Ucrania en busca de refugio digital

Raquel Jorge Ricart | Investigadora, Real Instituto Elcano | @RaquelJorgeR

En Ucrania está en juego la estabilidad del gobierno actual y del orden internacional, pero también la protección de su seguridad nacional y de las personas. En todo ello, el control sobre la infraestructura tecnológica –cuyos efectos ya permean en todos los aspectos la vida cotidiana– se presenta como un territorio poco explorado y que, sin embargo, tiene un papel esencial. De ahí, la importancia de analizar la capacidad de respuesta de Ucrania ante una posible toma de su infraestructura digital por parte de Rusia, así como los posibles escenarios más óptimos en los que Ucrania podría apoyarse para proteger los datos sensibles de su país, en especial en colaboración con terceros países.

Puede que no produzca una guerra en sí misma en muchos casos, pero sí añade cierta vulnerabilidad a aspectos tan vitales como la protección de infraestructuras críticas que están digitalizadas, como las redes eléctricas, los esquemas de ciberseguridad del sistema de comando y control (C2) militar, y el acceso al reconocimiento de imágenes precisas sobre el terreno con la ayuda de satélites para detectar movimientos de tropas, armamento y personas que buscan salir del país o aproximarse a zonas rurales.

Pero no es solamente algo de ámbito militar o de seguridad nacional. También puede suponer una emergencia nacional de alto calibre si un sistema público pierde el control sobre los centros de datos situados a lo largo del territorio y en los que se encuentran datos personales sensibles –desde la seguridad social hasta el registro civil–, e información sobre sectores económicos estratégicos. Ya ocurrió con el ciberataque *NotPetya* en 2017, dirigido por Rusia hacia Ucrania, el cual se presentó como un *ransomware* –un ciberataque por el que se secuestra un sistema a cambio de un rescate económico– cuando en realidad era un *wiper* dirigido a sectores estratégicos y agencias públicas –un ataque por el que se destruyen todos los datos del disco duro para que sean irrecuperables–, y que provocó pérdidas por 10.000 millones de dólares.

> "También puede suponer una emergencia nacional de alto calibre si un sistema público pierde el control sobre los centros de datos (…)"

En el actual conflicto en Ucrania, el gobierno ucraniano está tomando una posición preventiva en la defensa de su infraestructura digital, que busca adelantarse a cualquier tipo de toma física de los servicios, así como protegerse de cualquier ciberataque que, pese a haber ocurrido ya, en ningún caso ha sido a gran escala ni ha causado un efecto crítico hasta el momento. Por una parte, el Servicio Estatal de Comunicaciones Especiales y Protección de la Información del gobierno de Ucrania está preparando planes de contingencia y escenarios para borrar los servidores informáticos que hay a

lo largo del país y transferir todos los datos sensibles, primero a Kyiv, y posteriormente fuera del país, si fuera necesario, en caso de que las tropas rusas tomaran la capital.

Por otra parte, no se ha producido hasta el momento un ciberataque a gran escala que haya afectado a los pilares del sistema de seguridad ucraniano. Sí ha habido ciberataques en las últimas semanas, como ha sido la denegación distribuida de servicios (DDoS) contra páginas web oficiales por las que se bloqueaba su uso, e incursiones que buscaban atacar directamente la infraestructura digital del sector financiero, de organizaciones de ayuda humanitaria y de respuesta a emergencias. Varios actores están detrás de la defensa ante estos ciberataques: el propio continente de ciberseguridad de Ucrania, empresas privadas, la OTAN, la UE y ciber hacktivistas, como el grupo de Ciberpartisanos de Bielorrusia, que defienden la infraestructura ucraniana y están realizando actividades ofensivas contra sistemas rusos.

Capacidades actuales de protección digital en Ucrania

En este escenario, la capacidad de respuesta de Ucrania ante una posible toma de su infraestructura digital ha crecido en los últimos años, tanto a iniciativa propia como a través de la colaboración con terceros actores. Sin embargo, sigue teniendo ciertas necesidades que necesitan ser abordadas.

En primer lugar, el repliegue que se está produciendo actualmente de la infraestructura digital hacia la capital del país no es algo nuevo, aunque sí transitorio. Ya en 2014, el gobierno de Ucrania inició un proceso de centralización de los servidores informáticos y centros de datos tras la anexión de Crimea y la región de Donbás por parte de Rusia y los grupos separatistas. Este repliegue se hacía tanto con centros de datos como en cableado submarino, un activo a través del cual viaja el 99% del tráfico mundial de Internet a nivel global. Los cables submarinos son un componente estratégico de la seguridad global y que, sin embargo, no han sido demasiado explorados desde un punto de vista geopolítico.

En el caso de Ucrania, el Cable del Estrecho de Kerch que conecta Ilyich (Rusia) y Kerch (Ucrania) se estableció en abril de 2014, solo un mes más tarde de la anexión definitiva de Crimea. Es un cable pequeño –de 46 kilómetros–, pero es relevante estratégicamente porque fue creado por Rostelecom, la empresa pública de telecomunicaciones rusa. Tras la anexión, los proveedores de servicio de Internet en Crimea empezaron a utilizar este cable como ruta de este servicio hacia Rusia. El resto del territorio ucraniano –bajo control del gobierno central– tienen tráfico de Internet a través de otros cables conectados con los países a su oeste. En 2014 aparecieron noticias que, por un lado afirmaban que este cable había sido cortado por Rusia para bloquear el acceso a Internet, como otras asegurando que esto no había ocurrido, ya que el cable submarino era propiedad de una empresa rusa y había datos que mostraban las caídas de Internet.

Más allá de esta lucha de narrativas, a nivel material el gobierno de Ucrania ha acelerado sus planes de contingencia y de protección ante posibles vulnerabilidades en su infraestructura digital y, en buena medida, lo ha fortalecido en colaboración con la UE. En concreto, la UE ha apoyado la transformación digital de Ucrania con el programa

EU4DigitalUA, bajo el paraguas del *European Peace Facility* desde diciembre de 2020, con un proyecto de 25 millones de euros para el fortalecimiento institucional y el desarrollo de capacidades en la infraestructura digital del país, la mejora de la interoperabilidad de datos y de gobierno digital, así como el fomento de una ciudadanía y actores públicos y privados concienciados sobre la importancia de este tema. También se creó un capítulo de telecomunicaciones para realizar acciones conjuntas en el Acuerdo de Asociación UE-Ucrania en mayo de 2014, solo dos meses después de la anexión de Crimea.

Es un proyecto novedoso ya que normalmente estas ayudas de transformación digital se suelen canalizar a través de otras plataformas europeas –como es el Instrumento de Política Exterior (FPI), del Banco Europeo de Inversiones o de la Dirección General de Asociaciones Internacionales (INTPA). En este caso, se ha hecho a través del instrumento para la paz, con un claro foco en la importancia de la seguridad ucraniana en datos para toda la arquitectura de seguridad europea. También es destacable que la UE haya activado por primera vez en un contexto operacional los Equipos de Respuesta Rápida Cibernética y de Asistencia Mutua en Ciberseguridad (CRRT) a través del marco de la Cooperación Estructurada Permanente en materia de Defensa (PESCO) para dar apoyo cibernético a Ucrania. No es casualidad que este equipo esté coordinado por Lituania y, de los otros cinco países que participan, cuatro de ellos se encuentren en la Franja del Este (Croacia, Estonia, Polonia y Rumanía). Se está considerando enviar un equipo de entre ocho y 12 expertos a Ucrania, pero es algo todavía por decidir.

En ese sentido, la pregunta más importante es: ¿y si se toma la ciudad de Kyiv y toda la infraestructura crítica? El esfuerzo de fortalecimiento de la infraestructura tecnológica hacia dentro y el inicio de “ciberdiálogos” entre Ucrania y la UE en junio de 2021 son necesarios. Sin embargo, no vale solo con fortalecer la infraestructura tecnológica hacia dentro en colaboración con terceros.

Escenarios de respuesta

Hay varios escenarios y experiencias que permitirían a Ucrania proteger su infraestructura digital en mayor medida.

En primer lugar, se podría buscar un “refugio digital” en un país tercero. Es el caso de Estonia: tras el ciberataque masivo que se produjo a todos sus servicios gubernamentales en 2007 por parte de Rusia, decidió que el proceso de transformación digital en el que ya estaba inmerso debía complementarse con un nuevo pilar de cooperación internacional. Este pilar no debería ser solamente de apoyo técnico, sino también de asistencia mutua. En este sentido, Estonia llegó a un acuerdo con Luxemburgo para establecer la primera Embajada de Datos en el mundo. La Embajada de Datos es un servidor estonio que se encuentra ubicado fuera del país, pero que está bajo jurisdicción estonia. Todos los recursos de la Embajada están sujetos al control del gobierno de Estonia. El objetivo es el de asegurar la “continuidad digital” del Estado refugiándose en otro país. Para ello, el sistema de seguridad contra ciberataques o contra situaciones de crisis físicas que puedan afectar a la infraestructura digital se protegen con tecnología *blockchain* y son capaces, no solo de proporcionar copias de

seguridad de los datos, sino también de permitir que sigan operando los servicios más críticos.

Una Embajada de Datos es un modelo todavía poco aplicado en el mundo –solo lo han hecho Estonia y Mónaco, posteriormente, con Luxemburgo. Sin embargo, el hecho de que los servidores se sigan considerando embajadas soberanas plantea una oportunidad interesante tanto de adaptar la Convención de Viena sobre relaciones diplomáticas para dar apoyo diplomático al alojamiento de datos y sistemas informáticos ante crisis, como de que se pueda proveer de inmunidad al uso de datos cuando se considere necesario.

“Una Embajada de Datos es un modelo todavía poco aplicado en el mundo –solo lo han hecho Estonia y Andorra, posteriormente, con Luxemburgo.”

Ahora bien, el reto mayor es el de conseguir hacerlo con un país tercero, que sea a la vez confiable pero también estable para poder garantizar que la Embajada de Datos pueda sobrevivir en el tiempo y ante las crisis. También es importante que no haya restricciones legales para que el país de origen de los datos pueda implantar el nivel de seguridad que se considere oportuno –por ejemplo, en el caso de Estonia la Embajada de Datos tiene el nivel más alto para este tipo de servidores.

Un segundo escenario es el de apoyarse en las “diásporas” del país que viven en el extranjero. Por ejemplo, Irlanda y Lituania buscan estrechar lazos con sus nacionales que viven en el extranjero para promover el liderazgo de su país en inteligencia artificial, pero también como una forma de asegurar que los acuerdos de negocio y las cadenas de suministro puedan tener una relativa mayor seguridad con otros países.

Por otra parte, la UE creó en 2017 su Caja de Herramientas para la Ciberdiplomacia, según la cual puede emitir cibersanciones siempre y cuando exista unanimidad por parte de todos los Estados miembros. Por el momento, no se han aplicado en el caso de Ucrania-Rusia, aunque la efectividad de unas sanciones de este tipo, solo serían eficaces para detener el conflicto si van acompañadas de un apoyo a la defensa sobre el terreno.

En conclusión, no cabe duda de que Ucrania se encuentra en un momento de vulnerabilidad con su infraestructura digital. Puede que no haya habido un ciberataque a gran escala, pero la toma de centros de datos podría suponer una emergencia nacional tanto para la protección de las personas como de las infraestructuras físicas y la seguridad del país. En todo ello, Ucrania se ha apoyado en los últimos años en países terceros, pero una estrategia de salida, un “refugio digital”, sería un modelo necesario en caso de toma de la capital.