituciones gubernamentales durante ese año[7] escaló al punto que el ex-presidente ucraniano Petro Poroshenko declaró la existencia de una *ciberguerra* en progreso por parte de Rusia (Zinets, 2016). Por otro lado, tal como destaca Kim Zetter (2017), la cantidad y complejidad de los ataques comenzaban a apuntalar la posibilidad de que el país se hubiera transformado, para ciertos grupos o individuos, en una arena de experimentación para "refinar ataques a infraestructura crítica que pudieran ser utilizados alrededor del mundo".

El último hecho a destacar del periodo, y de los más destructivos hasta la fecha, es el ciberataque *Not-Petya* del 2017. La complejidad y alcance de este último superó por mucho a los anteriores, marcando un antes y un después en el mundo de la ciberseguridad. Se calcula que al menos un 10% de las computadoras de Ucrania se vieron afectadas (AP News, 2017), prácticamente todas vinculadas a empresas ucranianas, dado que el hackeo aprovechaba una vulnerabilidad del programa MeDoc, utilizado con fines tributarios por el 80% de las compañías del país. Además, la información almacenada en estos dispositivos quedó inutilizable – siendo que, a pesar de presentarse como un ataque *ransomware*, sus fines eran en realidad destructivos. Domésticamente los impactos fueron contundentes: paralización, por al menos 24 horas, de sectores bancarios, comerciales, financieros, de transporte, logístico, entre otros. Sin embargo, su alcance no se detuvo en las fronteras nacionales, viéndose afectados también empresas y dispositivos de otros países europeos y de EE.UU. –inclusive de Rusia–, con pérdidas valoradas en cientos de millones de dólares. Esto último causado principalmente por la naturaleza auto-reproducible del *malware* y la interconexión entre las empresas ucranianas con las de otros países, volviendo prácticamente incontrolable la expansión del radio de acción del ataque. Se calcula que los costos mundiales ocasionados por este ataque fueron de 10 mil millones de dólares (Greenberg, 2018).

Hubo otros eventos similares de mayores y menores repercusiones: tanto nuevos ataques posteriores al 2017[8] como ataques llevados a cabo por actores ucranianos[9] contra Rusia o de actores pro-rusos de las regiones de Donetsk, Lugansk y Crimea. Aunque esta cronología no pretende ser exhaustiva en términos de ciberataques a IICC, estos casos permiten vislumbrar la evolución de las tensiones cibernéticas en este marco conflictivo. En primer lugar, se puede observar claros avances en la complejidad de los ataques, su logística y aspectos técnicos. En segundo lugar, vinculado a la cuestión

[6] Bautizado por algunos expertos como Industroyer, nombre del potencial malware involucrado en este hecho (Cherepanov, 2017).
[7] Según Ucrania se habrían registrado, al menos, 6.500 ciberataques en los últimos meses del 2016 contra instituciones gubernamentales ucranianas, entre ellas, al Tesoro y Ministerio de Finanzas, impidiendo temporalmente pagos de haberes y transferencias.

anterior, se trata de ataques difícilmente atribuibles a Estados. Sin embargo, dada la magnitud y complejidad de los mismo, los objetivos seleccionados, las metas aspiradas y la profesionalidad y recursos requeridos por las operaciones, llevan a considerar en ciertos casos –como el ataque *Not-Petya*– que se trata de actores no-estatales vinculados y/o financiados por Estados y organismos de inteligencia o militares[10], llamados en el ámbito de la ciberseguridad como *Advanced Persistent Threat* (APT)[11]. A pesar de esto, es necesario tener en cuenta que no todos los ciberataques son llevados a cabo por APTs, también han involucrado grupos criminales, *hacktivistas* e individuos no necesariamente vinculados a Estados. Por último, se puede destacar que, aunque varios de estos ciberataques parecían tener alcances y objetivos principalmente de carácter simbólico, psicológico o incluso experimental –como en el caso de los cortes energéticos del 2015 y 2016–, no puede subestimarse el potencial destructivo que puede tener el conflicto en el ciberespacio, tanto en sus impactos materiales como de trascendencia internacional.

El inicio del conflicto: La ciberguerra desencadenada

Aunque el 24 de febrero del 2022 inició con una invasión militar en el sentido más tradicional del término, la artillería cibernética ya operaba silenciosamente en el ciberespacio en los momentos previos y durante las primeras operaciones militares. En enero de 2022, se presentó el ataque *WhisperGate*, dirigido contra organizaciones e instituciones gubernamentales ucranianas, guardando algunas similitudes con el ataque *Not-Petya* en sus aspectos técnicos (Microsoft, 2022). Otro ciberataque, que acompañaría las operaciones militares de 24 de febrero y e inauguraría definitivamente la conflagración cibernética entre ambos Estados, fue *HermeticWiper* que tuvo fines destructivos[12] (WeLiveSecurity, 2022). En esa misma semana, Mykhailo Federov[13] anunció la creación de la IT Army of Ukraine[14] (Pearson James, 2022). Estos acontecimientos, que parecen de escasa relevancia aparente, son muestras de un proceso macerado por años de experiencia, prueba y error en ciberataques y ciberdefensa, ganando una nueva intensidad, tanto en volumen como en sofisticación, desde el inicio de la guerra.

[9]Véase, por ejemplo, los ataques de *spearpishing* contra entidades gubernamentales ucranianas en el 2021 (Gutierrez Fred y Saengphaibul Val, 2021) y otros campañas similares realizados durante la pandemia de COVID-19 (Bellingcat Investigation Team, 2022).
[9]Véase la Operación *Groundbait* o las filtraciones de Surkov, por mencionar algunos casos.
[10]En el caso de *Not-Petya* y otros ataques a IICC contra Ucrania, suele apuntarse al grupo Sandworm, vinculado a la unidad militar 74455 de la agencia militar de inteligencia rusa GRU (Mitre Attack, s.f.).
[11]Se trata de ciberataques de largo plazo y complejos llevados a cabo por expertos, usualmente apoyados por Estados u organizaciones cibercriminales, con objetivos de alto valor y metas particulares: espionaje, robo de información, sabotaje o acceso y presencia sigilosa en ciertas redes para obtener ventajas estratégicas (Paloalto Networks, s.f.)-
[12]Tanto *WhiperGate* como *HermeticWiper* fueron ciberataques dirigidos contra organizaciones ucranianas, bajo el objetivo de destruir información y volver inoperables los dispositivos comprometidos.
[13]Funcionario en el Ministerio de Transformación Digital de Ucrania.
[14]Ejército cibernético de voluntarios pro-ucranianos, con foco en operaciones ciberofensivas contra Rusia.

Solo un mes después del comienzo de la invasión, tanto Rusia como Ucrania vieron un aumento como receptores de ciberataques en un 10% y 17% respectivamente. Este incremento también se corroboró en países de la OTAN y en otras regiones del mundo, aunque con matices (Check Point Research Team, 2022). También el Computer Emergency Response Team - EU (CERT-EU, 2023, p.5) remarcó un pico brusco en los ciberataques rusos a fines de febrero y durante marzo, seguido de una actividad menor pero constante a lo largo del resto de 2022. A su vez, entre los sectores más destacados como blancos de los ciberataques estaban: los organismos gubernamentales, defensa, telecomunicaciones, sociedad civil y el sector energético (CERT-EU, 2023; State Service of Special Communication and Information Protection of Ukraine [SSSCIP], 2022).

Observando el panorama general, desde el 2022 hasta la actualidad, la cantidad de incidentes cibernéticos registrados por el CERT-UA (SSSCIP, 2022, 2024a, 2025a) han ido en aumento constante, contando 2.100 en el 2022, 2.543 en el 2023 y 4.315 en el 2024 –un aumento de aproximadamente 105% entre los ataques registrados durante el primer año de la guerra y aquellos del 2024.

La evolución del conflicto: los ciberataques a partir del 2023

Una mirada más profunda sobre los ciberataques desde el 2023 revela detalles interesantes respecto a la evolución de la ciberguerra en el marco de este conflicto. En este sentido, los sucesivos informes sobre amenazas cibernéticas rusas realizados por el SSSCIP (2023, 2024b, 2024c, 2025b) permiten identificar varios patrones.

En primer lugar, las acciones llevadas a cabo por APTs pro-rusos se centran en el ciberespionaje y en la recolección de información sensible de ciudadanos, como bases de datos sanitarios. A esto se le suman ataques a medios ucranianos y proveedores de telecomunicaciones, acciones para intentar acceder a instalaciones vinculadas al suministro de servicios básicos[15] (energía, agua y gas), ataques a organismos gubernamentales y sectores de defensa, entre otros casos.

En segundo lugar, un foco de especial atención parecen ser los intentos de infiltración en eslabones diversos del sector energético –objetivo histórico por excelencia de estos actores–, lo cual ha sido fuente de innovaciones en tácticas ciberofensivas, complejizando aún más sus métodos[16] y prolongando su accionar.

[15]Véase los intentos de intrusión maliciosa del APT Sandworm a 20 instalaciones vinculadas a suministro de servicios críticos en el 2024 (Computer Emergency Response Team - UA [CERT-UA], 2024)
[16]Por ejemplo, frente a un robustecimiento de la ciberdefensa en sectores de energía ucranianos –dado los precedentes históricos de ataques al mismo–, nuevos métodos ciberofensivos apuntan ahora a eslabones más débiles de las cadenas de suministros (Mihir, 2025).

En tercer lugar, destaca la integración de la ciberguerra a la par de las acciones militares en el terreno. En este sentido, y como resalta Mihir Bagwe (2025), pareciera haber un patrón cada vez más presente de coordinación entre guerra cinética y cibernética, es el caso de los ataques informáticos al proveedor de telecomunicaciones Kyivstar, por un lado, y del lanzamiento de misiles a la zona de Kyiv, por otro, llevados a cabo de forma casi simultánea en diciembre del 2023, intensificando así los efectos materiales y psicológicos de la disrupción (SSSCIP, 2024b, p.18).

En cuarto lugar, el último informe del SSSCIP (2025, p.5) remarca que el aumento de los incidentes cibernéticos ha ido acompañado de una disminución drástica de los casos críticos y graves de ciberataques. Sin embargo, Mihir Bagwe (2025) parece cuestionar que esto se deba necesariamente a mejores capacidades de ciberdefensa, planteando que también podría tratarse de mejores –y más sigilosos– métodos ciberofensivos para ocultar el código malicioso. Por último, se hace necesario destacar uno de los principales ciberataques a IICC, en términos de repercusión, que haya sufrido Ucrania desde el inicio del conflicto. Se trata del sabotaje del Registro del Ministerio de Justicia a fines del 2024, con efectos disruptivos en varios sectores de la administración pública y la economía (SSSCIP, 2025, p.13), paralizando operativamente el área de migraciones, registro civil, aduana y procesos judiciales.

También se han registrado ataques recientes a IICC[17] en Ucrania, así como ofensivas de APTs ucranianos a objetivos rusos[18], aunque sus repercusiones por ahora poco han modificado el panorama retratado previamente.

[17]Véase, por ejemplo, los ciberataques a la empresa ferroviaria ucraniana de Ukrzaliznytsia en marzo del 2025 (Cadena SER, 2025, 24 de marzo)
[18]Véase los ciberataques al proveedor de internet ruso Nodex (Ciberseguridad LATAM, 2025) o a empresas contratistas de la energética Gazprom (Infobae, 2025)

Conclusiones: un laboratorio bélico digital y no tan digital

El ciberespacio ha ido transformándose, y el campo de batalla junto con él. Si se ha reflotado el concepto de GH para hablar de la ciberguerra como una modalidad clave de esta, es porque se aprecia que la lucha en el ciberespacio constituye un eje motorizador de diversos cambios en la guerra. Esto se refleja no solo en sus nuevas tácticas –queda claro el uso bélico de los ciberataques–, sino también en su alcance y naturaleza: la difuminación entre beligerantes y no beligerantes, entre Fuerzas Armadas y sociedad civil, entre momentos de paz y de guerra. Frente a esto, se considera que los ciberataques intercambiados entre Rusia y Ucrania antes y después del 2022, especialmente aquellos apuntados a la IICC –estrechamente vinculados a la meta última de la GH, que es el ataque a la "sociedad enemiga"–, han sido terreno fértil para el desarrollo de estos fenómenos.

Por un lado, se corroboró que el aumento de las tensiones hacia el 2022, así como su traducción en ciberataques sucesivos y cada vez más complejos a IICC ucraniana, ha implicado: ataques más sofisticados, agudización de sus impactos psicológicos (sobre población civil especialmente) y materiales (apuntando a paralizar sectores de la economía), un mayor involucramiento de actores no estatales (APTs, grupos hacktivistas, crimen organizado, etc.) y un estrechamiento de vínculos entre estos y los Estados-Nación implicados.

Por otro lado, con estos antecedentes en mente, también se observó cómo esta tendencia se ha profundizado a partir del inicio de la guerra en el 2022. En este marco los ciberataques han aumentado en volumen, tanto entre los beligerantes como hacia países no beligerantes pero inclinados geopolíticamente por uno u otro bando (como aquellos que componen la UE o la OTAN). A su vez, las operaciones cibernéticas se han vuelto aún más sofisticadas en sus técnicas, sus metas y su planificación y ejecución. En paralelo, los vínculos entre APTs y los Estados beligerantes parecen haberse estrechado aún más, muchas veces integrando y coordinando ataques militares cibernéticos y cinéticos de forma conjunta como parte de una misma táctica bélica, con tintes mucho más destructivos.

Algo cambió y está cambiando en las formas de la guerra, incluida su faceta cibernética, y el conflicto ruso-ucraniano parece por momentos ser el ojo de

la tormenta de estas transformaciones. En este sentido, y retomando las palabras de José Pardo de Santayana (2024), pareciera que esta arena se transformó en "el laboratorio en el que se está poniendo las bases para la próxima forma de guerra" (p.94). Queda pendiente ver en qué dirección realmente avanzarán estas transformaciones, qué profundidad tendrán exactamente los cambios que parecen imprimirse en el ámbito bélico y qué medidas preparatorias tomarán los principales actores del sistema internacional al respecto para aminorar sus riesgos potenciales.

Referencias

AP News. (2017, 6 de julio). *Ucrania estima que el ciberataque afectó al 10% de las PC*. https://apnews.com/general-news-domestic-news-domestic-news-6015377f3e644b27911e3d4bdf13396f

Bagwe, M. (2025, 30 de abril). *Ukraine Reports 48% Jump in Cyber Incidents in H2 2024, but 77% Drop in High-Severity Incidents*. The Cyber Express. https://thecyberexpress.com/cyber-incidents-in-h2-2024-ukraine/

Bellingcat Investigation Team. (23 de febrero de 2021). *Attack on Ukrainian Government Websites Linked to GRU Hackers.* Bellingcat. https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers

Cadena SER. (2025, 24 de marzo). *Las líneas de trenes de Ucrania informan de que sufren un ciberataque a gran escala*. https://cadenaser.com/nacional/2025/03/24/las-lineas-de-trenes-de-ucrania-informan-de-que-sufren-un-ciberataque-a-gran-escala-cadena-ser/

Check Point Research Team. (28 de marzo de 2022). *Resurgence of Increased Cyber Attacks on both Russia and Ukraine, a month into the war*. Check Point. https://blog.checkpoint.com/security/resurgence-of-increased-cyber-attacks-on-both-russia-and-ukraine-a-month-into-the-war/

Cherepanov, A. (2017, 12 de junio). *Industroyer: la mayor amenaza para sistemas de control industrial desde Stuxnet*. We Live Security. https://www.welivesecurity.com/la-es/2017/06/12/industroyer-amenaza-control-industrial/

Ciberseguridad LATAM. (2025, 10 de enero). *Proveedor de servicios de Internet ruso, confirmó que piratas informáticos ucranianos «destruyeron» su red*. https://ciberseguridadlatam.com/proveedor-de-servicios-de-internet-ruso-confirmo-que-piratas-informaticos-ucranianos-destruyeron-su-red/

Computer Emergency Response Team - EU. (2023). *Russia's War of Ukraine: one year of cyber operations*. https://cert.europa.eu/static/threat-intelligence/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf

Computer Emergency Response Team - UA. (19 de abril de 2024). *UAC-0133 (Sandworm) plans for cybersabotage at almost 20 critical infrastructure facilities in Ukraine*. https://cert.gov.ua/article/6278706

Cybersecurity and Infrastructure Security Agency [CISA]. (s.f.). *Critical Infrastructure Sectors*. recuperado el 04 de mayo de 2025. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

González, S. (2022, 10 de marzo). *Ciberataques a la infraestructura crítica de un país y sus consecuencias*. We Live Security. https://www.welivesecurity.com/la-es/2022/03/10/ciberataques-infraestructura-critica-pais-consecuencias/

Greenberg, A. (2018, 22 de agosto). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Gutierrez, F. y Saengphaibul, V. (3 de mayo de 2021). *Spearphishing Attack Uses COVID-21 Lure to Target Ukrainian Government*. Fortinet. https://www.fortinet.com/blog/threat-research/spearphishing-attack-uses-covid-21-lure-to-target-ukrainian-government

Hoffman, F. (2007). *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict*. Strategic Forum, 240, 1-8. https://www.files.ethz.ch/isn/98862/SF240.pdf

Infobae. (2025, 12 de febrero). *'Hackers' ucranianos atacan los sistemas informáticos de empresas energéticas rusas*. https://www.infobae.com/america/agencias/2025/02/12/hackers-ucranianos-atacan-los-sistemas-informaticos-de-empresas-energeticas-rusas/

Merino, G. (2024). *Transición de Poder Mundial y Guerra Mundial Híbrida. Principales focos y frentes de un conflicto mundial y las relaciones entre Estados Unidos, China y América Latina*. Revista Estado y Políticas Públicas, 23, 31-56. https://revistaeypp.flacso.org.ar/files/revistas/1730418327_31-56.pdf

Microsoft. (15 de enero de 2022). *Destructive malware targeting Ukrainian organizations*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

Mitre Attack. (s.f.). *Sandworm Team*. Recuperado el 04 de mayo de 2025. https://attack.mitre.org/groups/G0034/

Nye, J. (2015, 5 de febrero). *The Future of Force*. Project Syndicate. https://www.project-syndicate.org/commentary/modern-warfare-defense-planning-by-joseph-s--nye-2015-02

Paloalto Networks. (s.f.). *What Is an Advanced Persistent Threat?*. Recuperado el 04 de mayo de 2025. https://www.paloaltonetworks.com/cyberpedia/what-is-advanced-persistent-threat-apt

Pardo de Santayana, J. (2024). *La inteligencia artificial y la guerra de Ucrania*. Instituto Español de Estudios Estratégicos, 226, 87-104. https://www.defensa.gob.es/ceseden/-/cuaderno-de-estrategia-226

Pearson, J. (2022, 26 de febrero). *Ukraine launches 'IT army,' takes aim at Russian cyberspace*. Reuters. https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/

Prince, B. (2015, 28 de abril). *'Operation Armageddon' Cyber Espionage Campaign Aimed at Ukraine: Lookingglass*. Security Week. https://www.securityweek.com/operation-armageddon-cyber-espionage-campaign-aimed-ukraine-lookingglass/

Sánchez Medero, G. (2012). *La ciberguerra: los casos de Stuxnet y Anonymous*. Revista Internacional de Derecho de la Comunicación y las Nuevas Tecnología, 11, 124-133. https://dialnet.unirioja.es/ejemplar/336106

Sein, C. (2022). *Glosario de Ciberseguridad N°1*. Centro de Estudios Estratégicos de Relaciones Internacionales. https://www.ceeriglobal.org/wp-content/uploads/2022/07/Glosario-de-ciberseguridad-N%C2%B01.pdf

State Service of Special Communication and Information Protection of Ukraine [SSSCIP]. (2022, 30 de diciembre). *CERT-UA has processed over 2,000 cyberattacks against Ukraine year to date*. https://cip.gov.ua/en/news/cert-ua-vid-pochatku-roku-opracyuvala-bilshe-dvokh-tisyach-kiberatak-na-ukrayinu

State Service of Special Communication and Information Protection of Ukraine [SSSCIP]. (2023). *Russia's Cyber Tactics H1'2023*. https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=60068&embedded=true&a=bi

State Service of Special Communication and Information Protection of Ukraine [SSSCIP]. (2024a, 8 de febrero). *The CERT-UA Team has processed 2,543 cyber incidents over 2023*. https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti

State Service of Special Communication and Information Protection of Ukraine [SSSCIP]. (2024b). *Russian Cyber Operations: APT Activity Report #3 H2 2023*. https://docs.google.com/viewerng/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id%3D64622&a=bi

State Service of Special Communication and Information Protection of Ukraine [SSSCIP]. (2024c). *Russian Cyber Operations: APT Activity Report H1 2024*. https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=65898&embedded=true&a=bi

State Service of Special Communication and Information Protection of Ukraine [SSSCIP]. (2025a, 8 de enero). *CERT-UA recorded 4,315 cyber incidents in 2024*. https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

State Service of Special Communication and Information Protection of Ukraine [SSSCIP]. (2025b). *Russian Cyber Operations: Analytics for the H2 2024* https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=68753&embedded=true&a=bi

Traynor, I. (2007, 17 de mayo). *Russia accused of unleashing cyberwar to disable Estonia*. The Guardian. https://www.theguardian.com/world/2007/may/17/topstories3.russia

WeLiveSecurity. (2022, 24 de febrero). *HermeticWiper: Nuevo malware que borra datos ataca a Ucrania*. https://www.welivesecurity.com/la-es/2022/02/24/hermeticwiper-nuevo-malware-tipo-wiper-ataca-ucrania/

Zetter, K. (2016, 3 de marzo). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.* Wired. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zetter, K. (2017, 10 de enero). *The Ukrainian Power Grid Was Hacked Again*. Vice. https://www.vice.com/en/article/ukrainian-power-station-hacking-december-2016-report/

Zinets, N. (2016, 29 de diciembre). *Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'*. Reuters. https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC/

CEERI
Centro de Estudios Estratégicos
de Relaciones Internacionales

NUESTRAS REDES SOCIALES

@CEERI.GLOBAL @CEERI.GLOBAL @CEERI_GLOBAL

CENTRO DE ESTUDIOS ESTRATÉGICOS
DE RELACIONES INTERNACIONALES (CEERI)