ACADEMIA DE LAS CIENCIAS
Y LAS ARTES MILITARES

Comunicaciones académicas

El horizonte de las operaciones en el ciberespacio tras la guerra de Ucrania

Manuel Esteve Domingo
Academia de las Ciencias y las Artes Militares
Sección de Futuro de las Operaciones Militares

20 de enero de 2024

Introducción

La historia demuestra que, en la mayoría de las ocasiones, los países y sus ejércitos se preparan para la guerra «anterior». Sin duda, el ejemplo más conocido sería el de Francia, en el periodo entre las dos guerras mundiales, y su impresionante sistema defensivo conocido como Línea Maginot. Tras la experiencia de la guerra de trincheras en la conocida en su momento como «Gran Guerra», Francia se preparó para un tipo de guerra similar, con posiciones estáticas por uno y otro bando. Los estrategas franceses no tuvieron en cuenta las innovaciones técnicas como la aviación, las unidades de blindados o las comunicaciones por radio que facilitaban el mando y control de ejércitos completos que basaban sus operaciones en la maniobra.

En febrero de 2014 Rusia se anexionó Crimea, territorio soberano de Ucrania hasta esa fecha. Poco después, en abril de 2014, empezó la conocida como Guerra del Dombas, por el dominio de esta región entre Ucrania y los elementos prorrusos con apoyo más o menos evidente de Rusia.

Con estos dos hitos, antecedentes inmediatos de la actual guerra en Ucrania, comienza una nueva era en las operaciones militares, conocida con Guerra Híbrida. En este tipo de guerra, un país o un grupo independentista apoyado por un país, utiliza todos los medios a su alcance, militares y no militares, para conseguir sus objetivos estratégicos y operacionales.

Ligado al concepto de Guerra Híbrida, se desarrolla el concepto de Zona Gris, que podríamos definir como el periodo previo al enfrentamiento armado en el que se utilizan sobre todo operaciones en el ciberespacio y operaciones de influencia (muchas veces basadas en las propias operaciones en el ciberespacio) para producir efectos en el dominio cognitivo de la nación que es atacada, mediante acciones que tratan de deteriorar la economía, la confianza en los gobernantes y en definitiva alterar la vida de la sociedad atacada para ablandarla de cara a un ataque convencional.

Pues bien, en el caso de la guerra de Ucrania que comenzó en febrero de 2022, el país atacado, Ucrania, no sólo ha demostrado estar preparado para la siguiente guerra, si no que ha demostrado estar definiendo el camino de la guerra del futuro. Y particularmente en el campo de las operaciones en el ciberespacio.

Ucrania, en los 8 años que siguieron la anexión de Crimea y de parte del este del país por parte de Rusia, ha sabido aprender de las debilidades mostradas como nación en 2014. Pero no sólo eso, ha sabido aprender de las fortalezas mostradas por Rusia en esa fase antecedente del conflicto actual, para hacerlas suyas y devolver el golpe, sobre todo en el dominio objeto de este artículo, las operaciones en el ciberespacio con su correspondiente influencia en los dominios físicos y en el dominio cognitivo.

La guerra en el ciberespacio ya empezó en 2014

Si algo caracteriza la guerra híbrida, es la preeminencia de las operaciones en el ciberespacio como parte fundamental de la estrategia de desestabilización y debilitamiento de la nación atacada.

Por ello, está demostrado que Rusia basó gran parte de su ofensiva híbrida de 2014 en ciberataques sobre los sistemas de comunicaciones móviles y sobre la capacidad de acceso a internet de los ciudadanos ucranianos, llevando a la paralización de muchas actividades civiles en Ucrania, que sin duda penalizaron su capacidad de respuesta como nación. Ucrania tomó muy buena nota de este tipo de ataques, en principio no dirigido contra objetivos militares, pero que afectaron sobre todo al dominio cognitivo, como he indicado, dificultando muy grandemente la reacción nacional: nada de esto sucedió en 2022. Ucrania detectó como activo

estratégico y operacional fundamental, mantener la capacidad de acceso a las comunicaciones móviles y a internet, tanto por parte de las autoridades civiles y militares, como por el global de la ciudadanía.

Pero en el periodo de guerra híbrida, entre 2014 y 2022, ese largo conflicto en la zona gris mantenido entre Rusia y Ucrania durante 8 largos años, Ucrania ha sufrido por parte de Rusia innumerables ciberataques a lo que son el núcleo de la capacidad de funcionamiento de un país, las infraestructuras críticas. Particularmente, Ucrania sufrió varios ataques a los sistemas de distribución de energía eléctrica entre 2015 y 2016, y las infraestructuras de comunicaciones del sistema bancario en 2017. Este último ataque utilizando el ahora muy bien conocido *malware*, de tipo *ramsomware*, denominado *NotPetya*.

Tomando como fuente a SANS y al *Electricity Information Sharing and Analysis Center* (E-ISAC), vamos a centrarnos en el análisis de uno de estos ataques sufridos en 2015 a una infraestructura crítica tan importante como es la capacidad de distribución de energía eléctrica. Aparte del interés intrínseco del ataque como ejemplo de operación en el ciberespacio, con unos objetivos estratégicos muy bien definidos por parte de Rusia, nos interesa este ataque, muy bien estudiado y documentado, por las lecciones aprendidas que produjo que sin duda han influido mucho en que Ucrania haya mantenido en todo momento el dominio operacional en el ciberespacio en el conflicto actual desencadenado en 2022.

El 23 de diciembre de 2015, tres de las principales compañías de distribución de energía eléctrica de Ucrania sufrieron, con una diferencia de 30 minutos, una interrupción forzada del suministro de energía eléctrica a más 225.000 viviendas en

Ucrania. Nunca se había lanzado un ataque de estas características y con estos efectos, produciendo efectos sobre una cantidad tan grande de población civil. Sin embargo, no es el número de usuarios afectados lo que hace que este ataque sea tan significativo, aun siendo muy alto este número.

Lo que hace este ataque tan significativo es su complejidad y precisión. En el posterior análisis forense se demostró que el atacante había forzado las defensas de las compañías eléctricas al menos 6 meses antes introduciendo el *malware* que se activó en diciembre de 2015, como claro ejemplo de APT (*Advanced Persistent Threat*), y que permaneció indetectado durante todo ese tiempo.

Aunque realmente, más que de ataque deberíamos hablar de un conjunto de ataques coordinados y simultáneos que incluirían diversas técnicas como *spear phishing* para acceder a la información en las redes comerciales de las compañías, robo de credenciales, acceso a las VPN (*Virtual Private Networks*) de los sistemas de control de distribución por ataques de fuerza bruta, acciones de engaño introduciendo un *malware* conocido y poco peligroso, conocido como *Black Energy 3,* para hacer pensar que ese era el núcleo del ataque, el uso de un *software KillDisk* para borrar evidencias del ataque y todo ello combinado con un ataque de denegación de servicio al sistema de telefonía de los *call centers* de las empresas afectadas.

En definitiva, una completa operación en el ciberespacio con el objetivo de producir efectos tanto en el dominio físico como cognitivo, por la generación de la sensación de impotencia frente a la exposición posterior a este tipo de ataques por parte de la población civil.

Es bien conocido que la disuasión en el ciberespacio tiene unos fundamentos muy distintos que en los otros dominios. Precisamente, mostrar las capacidades demasiado pronto, producen en el adversario un efecto contrario al deseado: lo conminan a prepararse mejor para la siguiente cibercampaña.

Y esta es la principal lección que aprendió Ucrania como país durante los largos años de guerra híbrida, en la zona gris, antes de que empezara el conflicto abierto en 2022.

Ciberguerra en Ucrania

En la definición canónica de la gestión de incidentes de ciberseguridad, la primera fase siempre es la preparación. Un incidente de ciberseguridad a escala ciclópea, como es la ciberguerra, no debe tener un tratamiento distinto, y en particular, la

ciberguerra en Ucrania, si algo se ha caracterizado ha sido por la importancia que el país atacado ha dado a esta fase de la guerra.

Sin duda, las lecciones aprendidas del conflicto de 2014 y de los años de guerra híbrida han influido mucho. Ucrania se ha preparado como país y como sociedad para afrontar una guerra abierta multidominio que necesariamente, antes o después, tenía que llegar.

En el caso del dominio del ciberespacio, es hecho probado que Ucrania ha contado con el apoyo de los países occidentales para desarrollar sus capacidades de ciberdefensa desde 2015. Pero lo que hace más relevante este apoyo es que no ha sido solo un apoyo de gobiernos, sino, sobre todo, de empresas tecnológicas. Por supuesto ha sido posible por el buen criterio estratégico del gobierno de Ucrania y por la existencia de una ciudadanía ucraniana técnicamente desarrollada y muy evolucionada, sobre todo en estos últimos 8 años, capaz afrontar el reto de la digitalización como una preparación más, si no la más importante a tenor de los acontecimientos, para poder afrontar el inminente conflicto abierto.

Porque en un entorno de guerra multidominio, donde la superioridad en el dominio ciber es absolutamente necesaria para poder maniobrar e incluso obtener la superioridad en los otros dominios, una falta de preparación en este dominio, como en 2014, hubiera sido letal para Ucrania.

Cuatro meses antes del fatídico 24 de febrero de 2022 la ciberguerra ya había comenzado, antes por supuesto, de que empezarán las operaciones en los dominios físicos con la violación de fronteras y del espacio aéreo ucranianos.

En los cuatro meses anteriores al inicio del conflicto abierto, Ucrania sufrió más ciberataques que en los anteriores 8 años. Era el paso de la zona gris a la zona candente de conflicto, antes de que se disparara el primer misil o cayera la primera bomba en territorio ucraniano.

Y como consecuencia de las acciones desarrolladas en la fase de preparación para el conflicto, Ucrania consiguió mantener el acceso y la capacidad de movimiento en el ciberespacio.

Según análisis del Mando Conjunto de Ciberespacio, basado en el análisis de fuentes abiertas (OSINT, *Open Source Intelligence*), el gobierno y la población ucraniana ha mantenido incluso durante los peores momentos del conflicto una capacidad de acceso a Internet de al menos el 80% y la práctica disponibilidad de uso de la red de telefonía móvil, mientras ha habido capacidad de suministro eléctrico.

Estos dos servicios fueron objeto prioritario de ataque de Rusia en 2014 y en años posteriores. Gracias a conservar la capacidad de operación de estos dos servicios, se ha podido mantener cohesionada a la población, se han podido seguir prestando servicios esenciales como la gestión de emergencias y la seguridad y el orden público.

Pero no sólo eso. Además, ha posibilitado que la población civil, que en la guerra moderna sufre las penurias de la guerra de forma no muy distinta a como se sufre en el campo de batalla, se haya sentido parte de las capacidades de resistencia y respuesta mediante el uso de aplicaciones comerciales de sensorización y alerta temprana, por ejemplo, incrementando las capacidades de mando y control del ejército ucraniano.

Como cabía esperar, Rusia no ha permanecido tampoco inactiva en la lucha por el dominio operacional en el ciberespacio.

Desde hace muchos años, se da por hecho que detrás de algunas de las más famosas y letales APT está, como *sponsor* o como actor directo, el gobierno de Rusia a través del conocido en Occidente como *General Staff Main Intelligence Directorate*, o GRU por sus siglas en ruso, tomando como fuente a MITRE.

Las famosas y bien conocidas APT 28 y APT 29, proceden, sin lugar a dudas de este grupo de desarrollo. Algunas acciones famosas de estas APT tomaron como objetivo la campaña electoral de Hilary Clinton en 2016, la *World Anti-Doping Agency* (WADA), la *US Anti-Doping Agency*, la *Organization for the Prohibition of Chemical Weapons* (OPCW), el *Spiez Swiss Chemicals Laboratory* e incluso se les atribuye algún ataque no reconocido, por supuesto, a instalaciones nucleares de Estados Unidos. En abril de 2021, en plena pandemia por la COVID-19, se atribuye a la APT 29 el demoledor ataque a la empresa de ciberseguridad estadounidense *Solar Wind*, estrechamente ligada a la administración de Estados Unidos.

Tomando de nuevo como fuente a MITRE, el principal grupo APT que está participando en la guerra de Ucrania, sin duda actor directo de Rusia, es conocido como *Sandworm Team*. No se trata de un grupo nuevo o desconocido. Se le atribuye actividad al menos desde 2009. En 2020 la Inteligencia de Estados Unidos asoció a este grupo a seis oficiales del GRU Unit 74455 mediante técnicas de inteligencia de fuentes humanas (HUMINT).

Algunas acciones atribuidas a *Sandworm Team*, antes del comienzo del conflicto abierto con Ucrania, serían los propios ataques a las compañías de distribución de energía eléctrica ucranianas en 2015 y 2016, y los ataques al sistema financiero y a distintas empresas ucranianas con el *malware NonPetya* en 2017. Además, con el foco fuera de Ucrania, se le atribuyen ataques durante las campañas

presidenciales francesas de 2017, contra la organización de los juegos olímpicos de invierno de 2018 celebrados en China (sic), un nuevo ataque contra la *Organisation for the Prohibition of Chemical Weapons* en 2018, y diversos ataques contra la administración y empresas de Georgia durante 2018 y 2019.

Aunque, sin duda, junto con el ataque al sistema de distribución de energía eléctrica ucraniano de 2015 ya descrito, su ataque más significativo se desarrolló de nuevo contra esta infraestructura crítica tan relevante en 2016, incluyendo el desarrollo de un nuevo *malware* denominado *Industroyer*. Este malware es el primero (que se conozca) específicamente orientado a producir impacto en los sistemas de control industrial ICS de las subestaciones eléctricas que forman parte de los sistemas conocidos como *Smart Grid* para la distribución de energía eléctrica.

Otros grupos ligados al GRU cuya actividad ha sido identificada en la guerra de Ucrania, son *Iridium* o *Voodo Bear*.

En el conflicto ha entrado otro actor en un campo no menos importante como el «hacktivismo». Desde finales del mes de abril de 2022, tomando como fuente a la empresa S2 Grupo, se observó un nuevo grupo, de motivación hacktivista prorruso, denominado *Killnet*, cuyo principal objetivo fueron las webs de portales gubernamentales tanto de Polonia, República Checa, Rumanía, Reino Unido y Estados Unidos.

Hay que señalar que el hacktivismo opera en el dominio cognitivo, intentando crear estados de opinión, y atacando el objetivo principal en este dominio, la confianza, en este caso de la opinión pública de los países que más firmemente han apoyado a Ucrania. Las actividades de este nuevo grupo están siendo continuas durante toda la guerra.

Los organismos pertenecientes a la OTAN no han quedado tampoco libres de ciberataques por parte de grupos de nueva creación cuya atribución es prorrusa como las APT *Turla* y *Cyber Spetsnaz*.

Tomando como fuente a la empresa S2 Grupo, se han detectado ataques contra Ucrania y los países que apoyan su defensa en los siguientes sectores críticos: energético, sanitario, administración pública, financiero, alimentario, transporte, telecomunicaciones, industria, investigación y espacio exterior.

Hay que destacar los ataques a este último sector, el espacial, por el efecto cascada que ha producido, ya que buena parte de las operaciones del sector de emergencias, y también de forma no tan exclusiva del sector militar, se basan la utilización de sistemas de comunicaciones de banda ancha por satélite KA-SAT.

La principal empresa que proporciona servicio en este sector de las comunicaciones por satélite, Viasat, confirmó que sus módems satelitales habían sido ciberatacados con un nuevo tipo de *malware* denominado *Wiper AcidRain*, desarrollado ad-hoc para su uso en este conflicto.

La lista de ciberataques y de herramientas basadas en distintos tipos de *malware* que se han desarrollado y utilizado durante el conflicto de Ucrania es interminable, y entendemos que su enumeración está fuera del objeto de esta publicación.

Sin embargo, su sola mención hace muy evidente que las armas del futuro no van a ser solamente físicas, que en el dominio ciberespacial se desarrollan y utilizan sus propias armas, que cada vez permiten llevara a cabo operaciones multidominio más complejas y determinantes para el curso de la guerra.

El horizonte de las operaciones en el ciberespacio

Evidentemente, no existe a día de hoy información veraz y contrastable sobre los ciberataques que Ucrania debe sin duda estar sufriendo desde comienzos de 2022. Como indicábamos más arriba, la disuasión en el dominio ciber se basa en la prudencia en la comunicación sobre incidentes, aunque algún gobierno muy cercano no lo tenga tan claro.

Pero podemos hacer un análisis indirecto que nos permita obtener conclusiones razonables, extrapolables al futuro de las operaciones en el ciberespacio.

Si Rusia ha atacado el sistema de distribución de energía eléctrica de Ucrania sin estar en conflicto abierto, cruzando varias líneas rojas en lo que se refiere a ataques a infraestructuras críticas con afección a población civil, parece lógico pensar que estos ataques se habrán reduplicado durante el conflicto armado que comenzó el 24 de febrero de 2022.

Sin embargo, Rusia ha tenido que recurrir a ataques cinéticos, con armas convencionales, para interrumpir el suministro de energía eléctrica en amplias zonas de Ucrania, sin duda con un mayor coste económico que si hubiera tenido la capacidad de conseguir estos mismos efectos por medio de operaciones en el ciberespacio. Por no hablar del daño reputacional a la «causa rusa» que supone el uso de armas letales en zonas habitadas con posibles daños colaterales, que en cualquier caso favorece la superioridad de Ucrania en el dominio cognitivo.

Este análisis se puede aplicar a los ataques a otras infraestructuras críticas como sistemas de distribución agua, sistemas de telecomunicaciones o de transporte, que Rusia viene atacando mediante medios físicos desde el comienzo del conflicto,

sin duda por su incapacidad para atacarlos con medios ciber, gracias a las capacidades de ciberdefensa desarrolladas por Ucrania durante los últimos años, a raíz de los incidentes de 2014, y puestas en juego desde el comienzo del conflicto armado en 2022.

Lo que queda fuera de toda duda es que el dominio ciberespacial está siendo muy relevante en esta guerra y lo seguirá siendo en las guerras del futuro. La superioridad operacional en el ciberespacio posibilita la conducción de operaciones en otros dominios. La denegación de la libre operación en el ciberespacio imposibilita totalmente o dificulta hasta extremos nunca conocidos hasta ahora la operación en el resto de dominios.

Por tanto, el futuro de las operaciones militares, en base a las lecciones aprendidas de la guerra de Ucrania, se plantea claramente con carácter multidominio. Ni las operaciones sólo en los dominios físicos son determinantes, ni las operaciones solo en el dominio ciberespacial son suficientes para obtener la superioridad operacional.

Por otra parte, en la guerra de Ucrania se la revelado con especial impacto en las operaciones, la necesidad de dominar el espectro electromagnético. El espectro electromagnético pertenece al dominio físico. No es nada nuevo el concepto de guerra electrónica, *Electronic Warfare*, como se conoce internacionalmente. De hecho, sus conceptos básicos arrancan en la Segunda Guerra Mundial. Algunos de ellos como el *jamming*, o denegación de servicio de las comunicaciones del enemigo, sin perjudicar a las propias, se ha empleado en todas las guerras del siglo XX y XXI.

Nuevos conceptos como la denominada *Navegation Warfare*, cuyo objetivo es interferir las señales GPS del enemigo, son más recientes, pero igualmente efectivas con el objeto de anular la disponibilidad de las comunicaciones y de muchos sistemas de armas que dependen de la señal GPS.

Sin embargo, las acciones en el ámbito electromagnético inciden especialmente en el dominio ciberespacial, por su dependencia intrínseca de las comunicaciones.

Ucrania está aplicando la incipiente doctrina de OTAN, mucho más desarrollada previamente en Estados Unidos, en la que se define un nuevo concepto de operaciones, las operaciones CEMA (*Cyber Electromagnetic Activities*).

El concepto CEMA implica abordar de forma conjunta las más «tradicionales» actividades de guerra electrónica, las denominadas operaciones de gestión del espectro electromagnético (*Spectrum Management Operations*), con las más novedosas operaciones en el ciberespacio, por su relación intrínseca.

Posiblemente, en la guerra de Ucrania se están dando los primeros pasos prácticos de aplicación de este nuevo concepto CEMA, mostrándose claramente la relevancia del dominio ciberespacial y su interacción con los dominios físicos y cognitivo, en un paradigma bélico de operaciones multidominio.

Nota: Las ideas y opiniones contenidas en este documento son de responsabilidad del autor, sin que reflejen, necesariamente, el pensamiento de la Academia de las Ciencias y las Artes Militares.